# Anneaux

Christian Jean CYRILLE

7 mars 2019

# Table des matières

# Chapitre 1

# Généralités

## 1.1 Définition

Soit un ensemble $A$ muni de deux lois internes $+$ et $\times$.
On dira que $(A, +, \times)$ est un anneau lorsque

1. $(A, +)$ est un groupe abélien. On notera $0_A$ son élément neutre.
2. $\times$ est associative et distributive par rapport à $+$.

Si $\times$ est commutative alors l'anneau $A$ est commutatif.
Si $A$ admet un élément neutre $1_A$ pour la loi $\times$ alors l'anneau est dit unitaire.

### 1.1.1 Remarque

Si $1_A = 1_B$ alors $A = \{0\}$

### 1.1.2 Exemples

$(\mathbb{C}, +, \times)$; $(\mathbb{R}, +, \times)$; $(\mathbb{Z}, +, \times)$ ; $(A[X], +, \times)$ où $A$ est un anneau.

### 1.1.3 Autres propriétés des anneaux

1. Un élément $x \in A$ est dit idempotent lorque $x^2 = x$.
2. Un élément $x \in A$ est dit nilpotent si $\exists n \in \mathbb{N} - \{0; 1\} \qquad x^n = 0_A$.
3. Si $A$ est unitaire alors un élement $x \in A$ est involutif lorsque $x^2 = 1_A$
4. On dira qu'un élément $x \neq 0_A$ est diviseur de zéro à gauche lorsque $\exists y \in A \quad y \neq 0_A$ et $xy = 0_A$
5. Un anneau est dit intègre s'il n'a aucun diviseur de zéro c'est-à-dire que : $\forall (a, b) \in A^2 \quad ab = 0 \Longrightarrow a = 0$ ou $b = 0$

### 1.1.4 Exemples d'anneau intègre et d'anneau non intègre

1. $(\mathbb{R}, +, \times)$ est un anneau intègre car $\forall (a,b) \in \mathbb{R}^2 \quad ab = 0 \Longrightarrow a = 0$ ou $b = 0$.
   En effet, si $ab = 0$ ou bien $a = 0$ CQFD. ou bien $a \neq 0$ donc $\frac{1}{a}$ existe d'où $\frac{1}{a}(ab) = \frac{1}{a}0$ donc $(\frac{1}{a}a)b = 0$ donc $1b = 0$ d'où $b = 0$. CQFD.
2. L'anneau des matrices carrées d'ordre 2 , $\mathcal{M}_2(\mathbb{R})$ n'est pas intègre car par exemple :
   $\begin{pmatrix} 1 & 0 \\ 1 & 0 \end{pmatrix} \neq \begin{pmatrix} 0 & 0 \\ 0 & 0 \end{pmatrix} et \begin{pmatrix} 0 & 0 \\ 1 & 0 \end{pmatrix} \neq \begin{pmatrix} 0 & 0 \\ 0 & 0 \end{pmatrix} et \begin{pmatrix} 1 & 0 \\ 1 & 0 \end{pmatrix} \begin{pmatrix} 0 & 0 \\ 1 & 0 \end{pmatrix} = \begin{pmatrix} 0 & 0 \\ 0 & 0 \end{pmatrix}$

## 1.2 Régles de calcul dans un anneau

### 1.2.1 Théorème

1. $\forall a \in A \quad a\,0 = 0\,a = 0$
2. $\forall (a,b) \in A^2 \quad a(-b) = (-a)b = -(ab)$
3. $\forall (a,b) \in A^2 \quad (-a)(-b) = (ab)$

### 1.2.2 Puissances entières dans un anneau unitaire

Soit $a \in A$ alors :

1. $a^0 = 1_A$
2. $\forall n \in \mathbb{N}^* \quad a^n = a\,a^{n-1} = \underbrace{a\,a\,a \cdots a}_{n fois}$

### 1.2.3 Formule du binôme de Newton (1643 - 1727)

Soient $a$ et $b$ des éléments **commutables** de l'anneau $A$ c'est-à-dire tels que donc $ab = ba$. Alors :

$$\forall n \in \mathbb{N}\ (a+b)^n = \sum_{i=0}^{n} \binom{n}{i} a^i\, b^{n-i}$$

Or $\binom{n}{p} = \binom{n}{n-p}$ donc $\forall n \in \mathbb{N}\ (a+b)^n = \sum_{j=0}^{n} \binom{n}{j} a^{n-j}\, b^j$
en effectuant le changement d'indice $j = n - i$

**Démonstration**

: Notons $pr(n) : (a+b)^n = \sum_{i=0}^{n} \binom{n}{i} a^i\, b^{n-i}$.

1. Initialisation : elle est vraie en $n = 0$ car :
   $(a+b)^0 = 1 = \binom{0}{0} a^0\, b^{0-0}$
2. Hérédité : Supposons que la propriété est vraie pour un entier fixé $k \geq 0$ c'est-à-dire que :
   $(a+b)^k = \sum_{i=0}^{k} \binom{k}{i} a^k\, b^{n-k}$

   Alors $(a+b)^{k+1} = (a+b)(a+b)^k = (a+b)[\sum_{i=0}^{k} \binom{k}{i} a^k\, b^{n-k}]$

   $= (a+b)(\binom{k}{0} a^0 b^k + \binom{k}{1} a^1\, b^{k-1} + \cdots + \binom{k}{i} a^i\, b^{k-i} + \cdots + \binom{k}{k-1} a^{k-1}\, b^1 + \binom{k}{k} a^k b^0)$

   $= (a+b)(b^k + \binom{k}{1} a^1\, b^{k-1} + \cdots + \binom{k}{i} a^i\, b^{k-i} + \cdots + \binom{k}{k-1} a^{k-1}\, b^1 + a^k)$

   $= (ab^k + \binom{k}{1} a^2\, b^{k-1} + \cdots + \binom{k}{i} a^{i+1}\, b^{k-i} + \cdots + \binom{k}{k-1} a^k\, b^1 + a^{k+1}$

   $+b^{k+1} + \binom{k}{1} a^1\, b^k + \cdots + \binom{k}{i} a^i\, b^{k-i+1} + \cdots + \binom{k}{k-1} a^{k-1}\, b^2 + a^k b)$

   $= b^{k+1} + ab^k[\binom{k}{1} + \binom{k}{0}] + a^2\, b^{k-1}[\binom{k}{2} + \binom{k}{1}] + \cdots + a^i\, b^{k-i+1}[\binom{k}{i} + \binom{k}{i-1}] +$

   $a^{i+1}\, b^{k-i}[\binom{k}{i} + \binom{k}{i+1}] + \cdots + a^k\, b^1[\binom{k}{k} + \binom{k}{k-1}] + a^{k+1}$

   $= b^{k+1} + ab^k \binom{k+1}{1} + a^2\, b^{k-1} \binom{k+1}{2} + \cdots + a^i\, b^{k-i+1} \binom{k+1}{i} + a^{i+1}\, b^{k-i} \binom{k+1}{i+1} +$

   $\cdots + a^k\, b^1 \binom{k+1}{k} + a^{k+1}$

   $= \binom{k+1}{0} a^0 b^{k+1} + ab^k \binom{k+1}{1} + a^2\, b^{k-1} \binom{k+1}{2} + \cdots + a^i\, b^{k-i+1} \binom{k+1}{i} + a^{i+1}\, b^{k-i} \binom{k+1}{i+1} +$

   $\cdots + a^k\, b^1 \binom{k+1}{k} + \binom{k+1}{k+1} a^{k+1} b^0$
3. Conclusion : $pr$ étant initialisée en 0 et étant héréditaire est donc vraie pour tout entier naturel $n \geq 0$

**Cette formule est valable pour tous éléments $a$ et $b$ d'un anneau à condition que ces éléments soient commutables c'est-à-dire que $ab = ba$.**
C'est le cas pour des matrices carrées d'ordre $n$ : $A$ et $B$ à condition d'avoir vérifié que $AB = BA$.
Souvent $A = I$ la matice de l'identité donc $IB = B$ et $BI = B$ donc $IB = BI$ donc

$$\forall n \in \mathbb{N}\ (I+B)^n = \sum_{j=0}^{n} \binom{n}{j} I^{n-j}\, b^j = \sum_{j=0}^{n} \binom{n}{j} I\, B^j = \sum_{j=0}^{n} \binom{n}{j} B^j$$

### 1.2.4 Formule d'inversion de Pascal

Soient des familles $(a_i)_{0\leq i\leq n}$ et $(b_j)_{0\leq j\leq n}$ d'éléments d'un anneau commutatif.
Si $a_p = \sum_{k=0}^{p} \binom{p}{k} b_k$ alors $b_p = \sum_{k=0}^{p} \binom{p}{k} (-1)^{p-k} a_k$

**Démonstration utilisant la matrice des coefficients binomiaux**

- Notons $A_n = \begin{pmatrix} a_1 \\ a_2 \\ \vdots \\ a_n \end{pmatrix}$ et $B_n = \begin{pmatrix} b_1 \\ b_2 \\ \vdots \\ b_n \end{pmatrix}$. Alors si on a $a_p = \sum_{k=0}^{p} \binom{p}{k} b_k$ alors $A_n = M_n B_n$ où
$$M_n = \begin{pmatrix} 1 & 0 & 0 & \cdots & 0 & 0 \\ 1 & 1 & 0 & \cdots & 0 & 0 \\ 1 & 2 & 1 & \cdots & 0 & 0 \\ \vdots & & & & & \\ \binom{n}{0} & \binom{n}{1} & \binom{n}{2} & \cdots & \binom{n}{n-1} & \binom{n}{n} \end{pmatrix}$$
- $M_n$ est une matrice triangulaire de déterminant 1 donc $M_n$ est inversible. Il reste à déterminer son inverse $M_n^{-1}$ pour exprimer les $b_p$ en fonction des $a_p$.
- Or $\begin{pmatrix} 1 \\ 1+X \\ (1+X)^2 \\ \vdots \\ (1+X)^n \end{pmatrix} = \begin{pmatrix} 1 & 0 & 0 & \cdots & 0 & 0 \\ 1 & 1 & 0 & \cdots & 0 & 0 \\ 1 & 2 & 1 & \cdots & 0 & 0 \\ \vdots & & & & & \\ \binom{n}{0} & \binom{n}{1} & \binom{n}{2} & \cdots & \binom{n}{n-1} & \binom{n}{n} \end{pmatrix} \begin{pmatrix} 1 \\ X \\ X^2 \\ \vdots \\ X^n \end{pmatrix}$
donc $\begin{pmatrix} 1 \\ X \\ X^2 \\ \vdots \\ X^n \end{pmatrix} = M_n^{-1} \begin{pmatrix} 1 \\ 1+X \\ (1+X)^2 \\ \vdots \\ (1+X)^n \end{pmatrix}$
- La famille $(1, 1+X, (1+X)^2, \cdots, (1+X)^n)$ étant une famille de polynômes de degrés échelonnés dans $K_n[X]$ est donc une base de $K_n[X]$.
Dans cette base, déterminons alors l'écriture de $X^p$ : $X^p = (1+X-1)^p = \sum_{k=0}^{p} (-1)^{p-k} (1+X)^k$
Par conséquent,
$$M_n^{-1} = \begin{pmatrix} 1 & 0 & 0 & \cdots & 0 & 0 \\ -1 & 1 & 0 & \cdots & 0 & 0 \\ 1 & -2 & 1 & \cdots & 0 & 0 \\ \vdots & & & & & \\ (-1)^n \binom{n}{0} & (-1)^{n-1} \binom{n}{1} & (-1)^{n-2} \binom{n}{2} & \cdots & (-1)^1 \binom{n}{n-1} & (-1)^0 \binom{n}{n} \end{pmatrix}$$
Donc $b_p = \sum_{k=0}^{p} \binom{p}{k} (-1)^{p-k} a_k$

## 1.3 Elements inversibles ou unités d'un anneau unitaire

### 1.3.1 Définition

Soit $(A, +, \times)$ un anneau unitaire d'élément-unité $1_A$.
Un élément $u$ de $A$ est dit inversible si $\exists v \in A \quad uv = vu = 1_A$.
Un élément inversible de $A$ s'appelle aussi une unité de $A$.
On note $\mathcal{U}$ l'ensemble des éléments inversibles de l'anneau unitaire $A$.

### 1.3.2 Propriétés

$(\mathcal{U}, \times)$ est un groupe.

**Démonstration**

- $\mathcal{U} \subset A$ donc $\times$ est associative dans $\mathcal{U}$
- $1_A \in \mathcal{U}$ donc $\times$ admet $1_A$ comme élément neutre dans $\mathcal{U}$
- Tout élément $u \in \mathcal{U}$ a un symétrique $v$ dans $\mathcal{U}$ pour la loi $\times$ par définition.

Par conséquent, $(\mathcal{U}, \times)$ est un groupe.

### 1.3.3 Exemples

1. Si $(\mathbb{K}, +, \times)$ est un corps alors $(\mathbb{K}, +, \times)$ est un anneau avec comme ensemble des éléments inversibles $\mathcal{U} = \mathbb{K}^* = \mathbb{K} - \{O_{\mathbb{K}}\}$
2. $(\mathbb{Z}, +, \times)$ est un anneau commutatif unitaire intègre.
   $\mathcal{U} = \{-1; 1\}$ qui est un sous-groupe cyclique d'ordre 2.
3. $(\mathbb{Z}/p\mathbb{Z}, +, \times)$ est un anneau unitaire.
   $\mathbb{Z}/p\mathbb{Z}$ est un corps si et seulement si $p$ est premier.
   $\mathcal{U}$ est l'ensemble des classes $\bar{x}$ telles que $x$ et $p$ sont premiers entre eux.
4. L'ensemble $(\mathcal{M}_n, +, \times)$ des matrices carrées d'ordre $n$ à coefficients dans un corps $\mathbb{K}$ est un anneau non commutatif, unitaire avec $1_{\mathcal{M}_n} = I$ la matrice identité.
   $\mathcal{U}(\mathcal{M}_n)$ est l'ensemble $\mathcal{GL}_n$ des matrices carrées inversibles c'est-à-dire l'ensemble des matrices carrées de déterminant non nul.
5. L'ensemble $(\mathcal{L}(E), +, \circ)$ des endomorphismes de l'espace vectoriel $E$ sur un corps $\mathbb{K}$ est un anneau non commutatif, unitaire avec $id_E$ l'élément unité.
   $\mathcal{U}(\mathcal{L}(E))$ est l'ensemble $\mathcal{G}(E)$ des endomorphismes bijectifs( ou automorphismes) c'est-à-dire l'ensemble des endomorphismes de déterminant non nul.

## 1.4 Sous-anneaux

### 1.4.1 Définition

Soit $(A, +, \times)$ un anneau. Soit $A'$ une partie non vide de $A$.
On dira que $(A', +, \times)$ est un sous-anneau de $(A, +, \times)$ lorsque les restrictions de $+$ à $A' \times A'$ et de $\times$ à $A' \times A'$ confèrent à $A'$ une structure d'anneau.

### 1.4.2 Propriété caractéristique

$$(A', +, \times) \text{ est un sous-anneau de} (A, +, \times) \iff \begin{cases} (A', +) \text{ est un sous-groupe de } (A, +) \\ \times \text{ est interne dans } A' \end{cases}$$

$$\iff \begin{cases} 1_A \in A' \\ \forall x \in A' \quad \forall y \in A' \quad x - y \in A' \\ \forall x \in A' \quad \forall y \in A' \quad x\,y \in A' \end{cases}$$

### 1.4.3 Exercice

Soit l'ensemble $\mathbb{Z}[i] = (\{a + ib \ / \ a \in \mathbb{Z},\ b \in \mathbb{Z}\}, +, \times)$.

1. Démontrer que $(\mathbb{Z}[i], +, \times)$ est un anneau appelé anneau des entiers de Gauss.
2. Démontrer que $\forall z \in \mathbb{Z}[i]^* \quad |z| \geq 1$.
3. En déduire que l'ensemble des éléments inversibles $\mathcal{U}$ est $\{-1; 1; i; -i\}$

1. $(\mathbb{Z}[i], +, \times)$ est un anneau car c'est un sous-anneau de l'anneau $(\mathbb{C}, +, \times)$.
   En effet,
   (a) $1_{\mathbb{C}} = 1 = 1 + 0i \in \mathbb{Z}[i]$
   (b) $\forall \alpha \in Z[i] \quad \forall \beta \in Z[i] \quad \alpha - \beta \in \mathbb{Z}[i]$ :
   En effet, $\alpha - \beta = a + ib - (a' + ib') = (a - a') + i(b - b') \in \mathbb{Z}[i]$ car $a - a' \in \mathbb{Z}$ et $b - b' \in \mathbb{Z}$ puisque $a \in \mathbb{Z}, a' \in \mathbb{Z}, b \in \mathbb{Z}, b' \in \mathbb{Z}$
   (c) $\forall \alpha \in Z[i] \quad \forall \beta \in Z[i] \quad \alpha\beta \in \mathbb{Z}[i]$ :
   En effet, $\alpha\beta = (a + ib)(a' + ib') = (aa' - bb') + i(ab' + ba') \in \mathbb{Z}[i]$ car $aa' - bb' \in \mathbb{Z}$ et $ab' + ba' \in \mathbb{Z}$ puisque $a \in \mathbb{Z}, a' \in \mathbb{Z}, b \in \mathbb{Z}, b' \in \mathbb{Z}$
2. Soit $z = a + ib \in \mathbb{Z}[i]^*$ alors $|z|^2 = a^2 + b^2 \geq 1$ car $a^2 \geq 1$ ou $b^2 \geq 1$ puisque $a^2 \in \mathbb{N}^*$ ou $a^2 \in \mathbb{N}^*$.
   Par conséquent, $|z| \geq 1$.
3. Si $\alpha \in \mathbb{Z}[i]$ est inversible alors $\exists \beta \in \mathbb{Z}[i] \quad \alpha\beta = 1$ donc $\alpha \neq 0$ et $\beta = \dfrac{1}{\alpha}$.
   Or $|\alpha| \geq 1$ et $|\beta| \geq 1$ donc $|\alpha| \geq 1$ et $|\beta| = \dfrac{1}{|\alpha|} \geq 1$ d'où $|\alpha| = 1$.
   Par conséquent, comme $|\alpha|^2 = a^2 + b^2 = 1$ avec $a \in \mathbb{Z}$ et $b \in \mathbb{Z}$
   d'où 4 cas :
   $\begin{cases} a = 1 \\ b = 0 \end{cases}$ ou $\begin{cases} a = -1 \\ b = 0 \end{cases}$ ou $\begin{cases} a = 0 \\ b = 1 \end{cases}$ ou $\begin{cases} a = 0 \\ b = -1 \end{cases}$
   donc $\boxed{\mathcal{U} = \{-1\ ;\ 1\ ;\ i\ ;\ -i\}}$

### 1.4.4 Autre propriété

Toute intersection de sous-anneaux de $A$ est un sous-anneau de $A$.

### 1.4.5 Remarque

La réunion de sous-anneaux de $A$ n'est pas forcément un sous-anneau de $A$.

### 1.4.6 Famille filtrante de sous-anneaux

On appelle famille filtrante $(B_i)$ de sous-anneaux de $A$ toute famille de sous-anneaux tels que : $\begin{cases} \forall (i,j) \in I^2 \quad \exists k \in I \quad B_i \cup B_j \subset B_k \\ \text{Si } B_j \subset B_I \text{ alors } B_j \text{ est un sous-anneau de } B_i \end{cases}$ Toute union d'une famille filtrante de sous-anneaux de $A$ est un sous-anneau de $A$

## 1.5 Morphismes d'anneaux

### 1.5.1 Définition

Soient des anneaux $(A, +, \times)$ et $(B, \oplus, \otimes)$.
On appelle morphisme de l'anneau $A$ vers l'anneau $B$ toute application $f$ qui vérifie les deux propriétés suivantes :

1. $f$ est un morphisme du groupe $(A, +)$ vers le groupe $(B, +)$ c'est-à-dire que :
   $\forall (x, y) \in A^2 \quad f(x + y) = f(x) + f(y)$
2. $\forall (x, y) \in A^2 \quad f(x \times y) = f(x) \otimes f(y)$

### 1.5.2 Autres définitions

Soit $f$ un morphisme de l'anneau $(A, +, \times)$ vers l'anneau $(B, \oplus, \otimes)$.

- Un morphisme d'anneau s'appelle aussi un homomorphisme.
- Si $A = B$ alors $f$ est appelé un endomorphisme.
- Si $f$ est bijective alors $f$ est appelé un isomorphisme.
- Si $f$ est bijective et que $A = B$ alors $f$ est appelé un automorphisme.

### 1.5.3 Propriétés

Soit $f$ un morphisme de l'anneau $(A, +, \times)$ vers l'anneau $(B, \oplus, \otimes)$. Alors :

1. $f(0_A) = 0_B$
2. $\forall x \in A \quad f(-x) = -f(x)$
3. $(f < A >, \oplus)$ est un sous-groupe de $(B, \oplus)$
4. $f^{-1} < \{0_B\} >$ est un sous-groupe de $(A, +)$

### 1.5.4 Définition

Soient $A$ et $B$ des anneaux unitaires avec comme éléments unités respectifs $1_A$ et $1_B$.
Un morphisme de l'anneau $A$ vers l'anneau $B$ est dit unitaire lorsque $f(1_A) = 1_B$

### 1.5.5 Exemple de morphisme

Soit $A$ un anneau unitaire d'élément-unité $1_A$. Alors l'application

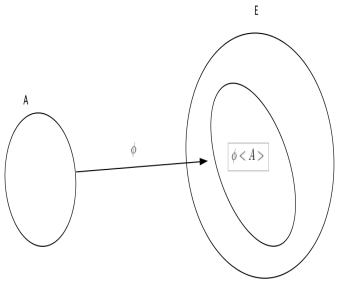
$$\begin{array}{rccccl} \phi : & \mathbb{Z} & \longrightarrow & & A & \\ & n & \longmapsto & \phi(n) = \left\{ \begin{array}{ll} n(1_A) & \text{si } n > 0 \\ 0_A & \text{si } n = 0 \\ (-n)(1_A) & \text{si } n < 0 \end{array} \right. & & \end{array}$$

est un morphisme d'anneau appelé morphisme naturel de $(\mathbb{Z}, +, \times)$ dans $(A, +, \times)$.
$\phi(\mathbb{Z}) = \mathbb{Z}1_A$ est donc un sous-groupe additif de $(A, +)$ et mieux un sous-anneau.
Son noyau $ker(\phi) = \{n \in \mathbb{Z} \ / \ \phi(n) = 0_A\}$ est un sous-groupe de $(\mathbb{Z}, +)$ donc de la forme $p\mathbb{Z}$.
**Le plus petit de ces $p$ est appelé la caractéristique de l'anneau $A$**

## 1.6 Extensions d'anneaux

### 1.6.1 Définition

Soit $(A, +, \times)$ un anneau.
On appelle extension de $A$ tout anneau $E$ tel qu'il existe un morphisme injectif $\phi$ de $A$ dans $E$.
$\phi < A >$ est alors un sous-anneau de $E$ isomorphe à $A$.




### 1.6.2 Propriété

Si $A$ est un sous-anneau de l'anneau $E$ alors $E$ est une extension de $A$.

### 1.6.3 Extension unitaire

L'extension $E$ d'un anneau $A$ est unitaire lorsque les deux anneaux sont unitaires et que $\phi(1_A) = 1_E$

**Exemples**

1. $(\mathbb{Q}, +, \times)$ est une extension unitaire de $(\mathbb{Z}, +, \times)$
2. $\mathbb{F}_n = \mathbb{Z}/n\mathbb{Z}$ est une extension unitaire de $\mathbb{F}_p = \mathbb{Z}/p\mathbb{Z}$ quand $n$ divise $p$
   car le morphisme
   $$\begin{array}{rccc} \phi : & \mathbb{Z}/n\mathbb{Z} & \longrightarrow & \mathbb{Z}/p\mathbb{Z} \\ & \dot{x} & \longmapsto & \phi(\dot{x}) = \bar{x} \end{array}$$
   est injectif.

### 1.6.4 Extension $A$-isomorphes

Deux extensions $E_1$ et $E_2$ d'un anneau $A$ sont dites $A$-isomorphes lorsque'il existe un isomorphisme $\phi$ de $E_1$ sur $E_2$ tel que $\phi/A = id_A$

### 1.6.5 Extension simple

Soit $(B, +, \times)$ un anneau. Soit $A$ un sous-anneau de $B$. Soit $\varepsilon \in B$ tel que $\varepsilon \notin A$.
On appelle $A[\varepsilon]$ le sous-anneau engendré par la partie $A \cup \{\varepsilon\}$ c'est-à-dire l'intersection de tous les sous-anneaux de $B$ contenant $A \cup \{\varepsilon\}$.

**Propriété**

$A[\varepsilon]$ est l'ensemble $\mathcal{P}$ des expressions polynomiales de la forme $\sum a_i \varepsilon^i$ où $\forall i \quad a_i \in A$. On l'appelle **une extension simple de l'anneau** $A$.
Cette extension est dite unitaire si $B$ et $A$ sont unitaires et que $1_B = 1_A$

Démonstration

- $\mathcal{P} \subset A[\varepsilon]$
  Soit $P \in \mathcal{P}$ donc $P = \sum a_i \varepsilon^i$.
  $\forall i \in [|0..n|] \quad a_i \in A$ donc $a_0 \in A[\varepsilon]$
  et $\forall i \in [|0..n|] \quad \varepsilon^i \in A[\varepsilon]$ car est un anneau donc le produit d'éléments de $A[\varepsilon]$ est un élément de $A[\varepsilon]$
  Donc $\forall i \in [|0..n|] \quad a_i \varepsilon^i \in A[\varepsilon]$. Par conséquent, $P = \sum a_i \varepsilon^i \in A[\varepsilon]$
- Il reste à prouver que $A[\varepsilon] \subset \mathcal{P}$.
  Pour cela, il suffira de prouver que $P$ est un sous-anneau de $B$ qui contient $A[\varepsilon]$.
  — $\mathcal{P} \subset B$.
  — $(\mathcal{P}, +)$ est un sous-groupe car
    — $\mathcal{P} \neq \emptyset$ puisque $0_B \in \mathcal{P}$
    — $\forall P_1 \in \mathcal{P} \quad \forall P_2 \in \mathcal{P} \quad P_1 - P_2 = \sum a_i \varepsilon^i - \sum b_i \varepsilon^i = \sum (a_i - b_i)\varepsilon^i \in \mathcal{P}$
  — $\forall P_1 \in \mathcal{P} \quad \forall P_2 \in \mathcal{P} \quad P_1 P_2 = \left(\sum a_i \varepsilon^i\right)\left(\sum b_i \varepsilon^i\right) = \sum c_k \varepsilon^k \in \mathcal{P}$
  — Donc $\mathcal{P}$ est un sous-anneau de $B$
  — $A[\varepsilon] \subset \mathcal{P}$ car $\{\varepsilon\} \subset \mathcal{P}$ puisque $\varepsilon \in \mathcal{P}$ et $A \subset \mathcal{P}$ puisque $\forall a \in A \quad a = a + \sum_{i=1}^{n} 0\varepsilon^i$

**Exemples**

1. $\sqrt{2} \notin \mathbb{Q}$ et $\mathbb{Q}[\sqrt{2}] = \{\sum a_i (\sqrt{2})^i \ / \ a_i \in \mathbb{Q}\} = \{a + b\sqrt{2} \ / \ a \in \mathbb{Q}, b \in \mathbb{Q}\}$
2. $\sqrt{3} \notin \mathbb{Q}$ et $\mathbb{Q}[\sqrt{3}] = \{\sum a_i (\sqrt{3}) \ / \ a_i \in \mathbb{Q}\} = \{a + b\sqrt{3} \ / \ a \in \mathbb{Q}, b \in \mathbb{Q}\}$
3. $i \notin \mathbb{Z}$ et $\mathbb{Z}[i] = \{\sum a_n i^n \ / \ a_n \in \mathbb{Z}\} = \{a + bi \ / \ a \in \mathbb{Z}, b \in \mathbb{Z}\}$
   $\mathbb{Z}[i]$ s'appelle l'anneau des entiers de Gauss.

**Propriétés**

Soit $(B, +, \times)$ un anneau commutatif unitaire tel que $1_B \in A$.
Soit $m \in A$ tel que $\sqrt{m} \notin A$ et tel que $A \cap A[\sqrt{m}] = \{0_A\}$
Alors :

1. $\forall (a,b) \in A \quad a + b\sqrt{m} = 0 \iff a = b = 0.$
2. $\forall (a,b) \in A \quad \forall (a',b') \in A \quad a + b\sqrt{m} = a' + b'\sqrt{m} \iff a = a'$ et $b = b'$.
3. Si $\alpha = a + b\sqrt{m}$ on appelle $\bar{\alpha} = a - b\sqrt{m}$ le conjugué de $\alpha$.
   On pose alors
   $$\begin{array}{rccc} N : & A[\sqrt{m}] & \longrightarrow & A \\ & \alpha = a + b\sqrt{m} & \longmapsto & N(\alpha) = \alpha\bar{\alpha} = a^2 - mb^2 \end{array}$$
   Démontrer que $\forall \alpha \in A[\sqrt{m}] \quad \forall \alpha' \in A[\sqrt{m}] \quad N(\alpha\alpha') = N(\alpha)N(\alpha')$
   c'est-à-dire que $N$ est un homomorphisme du groupe $(A[\sqrt{m}], \times)$ vers le groupe $(A, \times)$
4. Si $A$ est intégre alors :
   $$A[\sqrt{m}] \text{ est intègre } \iff (N(\alpha) = 0 \Longrightarrow \alpha = 0)$$
5. Soit $\alpha \in A[\sqrt{m}]$ et $\alpha$ non nul,
   Démontrer que : $\alpha$ est inversible $\iff N(\alpha)$ est inversible dans $A$.
6. En déduire que si $\alpha$ est inversible alors $\alpha^{-1} = \dfrac{\bar{\alpha}}{N(\alpha)}$

**Démonstrations :**

1. $\forall (a,b) \in A \quad a + b\sqrt{m} = 0 \iff a = b = 0$. démonstration à faire.
2. On en déduit que $\forall (a,b) \in A \quad \forall (a,b) \in A$
   $a + b\sqrt{m} = a' + b'\sqrt{m} \iff a - a' + b\sqrt{m} - b'\sqrt{m} = 0$
   $\iff (a - a') + (b - b')\sqrt{m} = 0 \iff a - a' = 0$ et $b - b' = 0 \iff a = a'$ et $b = b'$.
3. Si $\alpha = a + b\sqrt{m}$ et $\alpha' = a' + b'\sqrt{m}$ alors :
   $N(\alpha\alpha') = N((a + b\sqrt{m})(a' + b'\sqrt{m})) = N((aa' + mbb') + (ab' + a'b)\sqrt{m})$
   $= (aa' + mbb')^2 - m(ab' + a'b)^2 = a^2a'^2 + m2b^2b'^2 + 2aa'mbb' - ma^2b'^2 - ma'^2b^2 - 2mab'a'b$
   $= a^2a'^2 + m^2b^2b'^2 - ma^2b'^2 - ma'^2b^2$
   $= (a^2 - mb^2)(a'^2 - mb'^2) = N(\alpha)N(\alpha')$

4. Supposons que $A$ est intégre alors :
   - $\Longleftarrow$ :
     Supposons que $(N(\alpha) = 0 \Longrightarrow \alpha = 0)$.
     Soient $\alpha$ et $\alpha'$ éléments de $A[\sqrt{m}]$ tels que $\alpha\alpha' = 0$ alors
     $N(\alpha)N(\alpha') = N(\alpha\alpha') = N(0) = 0$.
     Or $N(\alpha)$ et $N(\alpha')$ sont des éléments de l'anneau $A$ qui est intègre
     donc $N(\alpha) = 0$ ou $N(\alpha') = 0$ donc $\alpha = 0$ ou $\alpha' = 0$.
     Par conséquent ,$A[\sqrt{m}]$ est intègre.
   - $\Longrightarrow$ :
     Supposons que $A[\sqrt{m}]$ est intègre.
     Posons $\alpha = a + b\sqrt{m}$. Supposons que $N(\alpha) = 0$ alors $(a + b\sqrt{m})(a - b\sqrt{m}) = 0$.
     Nous sommes en présence du produit nul de deux éléments de l'anneau $A[\sqrt{m}]$ qui est intègre donc $a + b\sqrt{m} = 0$ ou $a - b\sqrt{m} = 0$.
     Par conséquent, quelque soit le cas, d'après le $1^\circ$) on obtient $a = b = 0$ d'où $\alpha = 0$.
     CQFD.
5. Soit $\alpha \in A[\sqrt{m}]$ et non nul,
   - $\Longrightarrow$:
     Supposons que $\alpha$ est inversible donc $\exists \alpha' \in A[\sqrt{m}] \quad \alpha\alpha' = 1$.
     Donc $N(\alpha\alpha') = N(1)$ d'où $N(\alpha)N(\alpha') = 1$ donc $\mathbb{N}(\alpha)$ est inversible dans $A$ d'inverse $\dfrac{1}{N(\alpha)}$
   - $\Longleftarrow$:
     Supposons que $\mathbb{N}(\alpha)$ est inversible dans $A$ donc $\exists a' \in A \quad N(\alpha)a' = 1$ donc $\alpha\bar{\alpha}a' = 1$
     donc $\alpha$ est inversible et $\alpha^{-1} = \bar{\alpha}a'$
6. Comme $N(\alpha)a' = 1$ donc $a' = \dfrac{1}{N(\alpha)}$ avec $N(\alpha) \neq 0$ puisque $\alpha \neq 0$.
   Par conséquent, si $\alpha$ est inversible alors $\alpha^{-1} = \dfrac{\bar{\alpha}}{N(\alpha)}$

**L'anneau des entiers de Gauss**

L'anneau des entiers de Gauss est $\mathbb{Z}[i] = \{\sum a_n i^n \ / \ a_n \in \mathbb{Z}\} = \{a + bi \ / \ a \in \mathbb{Z}, b \in \mathbb{Z}\}$

1. L'ensemble des éléments inversibles de $\mathbb{Z}[i]$ est $\mathcal{U} = \{-i, -1; 1; i\}$
2. Soient $\alpha$ et $\beta \neq 0$ des éléments de $\mathbb{Z}[i]$.
   (a) $\beta$ divise $\alpha \Longrightarrow N(\beta) \leq N(\alpha)$
   (b) $\exists (q, r) \in \mathbb{Z}[i]^2 \quad \alpha = \beta q + r$ avec $(r = 0)$ ou $N(r) < N(\beta)$.
   **Cette application $N$ est appelée une valuation euclidienne ce qui fait de $(\mathbb{Z}[i], +, \times)$ un anneau euclidien**.
   Pour démontrer ceci, on pose $\frac{\alpha}{\beta} = x + iy$ où $x \in \mathbb{Q}$ et $y \in \mathbb{Q}$.
   On prend alors $(a, b) \in \mathbb{Z}^2 \quad |x - a| \leq \frac{1}{2}$ et $|y - b| \leq \frac{1}{2}$.
   Montrer qu'alors $\alpha = \beta(a + ib) + r$ avec $N(r) < N(\beta)$.
   Dans quel cas a-t-on l'unicité ?
   (c) Illustrer graphiquement le cas où $\alpha = 3 + 2i$ et $\beta = 2 + i$.
   (d) Illustrer graphiquement le cas où $\alpha = i$ et $\beta = 1 + i$
   (e) Déterminer le pgcd de $3 + 4i$ et de $4 - 3i$ puis le pgcd de $3 + 4i$ et de $-5i$.

Démonstration

1. $\alpha = a + ib$ est inversible dans $\mathbb{Z}[i]$
   $\Longleftrightarrow$ $N(\alpha) = a^2 + b^2$ est inversible dans $\mathbb{Z}$.
   $\Longleftrightarrow$ $a^2 + b^2 = 1$ ou $a^2 + b^2 = -1$ car les seuls éléments inversibles de $\mathbb{Z}$ sont 1 et $-1$
   $\Longleftrightarrow$ $a^2 + b^2 = 1$ car $a^2 + b^2 \geq 0$
   $\Longleftrightarrow \begin{cases} a = 1 \\ b = 0 \end{cases}$ ou $\begin{cases} a = -1 \\ b = 0 \end{cases}$ ou $\begin{cases} a = 0 \\ b = 1 \end{cases}$ ou $\begin{cases} a = 0 \\ b = -1 \end{cases}$
   car $a$ et $b$ sont des entiers relatifs.
   Donc l'ensemble des éléments inversibles de $\mathbb{Z}[i]$ est $\mathcal{U} = \{-i, -1; 1; i\}$
2. Soient $\alpha$ et $\beta$ des éléments de $\mathbb{Z}[i]$.
   (a) Si $\beta$ divise $\alpha$ alors $\exists \gamma \in Z[i] \quad \alpha = \beta\gamma$ donc $N(\alpha) = N(\beta\gamma) = N(\beta)N(\gamma)$ donc $N(\beta)$ divise $N(\alpha)$.
   Par conséquent, $N(\beta) \leq N(\alpha)$
   (b) Soient $\alpha = a + ib \in Z[i]$ et $\beta = a' + ib' \in Z[i]$ alors :
   $\frac{\alpha}{\beta} = \frac{a + ib}{a' + ib'} = \frac{(a + ib)(a' - ib')}{(a' + ib')(a' - ib')} = \frac{aa' + bb' + i(a'b - ab')}{a'^2 + b'^2} = x + iy$
   où $x = \frac{aa' + bb'}{a'^2 + b'^2} \in \mathbb{Q}$ et $y = \frac{a'b - ab'}{a'^2 + b'^2} \in \mathbb{Q}$.
   On prend alors $(u, v) \in \mathbb{Z}^2 \quad |x - u| \leq \frac{1}{2}$ et $|y - v| \leq \frac{1}{2}$.
   On prend $q = u + iv \in Z[i]$ alors $|\frac{\alpha}{\beta} - q| \leq \sqrt{|x - u|^2 + |y - v|^2} = \frac{\sqrt{2}}{2} < 1$
   Posons $r = \alpha - q\beta$ alors $r \in Z[i]$ et $|r| = |\beta||\frac{\alpha}{\beta} - q| < |\beta|$ On a donc trouvé $(q, r) \in Z[i]^2$ tels que $\alpha = \beta q + r$ avec $N(r) < N(\beta)$.

(c) Illustrer graphiquement le cas où $\alpha = 3 + 2i$ et $\beta = 2 + i$.

(d) Illustrer graphiquement le cas où $\alpha = i$ et $\beta = 1 + i$

## 1.7 Caractéristique d'un anneau

### 1.7.1 Définition

Soit $A$ un anneau unitaire. On note $0_A$ son élément neutre et $1_A$ son élément unité.
Soit l'application $\phi$ de $\mathbb{Z}$ dans $A$ qui à $n \mapsto \phi(n) = \begin{cases} n(1_A) & \text{si } n > 0 \\ 0_A & \text{si } n = 0 \\ (-n)(1_A) & \text{si } n < 0 \end{cases}$
Alors $\phi$ est un morphisme d'anneaux et $ker(\phi) = \{n \ / \ n(1_A) = 0_A\}$ est un sous-groupe de $\mathbb{Z}$ donc est de la forme $p\mathbb{Z}$. On suppose que p est le plus petit des éléments strictement positifs de $p\mathbb{Z}$. $p$ s'appelle la caractéristique de l'anneau A. On notera $p = car(A)$.

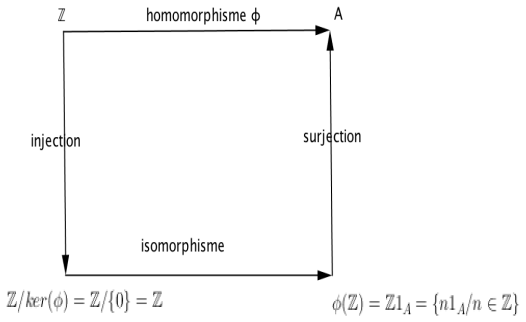
### 1.7.2 Propriétés

Soit un anneau $A$ de caractéristique $car(A) = p$. Alors

1. $\forall a \in A \quad pa = 0_A$
2. Tout autre entier naturel $q$ tel que $\forall a \in A \quad qa = 0_A$ alors $q$ est un multiple de $p$
3. Si $p = 0$ alors $A$ est un anneau infini.
4. Si $A$ est intègre alors $p = 0$ ou $p$ est premier.
   Par conséquent, comme un corps est un anneau intègre, la caractéristique d'un corps $\mathbb{K}$ est soit 0 soit un nombre premier
5. $\binom{p}{i}$ est un multiple de $p$ donc si $a$ et $b$ sont des éléments commutables de A alors $(a+b)^p = a^p + b^p$
6. Si $A$ est un anneau unitaire alors l'anneau $A[X]$ est unitaire et ont même élément unité donc même caractéristique.

Démonstration

1. $pa = (p1_A)a = 0_A a = 0_A$
2. si $qa = 0_A$ alors $\phi(q) = 0_A$ donc $q \in ker(\phi) = p\mathbb{Z}$ donc $p \mid q$.
3. si $car(A) = p = 0$ alors $ker(\phi) = p\mathbb{Z} = 0\mathbb{Z} = \{0\}$ donc $\phi$ est injectif.
   D'après le schéma de décomposition d'un homomorphisme



$A$ est donc un anneau qui contient le sous-anneau $\phi(\mathbb{Z}) = \mathbb{Z}1_A$ qui est infini car ce sous anneau est isomorphe à $\mathbb{Z}/0\mathbb{Z}$ c'est-à-dire isomorphe à $\mathbb{Z}$.
Par conséquent, $A$ est infini.

4. ou bien $p = 0$. CQFD
ou bien $p \neq 0$. Supposons que $p$ n'est pas premier donc il existe deux diviseurs $d_1$ et $d_2$ de $p$ compris entre 2 et $p-1$ tels que $p = d_1 d_2$ .
Comme $p1_A = 0_A$ donc $(d_1 d_2)1_A = 0_A$ . Alors $(d_1 1_A)(d_2 1_A) = 0_A$ mais comme $A$ est intègre alors $d_1 1_A = 0_A$ ou $d_2 1_A = 0_A$. Ce n'est pas possible car $p$ est le plus petit entier tel que $p1_A = 0_A$
5. - $\binom{p}{i} = \frac{p!}{i!(p-i)!} = \frac{p(p-1)\cdots(p-i+1)}{1.2.\cdots.i}$ donc $p(p-1)\cdots(p-i+1) = i!\binom{p}{i}$
$\forall i \in [|1;n|]$ comme $p$ est premier alors $i \wedge p = 1$ donc $i! \wedge p = 1$
Or $p \mid i!\binom{p}{i}$ et $p \wedge i! = 1$ donc $p \mid \binom{p}{i}$ donc $\exists k \in \mathbb{N} \quad \binom{p}{i} = kp$
   - $(a+b)^p = \sum_{i=0}^{p}\binom{p}{i}a^i b^{p-i} = a^p + \sum_{i=1}^{p-1}\binom{p}{i}a^i b^{p-i} + b^p = a^p + b^p$
car, pour tout i compris entre 1 et $p-1$, $\binom{p}{i}$ est un multiple de $p$ donc $\binom{p}{i}a^i b^{p-i}$ est de la forme $px$ avec $x \in A$ donc vaut $0_A$
6. l'application $f$ de $A$ dans $A[X]$ qui à tout $a$ associe le polynôme constant $(a, 0, 0, \cdots)$ est un isomorphisme de $A$ sur $f < A >$ donc $A$ et $A[X]$ ont même élément unité donc même caractéristique.

### 1.7.3 Exemples

1. L'anneau $\{0_A\}$ est le seul anneau de caractéristique 1.
2. $\mathbb{Z}, \mathbb{Q}, \mathbb{R}$ sont des anneaux de caractéristique 0.
3. Si $n \geq 2$ alors $F_n = \mathbb{Z}/n\mathbb{Z}$ est un anneau de caractéristique $n$
4. Un anneau de Boole c'est-à-dire un anneau $(A, +, \times)$ tel que $\forall x \in A \quad x^2 = x$ est un anneau de caractéristique 2
En effet, $(x+x)(x+x) = x + x$ d'où $x^2 + x^2 + x^2 + x^2 = x + x$ donc $x + x + x + x = x + x$ . On en déduit que $x + x = 0$

# 1.8 Idéaux

## 1.8.1 Définition

Soit un anneau $(A, +, \times)$.
- On appelle $I$ **idéal à gauche** de $A$ toute partie non vide $I$ de $A$ telle que :
  1. $(I, +)$ est un sous-groupe du groupe $(A, +)$.
  2. $IA \subset I$ c'est-à-dire $\forall i \in I \quad \forall a \in A \quad ia \in I$
- On définit de même la notion d'**idéal à droite**.
- Un idéal est dit **bilatère** s'il est idéal à gauche et à droite.
- Dans un anneau commutatif, tout idéal est bilatère.

## 1.8.2 Types d'idéaux

### Idéal premier

Un idéal $I$ est **premier** si
1. $I$ est propre c'est-à-dire que $I \neq 0_A$ et $I \neq A$
2. $\forall (x, y) \in A^2 \quad xy \in I \Longrightarrow x \in I$ ou $y \in I$

### Idéal maximal

Un idéal $I$ est maximal si
1. $I$ est propre c'est-à-dire que $I \neq 0_A$ et $I \neq A$
2. $I$ n'est strictement contenu dans aucun autre idéal propre de $A$
   c'est-à-dire que $\forall J$ idéal de $A$ si $I \subset J$ alors $J = A$

### Théorème

Dans un anneau commutatif, tout idéal maximal est premier.

Soit $I$ un idéal maximal de $A$.

- $I$ est forcément propre.
- Soit un couple $(x, y) \in A^2$ tel que $xy \in I$.
  Ou bien $x \in I$. CQFD.
  Ou bien $x \notin I$. Alors $J = I + Ax$ est un idéal de $A$. Comme $I \subset J$ et que $I$ est maximal alors $J = A$.
  Par conséquent, $1_A = i + ax$ où $a \in A$ et $i \in I$ donc $y = yi + yax = yi + a(xy)$.
  Or $xy \in I$ donc $axy \in I$. Or $yi \in I$ donc $y = yi + axy \in I$. CQFD.

## 1.9 Théorème chinois

## 1.10 Produit et somme directe d'anneaux

## 1.11 Exercices

### 1.11.1 Exercice

Soit un anneau $(A, +, \times)$ pas forcément unitaire.
Démontrer que si $A$ est intègre et fini alors $A$ est un corps.

### 1.11.2 Exercice

1. Déterminer tous les sous-anneaux de l'anneau $(\mathbb{Z}, +, \times)$.
2. Déterminer tous les automorphismes du groupe $(\mathbb{Z}, +)$.
3. Déterminer tous les endomorphismes et les automorphismes de l'anneau $(\mathbb{Z}, +, \times)$.

### 1.11.3 Exercice

1. Déterminer tous les morphismes du groupe $(\mathbb{Q}, +)$.
2. Démontrer que le seul endomorphismes de groupe $(\mathbb{Q}, +)$ dans le groupe $(\mathbb{Z}, +)$.

### 1.11.4 Exercice

Soit $A$ un anneau commutatif. Démontrer que :
$A[X]$ est principal si et seulement si $A$ est un corps.

### 1.11.5 Exercice

Définir tous les sous-anneaux de $\mathbb{Q}$.

### 1.11.6 Exercice

Tout anneau $A$ sans idéal propre est un corps.

### 1.11.7 Anneau de George BOOLE

On appelle anneau de Boole tout anneau $(A, +, \times)$ unitaire tel que $\forall a \in A \quad a^2 = a$

1. En calculant $(a+b)^2$ de deux façons différentes,
   démontrer que $\forall (a,b) \in A^2 \quad ab = -ba$
2. Démontrer que que tout élément de $A$ est son propre opposé.
3. En déduire qu'un anneau de Boole est un anneau de caractéristique 2
4. Démontrer que $A$ est commutatif.
5. Démontrer que $\forall (a,b) \in A^2 \quad ab(a+b) = 0$
6. En déduire que tout élément de $A$ autre que $0_A$ et $1_A$ est un diviseur de 0 donc $A$ n'est pas intègre donc n'est pas un corps.
7. On définit la relation suivante $\mathcal{R}$ dans $A$ par $a \mathcal{R} b \iff ab = a$
   Démontrer que $\mathcal{R}$ est une relation d'ordre.
   Que peut-on dire de $0_A$ et de $1_A$ pour cette relation d'ordre ?
8. (a) Quel est le nombre maximal d'éléments de $A$ qui ne divisent pas 0 ?
   (b) Quelle propriété un élément de $A$ qui ne divise pas 0 possède-t-il ?
   (c) Montrer que si l'anneau de Boole $(A, +, \times)$ ne possède pas de diviseur de 0 , l'ensemble $A$ est constitué soit du seul élément 0, soit des deux seule éléments 0 (élément neutre pour l'addition) et1(élément neutre pour la multiplication)
9. Trouver un anneau de Boole ayant 2 éléments.
10. Montrer qu'en essayant de construire la table d'addition et de multiplication qu'il n'y a pas d'anneau de Boole à 3 ou 5 éléments mais qu'il en existe à 4 éléments.
11. (a) Démontrer que si $E$ est un ensemble non vide alors $(\mathcal{P}(E), \Delta, \cap)$ est un anneau de Boole.
    (b) Quelle est la relation d'ordre $\mathcal{R}$ ?
12. Démontrer que dans un anneau de Boole
    (a) si 2 éléments engendrent le même idéal alors ils sont égaux.
    (b) si un idéal est premier alors il est maximal.

**Corrigé**

1. Comme $A$ est un anneau de Boole alors
   - $(a+b)^2 = (a+b)(a+b) = aa + ab + ba + bb = a^2 + ab + ba + b^2 = a + ab + ba + b$
   - $(a+b)^2 = a + b$
   - Par conséquent, $a + ab + ba + b = a + b$ donc $ab + ba = 0$ donc $ab = -ba$
2. En prenant $a = b$ on a donc $aa = -aa$ donc $a^2 = -a^2$ d'où $a = -a$.
3. Par conséquent, $a + a = 0$ donc un anneau de Boole est un anneau de caractéristique 2
4. Comme $A$ est de caractéristique 2 alors $ab + ab = 0$. Or $ab = -ba$ donc $ab - ba = 0$ d'où $ab = ba$ donc $A$ est un anneau commutatif.
5. $\forall (a,b) \in A^2 \quad ab(a+b) = (ab)a + (ab)b = a(ba) + a(bb) = a(ab) + ab = (aa)b + ab = ab + ab = 0$
6. Soit $a \neq 0$ et $a \neq 1$ et $b = 1$ on a $\forall a \in A \quad a(1)(a+1) = 0$.
   Alors $a + 1 \neq 0$ car $a + 1 = 0 \iff a + 1 = 1 + 1 \iff a = 1$.

Comme $a(a+1) = 0$ avec $a \neq 0$ et $a+1 \neq 0$ alors $a$ est un diviseur de 0 donc $A$ n'est pas intègre donc n'est pas un corps.

7. On définit la relation suivante $\mathcal{R}$ dans $A$ par $a \mathcal{R} b \iff ab = a$
   - $\forall a \in A \quad aa = a$ donc $a \mathcal{R} a$. $\mathcal{R}$ est donc réflexive.
   - Soit $(a,b) \in A^2$ si $a \mathcal{R} b$ et $b \mathcal{R} a$ alors $ab = a$ et $ba = b$. or $ab = ba$ donc $a = b$ . $\mathcal{R}$ est donc antisymétrique.
   - Soit $(a,b,c) \in A^3$ si $a \mathcal{R} b$ et $b \mathcal{R} c$ alors $ab = a$ et $bc = b$.
     Donc $ac = (ab)c = a(bc) = ab = a$ donc $a \mathcal{R} c$ . $\mathcal{R}$ est donc transitive.

   $\mathcal{R}$ est donc une relation d'ordre.
   $\forall a \in A \quad 0\, a = 0$ donc $0\, \mathcal{R} a$ donc 0 est le plus petit élément.
   $\forall a \in A \quad a\, 1 = a$ donc $a\, \mathcal{R} 1$ donc 1 est le plus grand élément.

### 1.11.8 Eléments Nilpotents

Soit $(A, +, \times)$ un anneau.
On dit qu'un élément $a \in A$ est nilpotent(du latin *nihil* : rien, et *potere* : pouvoir) lorsque $\exists n \in \mathbb{N}^* \quad x^n = 0_A$.

1. Démontrer que si $A$ est unitaire d'élément unité $1_A$ et si $a$ est nilpotent alors $1 - a$ est inversible.
2. Soient $a \in A$ et $b \in A$.
   Démontrer que si $a$ est nilpotent et si $b$ est quelconque alors $ab$ est nilpotent.
3. En déduire que si $a$ est nilpotent et $b$ inversible alors $a - b$ est inversible.
4. Soient $a \in A$ et $b \in A$.
   Démontrer que si $a$ et $b$ sont nilpotents et permutables (c'est-à-dire $ab = ba$) alors
   - $a + b$ est nilpotent.
   - $a - b$ est nilpotent.

**Corrigé**

1. Comme $a$ est nilpotent alors $\exists n \in \mathbb{N}^* \quad a^n = 0$
   Par conséquent, $1 = 1 - a^n = 1^n - a^n = (1 - a)(1 + a + a^2 + \cdot + a^{n-1})$
   De même $1 = 1 - a^n = (1 + a + a^2 + \cdot + a^{n-1})(1 - a)$.
   Donc $1 - a$ est inversible dans $A$ et son inverse est $1 + a + a^2 + \cdot + a^{n-1}$.
   **Rappel : Dans un anneau si $ab = ba$ alors**

   $\forall n$ **entier** $\geq 2 \quad a^n - b^n = (a - b)(a^{n-1} + a^{n-2}b + a^{n-2}b + \cdots a^{n-2}b + + ab^{n-2} + b^{n-1})$
2. Soient $a \in A$ et $b \in A$.
   Comme $a$ est nilpotent alors $\exists n \in \mathbb{N}^* \quad a^n = 0$
   Soit $b \in A$ quelconque alors $((ab)^n = a^n b^n = 0b^n = 0$ donc $ab$ est nilpotent.
3. Comme $b$ est inversible alors $\exists c \in A \quad bc = 1$ Par conséquent, $b - a = b - 1.a = b - (bc)a - b = b - b(ca) = b(1 - ca)$.
   Comme $a$ est nilpotent , on peut en déduire d'après la question précédente que $ca$ est nilpotente. Mais alors $1 - ca$ est inversible.
   Dans un anneau le produit d'éléments inversibles est inversible, comme $b$ est inversible et $1 - ca$ est inversible alors $b - a$ est inversible.
4. Soient $a \in A$ et $b \in A$.
   - Comme $a$ est nilpotent alors $\exists n \in \mathbb{N}^* \quad a^n = 0$
     Comme $b$ est nilpotent alors $\exists m \in \mathbb{N}^* \quad b^m = 0$
     Comme $a$ et $b$ sont des éléments **commutables** de l'anneau $A$ c'est-à-dire tels que donc $ab = ba$. Alors d'après la Formule du binôme de Newton :
     $\forall n \in \mathbb{N}\ (a + b)^{n+m} = \sum_{i=0}^{n+m} \binom{n+m}{i} a^i\, b^{n+m-i}$.
     Examinons tous les termes de cette somme :
     — Pour $i = n$ alors $a^i = 0$ donc le terme correspondant de la somme s'annule.
     — Pour $i > n$ on obtient $a^i = a^n\, a^{i-n} = 0\, a^{i-n} = 0$ donc les termes correspondants de la somme s'annulent.

— Pour $i < n$ on obtient $b^{n+m-i} = 0$ car $m + n - i > m$ puisque $n > i$ donc $a^i\, b^{n+m-i} = 0$ donc les termes correspondants de la somme s'annulent.

Par conséquent $(a+b)^{n+m} = 0$ donc $a + b$ est nilpotent.

- En utilisant un raisonnement analogue en remplaçant $b$ par $(-b)$ dans la Formule du binôme de Newton, on démontre que $a - b$ est nilpotent.

### 1.11.9 Radical d'un idéal

Soit $A$ un anneau et $I$ un idéal de $A$.
On appelle Radical de $I$ que l'on note $Rad(I) = \{x \in A / \exists n \in \mathbb{N} \ x^n \in I\}$.
On dit qu'un idéal $I$ est primaire lorsque : si $xy \in I$ et $x \notin I$ alors $\exists n \in \mathbb{N} \quad y^n \in I$.
On dit qu'un idéal $I$ est premier lorsque : si $xy \in I$ alors $x \in I$ ou $y \in I$. Démontrer les résultats suivants :

1. $I \subset Rad(I)$
2. $Rad(I)$ est un idéal de $A$
3. Si $I$ et $J$ sont des idéaux de $A$ tels que $I \subset J$ alors $Rad(I) \subset Rad(J)$
4. $Rad(Rad(I)) = Rad(I)$
5. Si $I$ et $J$ sont des idéaux de $A$ alors $Rad(I \cap J) = Rad(I) \cap Rad(J) = Rad(IJ)$
6. Si $I$ est un idéal primaire alors $Rad(I)$ est premier, en supposant $A$ commutatif.
7. $\exists r \in \mathbb{N}^* \quad Rad(n\mathbb{Z}) = Rad((\prod_{i=1}^{r} p_i^{\alpha_i})\mathbb{Z}) = (\prod_{i=1}^{r} p_i)\mathbb{Z}$
8. En déduire que $Rad(3648\mathbb{Z}) = 144\mathbb{Z}$
9. Les idéaux premiers de $\mathbb{Z}$ sont les $p\mathbb{Z}$ et les idéaux primaires de $\mathbb{Z}$ sont les $p^\alpha\mathbb{Z}$ où $p$ premier.
10. $Rad(I) + Rad(J) \subset Rad(I + J)$

**Démonstrations :**

1. Soit $x \in I$ alors $x^1 = x \in I$ donc $x \in Rad(I)$.CQFD.
2. $Rad(I)$ est un idéal de $A$ car
   (a) $Rad(I) \subset A$.
   (b) $(Rad(I), +)$ est un sous-groupe de $(A, +)$ puisque
      i. $Rad(I) \neq \emptyset$ car $0 \in Rad(I)$ car comme $I$ est un idéal alors $(I, +)$ est un sous groupe de $(A, +-)$ donc $0 \in I$.
      Alors $0 = 0^1 \in I$ donc $0 \in Rad(I)$.
      ii. Soit $x \in Rad(I)$ et $y \in Rad(I)$ nous allons démontre que $x - y \in Rad(I)$
      beginitemize
      iii. Comme $x \in Rad(I)$ alors $\exists n \in \mathbb{N}^* \quad x^n \in I$
      Comme $y \in Rad(I)$ alors $\exists m \in \mathbb{N}^* \quad y^m \in I$

      Comme $x$ et $y$ sont des éléments **commutables** de l'anneau $A$ c'est-à-dire tels que donc $ab = ba$. Alors d'après la Formule du binôme de Newton :
      $\forall n \in \mathbb{N} \ (x-y)^{n+m} = \sum_{i=0}^{n+m} \binom{n+m}{i} x^i \ (-1)^{n+m-i} \ y^{n+m-i}$.
      Examinons tous les termes de cette somme :
      - Pour $i \geq n$ on obtient $a^i = a^n \ a^{i-n} \in I$ car $a^n \in I$ et $IA \subset I$ donc $x^i \ y^{n+m-i} \in I$
      - Pour $i < n$ on a $m + n - i > m$ puisque $n > i$ donc $x^i y^{n+m-i} = y^m y^{n-i} x^i \in I$ car $y^m \in I$ et $IA \subset I$ .

      Par conséquent,
      la somme d'éléments de $I$ étant un élément de $I$ alors $(x-y)^{n+m} \in I$
      donc $x - y \in Rad(I)$. CQFD.

(c) Il reste à démontrer que $Rad(I)\ A \subset Rad(I)$.
Soit $x \in Rad(I)$ donc $\exists n \in \mathbb{N}^* x^n \in I$. alors soit $a \in I$ . On a donc :
$(xa)^n = x^n\ a^n \in I$ car $x^n \in I$ et $a^n \in A$ et $IA \subset I$.
Par conséquent, $xa \in Rad(I)$. CQFD.

3. Soit $x \in Rad(I)$ donc $\exists n \in \mathbb{N}^* \quad x^n \in I$. Or $I \subset J$ donc $x^n \in J$.
Par conséquent, $x \in Rad(J)$. Ainsi si $I \subset J$ alors $Rad(I) \subset Rad(J)$.

4. • On sait que $I \subset Rad(I)$ donc d'après la question précédente, l'on a $Rad(I) \subset Rad(Rad(I))$.
   • Il reste à prouver que $Rad(Rad(I)) \subset I$ .
   Soit $x \in Rad(Rad(I))$ donc $\exists n \in \mathbb{N}^* \quad x^n \in Rad(I)$ donc $\exists p \in \mathbb{N}^* \quad (x^n)^p \in I$ donc $x^{np} \in I$ donc $x \in Rad(I)$.
   • Comme $Rad(I) \subset Rad(Rad(I))$ et alors $Rad(Rad(I)) \subset Rad(I)$ alors $Rad(I) = Rad(Rad(I))$.

5. • Démontrons d'abord que $Rad(I \cap J) = Rad(I) \cap Rad(J)$
   — $I \cap J \subset I$ donc $Rad(I \cap J) \subset Rad(I)$.
   De même, $I \cap J \subset J$ donc $Rad(I \cap J) \subset Rad(J)$.
   Par conséquent, $Rad(I \cap J) \subset Rad(I) \cap Rad(J)$
   — Soit $x \in Rad(I) \cap Rad(J)$ alors $x \in Rad(I)$ et $x \in Rad(J)$ donc $\exists n \in N^* \quad x^n \in I$ et $\exists p \in N^* \quad x^p \in J$.
   Alors $x^{np} = (x^n)^p \in I$ car $x^n \in I$.
   De même, $x^{np} = (x^p)^n \in J$ car $x^p \in J$.
   Donc $x^{np} \in I \cap J$ donc $x \in Rad(I \cap J)$.
   Par conséquent, $Rad(I \cap J) \subset Rad(I) \cap Rad(J)$.
   — Comme $Rad(I \cap J) \subset Rad(I) \cap Rad(J)$ et $Rad(I \cap J) \subset Rad(I) \cap Rad(J)$ alors $Rad(I \cap J) = Rad(I) \cap Rad(J)$
   • Démontrons maintenant que $Rad(IJ) = Rad(I \cap J)$
   — Comme $I$ est un idéal de $A$ et que $J \subset A$ alors $IJ \subset I$ donc $Rad(IJ) \subset Rad(I)$.
   De même, $J$ est un idéal de $A$ et que $I \subset A$ alors $IJ \subset J$ donc $Rad(IJ) \subset Rad(J)$.
   Par conséquent, $Rad(IJ) \subset Rad(I) \cap Rad(J)$.
   — Soit $x \in Rad(I) \cap Rad(J)$ donc $x \in Rad(I)$ et$x \in Rad(J)$.
   Par conséquent, $\exists n \in N^* \quad x^n \in I$ et $\exists p \in N^* \quad x^p \in J$.
   Alors $x^{n+p} = x^n x^p \in IJ$ car $x^n \in I$ et $x^p \in J$.
   Donc $x \in Rad(IJ)$. On a donc $Rad(I) \cap Rad(J) \subset Rad(IJ)$
   — Comme $Rad(I) \cap Rad(J) \subset Rad(IJ)$ et $Rad(IJ) \subset Rad(I) \cap Rad(J)$ alors $Rad(I) \cap Rad(J) = Rad(IJ)$
   • En conclusion $Rad(I \cap J) = Rad(I) \cap Rad(J) = Rad(IJ)$

6. Supposons que $I$ est un idéal primaire. démontrons que $Rad(I)$ est premier.
Pour cela, soit $xy \in Rad(I)$ donc $\exists n \in \mathbb{N} * \quad (xy)^n \in I$.
Par conséquent, $x^n y^n \in I$ car $(xy)^n = x^n\ y^n$ puisque $A$ est commutatif.

   • ou bien $x \in Rad(I)$. CQFD.
   • ou bien $x \notin Rad(I)$. Par conséquent, $\forall p \in \mathbb{N}^* \quad x^p \notin I$.
   Or $I$ est primaire donc comme $x^n\ y^n \in I$ et que $x^n \notin I$ alors $y^n \in I$.
   Par conséquent $y \in Rad(I)$. CQFD.

7. • Soit $n \in \mathbb{N}^*$ alors $n$ est décomposable en produit de facteurs premiers $n = p_1^{\alpha_1} p_2^{\alpha_2} \cdots p_r^{\alpha_r}$ avec $p_1, p_2, \cdots, p_r$ premiers.
   $I = n\mathbb{Z}$ est un idéal de l'anneau $\mathbb{Z}$ donc $Rad(I) = Rad(n\mathbb{Z})$ est un idéal de $\mathbb{Z}$. Par conséquent, $\exists d \in \mathbb{N} \quad Rad(n\mathbb{Z}) = d\mathbb{Z}$.
   $d\mathbb{Z}$ donc $d \in Rad(n\mathbb{Z})$ donc $\exists k \in \mathbb{N}^* \quad d^k \in n\mathbb{Z}$ donc $\exists \lambda \in \mathbb{N} \quad d^k = \lambda n = \lambda \prod_{i=1}^{r} p_i^{\alpha_i}$.

Pout tout $i$ variant de 1 à $r$, on a $p_i$ qui divise $d^k$ donc $p_i$ divise $d$ car $p_i$ premier.
Par conséquent, $d = \mu \prod_{i=1}^{r} p_i$

- Réciproquement, si $d = \mu \prod_{i=1}^{r} p_i$ alors $(\prod p_i)^{sup\ \alpha_i} \in n\mathbb{Z}$ donc $d \in Rad(n\mathbb{Z})$
- En conclusion, $Rad(n\mathbb{Z}) = Rad((\prod_{i=1}^{r} p_i^{\alpha_i})\mathbb{Z}) = (\prod_{i=1}^{r} p_i)\mathbb{Z}$.

8. Par exemple, $3648 = 2^6\ 3^6\ 19$ donc $Rad(3648\mathbb{Z})$ est un idéal de $\mathbb{Z}$ donc est de la forme $d\mathbb{Z}$.
Comme $d \in d\mathbb{Z}$ alors $d \in Rad(2^6\ 3^6\ 19\ \mathbb{Z})$ donc $\exists k \in \mathbb{Z} \quad d^k \in 2^6\ 3^6\ 19\ \mathbb{Z}$.
Par conséquent, $2^6\ 3^6\ 19$ divise $d^k$ donc 2, 3 et 19 divisent $d^k$.
Or 2 est premier donc 2 divise $d$. De même 3 divise $d$ ainsi que 19 donc leur ppcm $2 \times 3 \times 19 = 144$ divise $d$
donc $Rad(3648\mathbb{Z}) = Rad((2^6\ 3^6\ 19)\mathbb{Z}) = (2.3.19)\mathbb{Z} = 144\mathbb{Z}$

9. - Soit $I = n\mathbb{Z}$ un idéal primaire de $\mathbb{Z}$ donc $Rad(I) = Rad(n\mathbb{Z})$ est premier donc $\exists p$ premier tel que $Rad(n\mathbb{Z}) = p\mathbb{Z}$ donc $\exists \alpha \in \mathbb{N}^* \quad n = p^\alpha$
   - Réciproquement, si $\exists \alpha \in \mathbb{N}^* \quad n = p^\alpha$, soit $I = n\mathbb{Z} = p^\alpha\mathbb{Z}$.
   Soit $xy \in I$.
   ou bien $x \in I$.
   ou bien $x \notin I$ alors $x = p^k\ u$ avec $p$ qui ne divise pas $u$ donc $k < \alpha$.
   $y = p^l u'$ avec $p$ qui ne divise pas $u'$.
   $xy = p^{k+l} uu'$ avec $k + l > \alpha$ donc $l \neq 0$ donc $l \geq 1$ donc $p$ divise $y$ donc $y\alpha \in I = p^\alpha\mathbb{Z}$

   En conclusion, les idéaux premiers de $\mathbb{Z}$ sont les $p\mathbb{Z}$ et les idéaux primaires de $\mathbb{Z}$ sont les $p^\alpha\mathbb{Z}$ où $p$ premier et $\alpha \in \mathbb{N}^*$.

10. soit $x \in Rad(I) + Rad(J)$ donc $x = x_1 + x_2$ où $x_1 \in Rad(I)$ et $x_2 \in Rad(J)$.
Par conséquent $\exists n_1 \in \mathbb{N}^* \quad x^{n_1} \in I$ et $\exists n_2 \in \mathbb{N}^* \quad x^{n_2} \in J$.
Alors $(x_1 + x_2)^{n_1+n_2} = \sum_{k=0}^{n_1+n_2} \binom{n_1+n_2}{k} x_1^k x_2^{n_1+n_2-k}$
$(x_1 + x_2)^{n_1+n_2} = \sum_{k=0}^{n_1-1} \binom{n_1+n_2}{k} x_1^k x_2^{n_1+n_2-k} + \sum_{k=n_1}^{n_1+n_2} \binom{n_1+n_2}{k} x_1^k x_2^{n_1+n_2-k}$.
La première somme appartient à $J$ car $x_2^{n_2} \in J$ et $n_1 + n_2 - k > n_2$ et $J$ idéal.
La deuxième somme appartient à $I$ car $x_1^{n_1} \in I$ et $n_1 + n_2 - k > n_1$ et $I$ idéal.
Par conséquent, $(x_1 + x_2)^{n_1+n_2} \in J + I$ donc $x_1 + x_2 \in Rad(I + J)$. CQFD.

### 1.11.10 Baccalauréat C

1. (a) Soit $\phi$ l'application de $\mathbb{R}$ dans $\mathbb{R}$ définie par
$$\begin{cases} \forall x \neq 0 \quad \phi(x) = \dfrac{x^2}{2} ln(|x|) - \dfrac{x^2}{4} + \dfrac{1}{4} \\ \phi(0) = 0 \end{cases}$$
Démontrer que $\phi$ est continue et dérivable sur $\mathbb{R}$.

   (b) Déterminer la fonction dérivée $\phi'$ de $\phi$.

   (c) Construire la courbe représentative $\Gamma$ de $\phi$ dans un repère orthonormé.
On prendra pour unité 4 $cm$ ; $\dfrac{1}{e} \approx 0,37$ et $\dfrac{1}{e^2} \approx 0,14$.

2. On définit dans le corps $\mathbb{C}$ des nombres complexes une loi interne $\star$ définie par
$$\forall z = x + iy \in \mathbb{C} \quad \forall z' = x' + iy' \in \mathbb{C} \quad z \star z' = xx' + i(xy' + x'y)$$

   (a) Démontrer que $(\mathbb{C}, +, \star)$ est un anneau commutatif unitaire.

   (b) Déterminer l'ensemble $\mathbb{C}'$ des éléments de $\mathbb{C}$ inversibles pour la loi $\star$.

   (c) Démontrer que tout élément $z = x + iy \in \mathbb{C}'$ a pour inverse $\tilde{z} = \dfrac{\bar{z}}{x^2}$

   (d) Démontrer que $(\mathbb{C}', \star)$ est un groupe abélien.

   (e) Soit $G$ le sous-ensemble de $\mathbb{C}$ défini par $G = \{z \in \mathbb{C} / \exists t \in \mathbb{R} \quad z = e^t + ite^t\}$.
Démontrer que $G$ est un sous-groupe du groupe $(\mathbb{C}', \star)$

   (f) Le nombre complexe $z = x + iy$ a pour image $m(x, y)$ dans le plan $P$.
Démontrer que dans $P$, l'ensemble des points images des éléments de $G$ est une partie $\gamma$ de $\mathcal{C}$ que l'on précisera.

# Chapitre 2

# Anneaux factoriels, Anneaux principaux, Anneaux euclidiens

## 2.1 Anneaux factoriels

## 2.2 Anneaux principaux

### 2.2.1 Définition

### 2.2.2

### 2.2.3

### 2.2.4

## 2.3 Anneaux euclidiens

### 2.3.1 Théorème

1. Tout anneau euclidien est principal.
2. Par conséquent, tout anneau euclidien intègre est donc principal.
3.

# Chapitre 3

# Anneaux noetheriens

# Chapitre 4

# Anneaux Artiniens

# Chapitre 5

# Anneau $\mathbb{Z}/n\mathbb{Z}$

## 5.1 Relation de congruence modulo n

### 5.1.1 Définition

Soit $n \in \mathbb{N}$. On définit ainsi la relation de congruence modulo $n$ dans $\mathbb{Z}$ par :

$$\forall (x,y) \in \mathbb{Z}^2 \;\; x \equiv y \;[n] \iff x - y \in n\mathbb{Z}$$

### 5.1.2 Théorème

La relation de congruence est une relation d'équivalence dans $\mathbb{Z}$

**Démonstration**

1. $\equiv$ est réflexive car $\forall x \in \mathbb{Z}$ l'on a $x \equiv x \;[n]$ puisque $x - x = 0 = 0 \times n \in n\mathbb{Z}$
2. $\equiv$ est réflexive car $\forall x \in \mathbb{Z}\; \forall y \in \mathbb{Z}$ , si l'on a $x \equiv y \;[n]$ alors $x - y \in n\mathbb{Z}$ donc $x - y = nk$ où $k \in \mathbb{Z}$ donc $y - x = -(nk) = n(-k)$ avec $-k \in \mathbb{Z}$ donc $y \equiv x \;[n]$
3. $\equiv$ est transitive car $\forall x \in \mathbb{Z}\; \forall y \in \mathbb{Z}\; \forall y \in \mathbb{Z}$ , si l'on a $x \equiv y \;[n]$ et $y \equiv z \;[n]$ alors $x - y \in n\mathbb{Z}$ et $y - z \in n\mathbb{Z}$ donc $x - y = nk$ et $y - z = nk'$ où $(k,k') \in \mathbb{Z}^2$ donc $x - z = x - y + y - x = nk + nk' = n(k + k')$ avec $k + k' \in \mathbb{Z}$ donc $z \equiv x \;[n]$

### 5.1.3 Théorème

$\forall (x,y) \in \mathbb{Z}^2 \qquad x \equiv y \;[n] \iff x$ et $y$ ont même reste dans la division euclidienne par $n$

**Démonstration**

- On peut diviser euclidiennement $x$ et $y$ par $n$ donc $x = nq + r$ et $y = nq' + r'$ avec $0 \leq r < n$ et $0 \leq r' < n$
- Alors $x \equiv y \;[n] \iff x - y \in n\mathbb{Z} \iff nq + r - (nq' + r') \in n\mathbb{Z}$
  $\iff n(q - q') + (r - r') \in n\mathbb{Z} \;\; (*)$
- Or $r - r' = 0 \implies (*)$
- de même, $(*) \implies r - r' = 0$ car $(*) \implies r - r' \in n\mathbb{Z}$ et $0 \leq r - r' < n$ puisque $0 \leq r < n$ et $-n < -r' \leq 0$
- Par conséquent $x \equiv y \;[n] \iff r = r'$. CQFD.

### 5.1.4 Définition

L'ensemble des classes d'équivalence s'appelle l'ensemble des entiers modulo $n$ et se note $F_n = \mathbb{Z}/n\mathbb{Z}$

**Remarques**

1. $\mathbb{Z}/0\mathbb{Z} \simeq \mathbb{Z}$.
   En effet, $x \equiv y\ [0] \iff x - y \in 0\mathbb{Z} = \{0\} \iff x = y$
2. $\forall x \in \mathbb{Z}\ \ \mathbb{Z}/1\mathbb{Z} = \{\bar{x}\}$ n'est formé que d'une seule classe.
   En effet, $x \equiv y\ [1] \iff x - y \in 1\mathbb{Z} \iff x - y \in \mathbb{Z}$
3. $Card(\mathbb{Z}/n\mathbb{Z}) = n$ car $\mathbb{Z}/n\mathbb{Z} = \{\bar{0}, \bar{1}, \bar{2}, \cdots, \overline{n-1}\}$.
   En effet, soit $x \in \mathbb{Z}$ alors $x = nq + r$ donc $x - r \in n\mathbb{Z}$ donc $x \equiv r\ [n]$.
   Il y a autant de classes dans $\mathbb{Z}/n\mathbb{Z}$ qu'il y a de restes : $\{0; 1; 2; \cdots; n-1\}$ dans la division euclidienne par $n$.
4. $\mathbb{Z}/2\mathbb{Z} = \{\bar{0}; \bar{1}\}$ où $\bar{0}$ est l'ensemble des entiers pairs et $\bar{1}$ l'ensemble des entiers impairs
5. $\mathbb{Z}/1\mathbb{Z} = \{\bar{0}; \bar{1}; \bar{2}\}$

### 5.1.5 Théorème

$\mathbb{Z}/0\mathbb{Z}$ est identifiable à $\mathbb{Z}$ et $\forall n \in \mathbb{N}^*$ l'on a $\mathbb{Z}/n\mathbb{Z} = \{\bar{0}, \bar{1}, \bar{2}, \cdots, \overline{n-1}\}$.

## 5.2 Anneau $\mathbb{Z}/n\mathbb{Z}$

### 5.2.1 Théorème et définition

La relation de congruence modulo $n$ est compatible avec l'addition et la multiplication dans $\mathbb{Z}$ c'est-à-dire

1. $\forall (x, y, z, t) \in \mathbb{Z}^4 \qquad x \equiv y\ [n]\ et\ \ z \equiv t\ [n] \Longrightarrow x + z \equiv y + t\ [n]$
2. $\forall (x, y, z, t) \in \mathbb{Z}^4 \qquad x \equiv y\ [n]\ et\ \ z \equiv t\ [n] \Longrightarrow x \times z \equiv y \times t\ [n]$

Cette propriété permet alors de définir dans $\mathbb{Z}/n\mathbb{Z}$ une addition $\dot{+}$ et une multiplication $\dot{\times}$

1. $\forall (x, y) \in (\mathbb{Z}/n\mathbb{Z})^2 \qquad \bar{x} \dot{+} \bar{y} = \overline{x + y}$
2. $\forall (x, y) \in (\mathbb{Z}/n\mathbb{Z})^2 \qquad \bar{x} \dot{\times} \bar{y} = \overline{x \times y}$

**Démonstration**

1. Si $x \equiv y\ [n]\ et\ \ z \equiv t\ [n]$ alors $x - y \in n\mathbb{Z}$ et $z - t \in n\mathbb{Z}$ donc $\exists (q, q') \in \mathbb{Z}^2$ tel que $x - y = nq$ et $z - t = nq'$ donc $(x + z) - (y + t) = nq + nq' = n(q + q') = nq''$ où $q'' = (q + q') \in \mathbb{Z}$ donc $(x + z) - (y + t) \in n\mathbb{Z}$ donc $x + z \equiv y + t\ [n]$

2. Si $x \equiv y\ [n]\ et\ \ z \equiv t\ [n]$ alors $x - y \in n\mathbb{Z}$ et $z - t \in n\mathbb{Z}$ donc $\exists (q, q') \in \mathbb{Z}^2$ tel que $x - y = nq$ et $z - t = nq'$ donc $(xz) - (yt) = (x-y)z + y(z-t) = nqz + ynq' = n(qz + q'y) = nq''$ où $q'' = (qz + q'y) \in \mathbb{Z}$ donc $(xz) - (yt) \in n\mathbb{Z}$ donc $xz \equiv yt\ [n]$

### 5.2.2 Théorème

> $(\mathbb{Z}/n\mathbb{Z}, \dot{+}, \dot{\times})$ est un anneau commutatif unitaire.
> L'élément neutre pour $\dot{+}$ et $\bar{0}$.
> L'élément neutre pour $\dot{\times}$ est $\bar{1}$.

**Démonstration**

Les propriétés des lois $\dot{+}$ et $\dot{\times}$ proviennent des propriétés des lois $+$ et $\times$ dans $\mathbb{Z}$. On dit alors que les lois $\dot{+}$ et $\dot{\times}$ sont définies par passage au quotient.

$\mathbb{Z}/2\mathbb{Z}$

| $\dot{+}$ | $\bar{0}$ | $\bar{1}$ |
|---|---|---|
| $\bar{0}$ | $\bar{0}$ | $\bar{1}$ |
| $\bar{1}$ | $\bar{1}$ | $\bar{0}$ |

| $\dot{\times}$ | $\bar{0}$ | $\bar{1}$ |
|---|---|---|
| $\bar{0}$ | $\bar{0}$ | $\bar{0}$ |
| $\bar{1}$ | $\bar{0}$ | $\bar{1}$ |

- $(\mathbb{Z}/2\mathbb{Z}, \dot{+}, \dot{\times})$ est un anneau commutatif unitaire.
- De plus, tout élément $\neq \bar{0}$ est inversible : en effet $\bar{1}$ a pour inverse lui-même.
- Donc $(\mathbb{Z}/2\mathbb{Z}, \dot{+}, \dot{\times})$ est un corps commutatif

$\mathbb{Z}/3\mathbb{Z}$

| $\dot{+}$ | $\bar{0}$ | $\bar{1}$ | $\bar{2}$ |
|---|---|---|---|
| $\bar{0}$ | $\bar{0}$ | $\bar{1}$ | $\bar{2}$ |
| $\bar{1}$ | $\bar{1}$ | $\bar{2}$ | $\bar{0}$ |
| $\bar{2}$ | $\bar{2}$ | $\bar{0}$ | $\bar{1}$ |

| $\dot{\times}$ | $\bar{0}$ | $\bar{1}$ | $\bar{2}$ |
|---|---|---|---|
| $\bar{0}$ | $\bar{0}$ | $\bar{0}$ | $\bar{0}$ |
| $\bar{1}$ | $\bar{0}$ | $\bar{1}$ | $\bar{2}$ |
| $\bar{2}$ | $\bar{0}$ | $\bar{2}$ | $\bar{1}$ |

- $(\mathbb{Z}/3\mathbb{Z}, \dot{+}, \dot{\times})$ est un anneau commutatif unitaire.
- De plus, tout élément $\neq \bar{0}$ est inversible : en effet $\bar{1}$ a pour inverse lui-même ainsi que $\bar{2}$.
- Donc $(\mathbb{Z}/3\mathbb{Z}, \dot{+}, \dot{\times})$ est un corps commutatif

$\mathbb{Z}/4\mathbb{Z}$

| $\dot{+}$ | $\bar{0}$ | $\bar{1}$ | $\bar{2}$ | $\bar{3}$ |
|---|---|---|---|---|
| $\bar{0}$ | $\bar{0}$ | $\bar{1}$ | $\bar{2}$ | $\bar{3}$ |
| $\bar{1}$ | $\bar{1}$ | $\bar{2}$ | $\bar{3}$ | $\bar{0}$ |
| $\bar{2}$ | $\bar{2}$ | $\bar{3}$ | $\bar{0}$ | $\bar{1}$ |
| $\bar{3}$ | $\bar{3}$ | $\bar{0}$ | $\bar{1}$ | $\bar{2}$ |

| $\dot{\times}$ | $\bar{0}$ | $\bar{1}$ | $\bar{2}$ | $\bar{3}$ |
|---|---|---|---|---|
| $\bar{0}$ | $\bar{0}$ | $\bar{0}$ | $\bar{0}$ | $\bar{0}$ |
| $\bar{1}$ | $\bar{0}$ | $\bar{1}$ | $\bar{2}$ | $\bar{3}$ |
| $\bar{2}$ | $\bar{0}$ | $\bar{2}$ | $\bar{0}$ | $\bar{2}$ |
| $\bar{3}$ | $\bar{0}$ | $\bar{3}$ | $\bar{2}$ | $\bar{1}$ |

- $(\mathbb{Z}/4\mathbb{Z}, \dot{+}, \dot{\times})$ est un anneau commutatif unitaire.
- Mais $\bar{2}\dot{\times}\bar{2} = \bar{0}$ et $\bar{2} \neq \bar{0}$ donc $\bar{2}$ est un diviseur de $\bar{0}$.
- Par conséquent, $(\mathbb{Z}/4\mathbb{Z}, \dot{+}, \dot{\times})$ n'est pas intègre donc ne peut être un corps.

### 5.2.3 Théorème

> Soit $n \geq 2$.
> Dans $(\mathbb{Z}/n\mathbb{Z}, \dot{+}, \dot{\times})$ les seuls éléments inversibles sont les classes $\bar{x}$ telles que $x \wedge n = 1$

**Démonstration**

$\bar{x}$ est inversible $\iff \exists \bar{x'} \in \mathbb{Z}/n\mathbb{Z} \quad \bar{x}\dot{\times}\bar{x'} = \bar{1} \iff \exists x' \in \mathbb{Z} \quad xx' \equiv 1[n]$
$\iff \exists (x', k) \in \mathbb{Z}^2 \quad xx' = nk+1 \iff \exists (x', k) \in \mathbb{Z}^2 \quad xx' - nk = 1 \iff$ x et n sont premiers entre eux d'après le théorème de Bachet-Bezout.

### 5.2.4 Corollaire

> $(\mathbb{Z}/n\mathbb{Z}, \dot{+}, \dot{\times})$ est un corps commutatif $\iff$ $n$ est premier.

**Démonstration**

$\Longrightarrow$:
Supposons que $(\mathbb{Z}/n\mathbb{Z}, \dot{+}, \dot{\times})$ soit un corps commutatif donc forcément $n \geq 2$. L'élément nul de $\mathbb{Z}/n\mathbb{Z}$ est $\bar{0}$ et son élément unité est $\bar{1}$.
On a donc $\mathbb{Z}/n\mathbb{Z} = \{\bar{0}, \bar{1}, \bar{2}, \cdots, \overline{n-1}\}$.
Or dans un corps, les éléments non nuls sont inversibles donc d'après le théorème précédent $1, 2, \cdots n-1$ sont premiers avec $n$.
Par conséquent, les seuls diviseurs relatifs de $n$ sont $-n, -1, 1, n$ donc $n$ est premier.
$\Longleftarrow$:
Réciproquement si nous supposons que $n$ est premier donc $n$ ne divise pas $1, 2, \cdots, n-1$ donc $1, 2, \cdots n-1$ sont premiers avec $n$.
D'après le théorème précédent, on a donc $\bar{1}, \bar{2}, \cdots, \overline{n-1}$ qui sont inversibles dans l'anneau commutatif $(\mathbb{Z}/n\mathbb{Z}, \dot{+}, \dot{\times})$ .
Par conséquent cet anneau commutatif devient un corps commutatif.

## 5.3 Propriétés de la congruence

### 5.3.1

$\forall n \in \mathbb{N}$ l'on a : $x \equiv y\ [n] \iff x - y \in n\mathbb{Z}$.

### 5.3.2

$\forall n \in \mathbb{N}$ l'on a : $x \equiv y\ [n] \iff$ $x$ et $y$ ont le même reste dans la division euclidienne par $n$.

### 5.3.3

La relation de congruence $\equiv$ est une relation d'équivalence
c'est-à-dire

$$\begin{cases} x \equiv x\ [n] \\ x \equiv y\ [n] \Longrightarrow y \equiv x\ [n] \\ (x \equiv y\ [n] \text{ et } y \equiv z\ [n]) \Longrightarrow x \equiv z\ [n] \end{cases}$$

### 5.3.4

Pour tous entiers relatifs $x, y, z, t$, pour tous entiers naturels $n$ et $k$
$(x \equiv y\ [n] \text{ et } z \equiv t\ [n]) \Longrightarrow x + z \equiv y + t\ [n]$
$(x \equiv y\ [n] \text{ et } z \equiv t\ [n]) \Longrightarrow xz \equiv yt\ [n]$
$x \equiv y\ [n] \Longrightarrow x^k \equiv y^k\ [n]$

### 5.3.5

$\forall n \in \mathbb{N}\ \forall (x, y, k) \in \mathbb{Z}^3 \qquad x \equiv y\ [n] \Longrightarrow kx \equiv ky\ [n]$
**Attention ! La réciproque est fausse :** $2 \times 3 \equiv 2 \times 6\ [6]$ et pourtant $3 \not\equiv 6\ [6]$

### 5.3.6

$\forall n \in \mathbb{N} \qquad \forall (x, y) \in \mathbb{Z}^2\ \ \forall d \in \mathbb{Z}^* \qquad x \equiv y\ [n] \iff xd \equiv yd\ [nd]$

**Démonstration**

$xd \equiv yd\ [nd] \iff xd - yd \in nd\mathbb{Z} \iff \exists q \in \mathbb{Z} \qquad xd - yd = ndq$
$\iff \exists q \in \mathbb{Z} \qquad d(x - y) = dnq \iff \exists q \in \mathbb{Z} \qquad x - y = nq \iff x \equiv y\ [n]$

### 5.3.7 Corollaire

Si $n_1 \wedge n_2 = 1$ et $a \equiv b\ [n_1]$ et $a \equiv b\ [n_2]$ alors $a \equiv b\ [n_1 n_2]$

**Démonstration**

Supposons que $a \equiv b\ [n_1]$ et $a \equiv b\ [n_2]$
alors $\exists (q, q') \in Z^2$ tel que $a = n_1 q + b = n_2 q + b$.
Donc $n_1 q = n_2 q'$ d'où $n_2 \mid (n_1 q)$. Mais $n_1 \wedge n_2 = 1$ alors d'après Gauss on a $n_2 \mid q$.
Par conséquent, $\exists k \in \mathbb{Z}$ tel que $q = n_2 k$ donc $a = n_1 q + b = n_1 n_2 k + b$ d'où $a \equiv b\ [n_1 n_2]$.CQFD.

## 5.4 Applications

### 5.4.1 Restes de division euclidienne

> Déterminer le reste de la division euclidienne de $19^{52}$ par 7

On sait que $19 \equiv 5\ [7]$ car $19 = 7 \times 2 + 5$ donc $19^{52} \equiv 5^{52}\ [7]$.
Il reste donc à déterminer le reste de la division euclidienne de $19^{52}$ par 7
Or

- $$\begin{cases} 5^0 \equiv 1\ [7] \\ 5^1 \equiv 5\ [7] \\ 5^2 \equiv 4\ [7] \\ 5^3 \equiv 6\ [7] \\ 5^4 \equiv 2\ [7] \\ 5^5 \equiv 3\ [7] \\ 5^6 \equiv 1\ [7] \end{cases}$$

- Soit un rang $n \in \mathbb{N}$ supposons que

$$\begin{cases} 5^{6n} \equiv 1\ [7] \\ 5^{6n+1} \equiv 5\ [7] \\ 5^{6n+2} \equiv 4\ [7] \\ 5^{6n+3} \equiv 6\ [7] \\ 5^{6n+4} \equiv 2\ [7] \\ 5^{6n+5} \equiv 3\ [7] \end{cases}$$

alors

$$\begin{cases} 5^{6(n+1)} = 5^{6n}5^6 \equiv 1 \times 1 = 1\ [7] \\ 5^{6(n+1)+1} = 5^{6(n+1)}5^1 \equiv 5\ [7] \\ 5^{6(n+1)+2} = 5^{6(n+1)}5^2 \equiv 4\ [7] \\ 5^{6(n+1)+3} = 5^{6(n+1)}5^3 \equiv 6\ [7] \\ 5^{6(n+1)+4} = 5^{6(n+1)}5^4 \equiv 2\ [7] \\ 5^{6(n+1)+5} = 5^{6(n+1)}5^5 \equiv 3\ [7] \end{cases}$$

- On a donc démontré par récurrence que

$$\begin{cases} 5^{6n} \equiv 1\ [7] \\ 5^{6n+1} \equiv 5\ [7] \\ 5^{6n+2} \equiv 4\ [7] \\ 5^{6n+3} \equiv 6\ [7] \\ 5^{6n+4} \equiv 2\ [7] \\ 5^{6n+5} \equiv 3\ [7] \end{cases}$$

Or $52 = 6 \times 8 + 4$ donc $5^{52} = 5^{6\times 8+4} \equiv 2\ [7]$ donc $19^{52} \equiv 2\ [7]$

### 5.4.2 Caractères de divisibilité par $2, 3, 4, 5, 8, 9, 11, 25, 125$

Soit $a = \overline{x_n x_{n-1} \cdots x_1 x_0}^{10} = x_n 10^n + x_{n-1} 10^{n-1} + \cdots + 10x_1 + x_0$

1. Comme
$$\begin{cases} 10 \equiv 0 \ [2 \ ou \ 5] \\ 100 \equiv 0 \ [4 \ ou \ 25] \\ 1000 \equiv 0 \ [8 \ ou \ 125] \end{cases}$$
alors
   (a) $a$ est divisible par 2 $\iff$ $x_0 \in \{0, 2, 4, 6, 8\}$ $\iff$ $x_0$ est divisible par 2
   (b) $a$ est divisible par 5 $\iff$ $x_0 \in \{0, 5\}$
   (c) $a$ est divisible par 4 $\iff$ $\overline{x_1 x_0}$ est divisible par 4
   (d) $a$ est divisible par 25 $\iff$ $\overline{x_1 x_0}$ est divisible par 25
   (e) $a$ est divisible par 8 $\iff$ $\overline{x_2 x_1 x_0}$ est divisible par 8
   (f) $a$ est divisible par 125 $\iff$ $\overline{x_2 x_1 x_0}$ est divisible par 125
2. Comme $10 \equiv 1 \ [3 \ ou 9]$
alors
   (a) $a$ est divisible par 3 $\iff$ la somme $\sum_{k=0}^{n} x_k$ est divisible par 3.
   (b) $a$ est divisible par 9 $\iff$ la somme $\sum_{k=0}^{n} x_k$ est divisible par 9.
3. Comme $\forall k \in \mathbb{N} \ 10^k \equiv (-1)^k \ [11]$
alors
$a$ est divisible par 11 $\iff$ la somme des chiffres de rang pair est congrue à la somme des chiffres de rang impair.

### 5.4.3 Théorème des restes chinois

Selon Wikipedia : La forme originale du théorème, contenue dans un livre du mathématicien chinois **Qin Jiushao** publié en 1247, est un résultat concernant les systèmes de congruences. Mais on trouve trace d'un problème analogue dans le livre du mathématicien et astronome chinois **Sun Zi**, le Sunzi suanjing datant du $3^{me}$ siècle :
*Combien l'armée de Han Xing comporte-t-elle de soldats si, rangés par 3 colonnes, il reste deux soldats, rangés par 5 colonnes, il reste trois soldats et, rangés par 7 colonnes, il reste deux soldats ?*
On peut penser que les Chinois, férus de calculs astronomiques, puissent être intéressés par des concordances de calendrier et qu'ils aient été amenés très tôt à s'intéresser à des questions du type :
*Dans combien de jours la pleine lune tombera-t-elle au solstice d'hiver ?*
Si la question se pose alors qu'il reste 6 jours avant le solstice d'hiver et 3 jours avant la pleine lune, la question se traduit par :
*Existe-t-il un entier x tel que le reste de la division de x par 365 donne 6 et le reste de la division de x par 28 donne 3 ?*
La résolution proposée par Sun Zi pour le problème des soldats est la suivante :
Multiplie le reste de la division par 3, c'est-à-dire 2, par 70, ajoute lui le produit du reste de la division par 5, c'est-à-dire 3, avec 21 puis ajoute le produit du reste de la division par 7, c'est-à-dire 2 par 15. Tant que le nombre est plus grand que 105, retire 105.
Mais la solution n'explique qu'imparfaitement la méthode utilisée.

En fait $x \in \mathcal{S} \iff \begin{cases} x \equiv 2[mod\ 3] \\ x \equiv 3[mod\ 5] \\ x \equiv 2[mod\ 7] \end{cases}$ Or $3 \times 5 \times 7 = 105$ donc si $x \in \mathcal{S}$ alors $x + 105 \in \mathcal{S}$.

Cherchons donc une solution $x \in ]|0; 105|[$ :

$\begin{cases} x = 2, 5, 8, 11, 13, 17, 20, 23, 26, \cdots \text{ sont } \equiv 2[mod\ 3] \\ x = 3, 8, 13, 18, 23, 28, \cdots \text{ sont } \equiv 3[mod\ 5] \\ x = 2, 9, 16, 23, 30, \cdots \text{ sont } \equiv 2[mod\ 7] \end{cases}$ donc $23 \in \mathcal{S}$ d'où $\{23 + 105k \ / \ k \in \mathbb{Z}\}$

**Enoncé classique :**

Soient $n_1, n_2, \cdots, n_k$ des entiers deux à deux premiers entre eux (ce qui veut dire $pgcd(n_i, n_j) = 1$ lorsque $i \neq j$).

Alors pour tous entiers $a_1, a_2, \cdots, a_k$ il existe un entier $x$ unique modulo $n = \prod_{i=1}^{k} n_i$ tel que

$\begin{cases} x \equiv a_1[mod\ n_1] \\ x \equiv a_2[mod\ n_2] \\ \vdots \\ x \equiv a_k[mod\ n_k] \end{cases}$ Une solution $x$ peut être trouvée comme suit :

Pour tout $i$ , $n_i$ et $\widetilde{n}_i = \dfrac{n}{n_i} = n_1 n_2 \cdots n_{i-1} n_{i+1} \cdots n_k$ sont premiers entre eux.

Alors d'après le théorème de Bachet-Bezout, il existe au moins un couple d'entiers relatifs $(u_i; v_i)$ tel que $u_i n_i + v_i \widetilde{n}_i = 1$.

Alors $v_i$ est l'inverse de $\widetilde{n}_i$ modulo $n_i$. En posant $e_i = v_i \widetilde{n}_i$ on obtient donc :

$\begin{cases} e_i \equiv 1[mod\ n_i] \\ e_i \equiv 0[mod\ n_j] \end{cases}$ pour $i \neq j$ Une solution particulière est $x = \sum_{i=1}^{k} a_i e_i$

et les autres solutions sont les entiers congrus à ce $x$ modulo le produit $n = \prod_{i=1}^{k} n_i$

**Retour sur l'exemple**

$p = 3; q = 5; r = 7$ donc $n = pqr = 105$ et $p' = \frac{n}{p} = 35; q' = \frac{n}{q} = 21; r' = \frac{n}{r} = 15$
L'inverse de $p = 35$ modulo 3 est $u = 2$ car $2 \times 35 = 70 \equiv 1\ [mod\ 3]$
L'inverse de $q = 21$ modulo 5 est $v = 1$ car $1 \times 21 = 21 \equiv 1\ [mod\ 5]$
L'inverse de $r = 15$ modulo 7 est $w = 1$ car $1 \times 15 = 15 \equiv 1\ [mod\ 7]$
Alors $x = ua_1p + va_2q + wa_3r = 2 \times 2 \times 35 + 1 \times 3 \times 21 + 1 \times 2 \times 15 = 140 + 63 + 30 = 233 = 2 \times 105 + 23 \equiv 23\ [mod\ 105]$

**Autre Exemple**

Enfin, il serait dommage de ne pas présenter ce problème concernant des pirates et un trésor, très fréquemment cité pour illustrer le théorème des restes chinois :

*Une bande de 17 pirates possède un trésor constitué de pièces d'or d'égale valeur. Ils projettent de se les partager également, et de donner le reste au cuisinier chinois. Celui-ci recevrait alors 3 pièces. Mais les pirates se querellent, et six d'entre eux sont tués. Un nouveau partage donnerait au cuisinier 4 pièces. Dans un naufrage ultérieur, seuls le trésor, six pirates et le cuisinier sont sauvés, et le partage donnerait alors 5 pièces d'or à ce dernier. Quelle est la fortune minimale que peut espérer le cuisinier s'il décide d'empoisonner le reste des pirates ?*
L'arithmétique modulaire a rendu ce type de problème plus facile à résoudre.
Il s'agit de trouver $x$ positif et minimal vérifiant le système

$$\begin{cases} x \equiv 3\ [17] \\ x \equiv 4\ [11] \\ x \equiv 5\ [6] \end{cases}$$

D'après le théorème des restes chinois (puisque 17, 11 et 6 sont premiers entre eux deux à deux), les solutions sont de la forme :
$x = u_1 \times 11 \times 6 \times 3 + u_2 \times 17 \times 6 \times 4 + u_3 \times 17 \times 11 \times 5 + n \times 17 \times 11 \times 6$
ou encore $x = 198u_1 + 408u_2 + 935u_3 + 1122n$.
Il reste à trouver les $u_i$ :
On a par division euclidienne : $\begin{cases} 66 = 3 \times 17 + 15 \\ 17 = 1 \times 15 + 2 \\ 15 = 7 \times 2 + 1 \end{cases}$
On en déduit que $1 = 15 - 7 \times 2$ et puisque $2 = 17 - 1 \times 15$, on a $1 = 15 - 7(17 - 1 \times 15)$ c'est-à-dire $1 = 8 \times 15 - 7 \times 17$.
Mais $15 = 66 - 3 \times 17$ d'où $1 = 8(66 - 3 \times 17) - 7 \times 17$.

On obtient pour finir $1 = 8 \times 66 - 31 \times 17$ et $u_1 = 8$. De la même manière, on trouve $u_2 = 4$ et $u_3 = 1$.
Donc $x = 198 \times 8 + 408 \times 4 + 935 + 1122n = 4151 + 1122n$. 4151 est donc une solution possible pour notre cuisinier, mais ce n'est pas la plus petite.
Il suffit d'effectuer la division de 4151 par 1122 pour trouver comme reste 785 qui est le nombre minimal de pièces que peut obtenir le cuisinier.

**Enoncé abstrait dans $\mathbb{Z}/n\mathbb{Z}$**

> Si $m \in \mathbb{N}$ *et* $n \in \mathbb{N}$ sont tels que $pgcd(m,n) = 1$
> alors $\mathbb{Z}/mn\mathbb{Z} \approx \mathbb{Z}/m\mathbb{Z} \times \mathbb{Z}/n\mathbb{Z}$

**Démonstration :**
Soit l'application

$$\phi : (\mathbb{Z}, +) \mapsto (\mathbb{Z}/m\mathbb{Z} \times \mathbb{Z}/n\mathbb{Z}, +)$$
$$x \mapsto (\dot{x}, \bar{x})$$

1. $\phi$ est un homorphisme de groupes.
2. $ker(\phi) = \{x/\phi(x) = (\dot{0}, \bar{0})\} = \{x/(\dot{x}, \bar{x}) = (\dot{0}, \bar{0})\} = \{x/\dot{x} = \dot{0}\ et\ \bar{x} = \bar{0}\}$
   donc $ker(\phi) = \{x/x \equiv 0[m]\ et\ x \equiv 0[n]\} = \{x/m|x \text{ et } n|x\}$.
   Par conséquent $ker(\phi)$ est le sous groupe de $\mathbb{Z}$ formé des multiples de $m$ et de $n$ . Donc $ker(\phi) = (ppcm(m,n)) = (mn) = mn\mathbb{Z}$ car $pgcd(m,n) = 1$
3. On en déduit que :
   Il existe un homomorphisme injectif $\psi : \mathbb{Z}/mn\mathbb{Z} \mapsto \mathbb{Z}/m\mathbb{Z} \times \mathbb{Z}/n\mathbb{Z}$.
   Or $card(mn\mathbb{Z}) = mn = card(\mathbb{Z}/m\mathbb{Z} \times \mathbb{Z}/n\mathbb{Z})$ donc $\psi$ devient bijectif donc un isomorphisme . Par conséquent $\mathbb{Z}/mn\mathbb{Z} \equiv \mathbb{Z}/m\mathbb{Z} \times \mathbb{Z}/n\mathbb{Z}$

## 5.5 Sous-anneaux de $\mathbb{Z}/n\mathbb{Z}$

### 5.5.1 Sous-groupes additifs de $\mathbb{Z}/n\mathbb{Z}$

Les sous-groupes additifs de $\mathbb{Z}/n\mathbb{Z}$ sont cycliques

### 5.5.2 Sous -anneaux de $\mathbb{Z}/n\mathbb{Z}$

L'ensemble des sous -anneaux de $\mathbb{Z}/n\mathbb{Z}$ est l'ensemble des sous-groupes de $\mathbb{Z}/n\mathbb{Z}$

**Eléments unités des sous anneaux de $\mathbb{Z}/n\mathbb{Z}$**

Attention ! Certains de ces sous-anneaux n'ont pas le même élément unité que $\mathbb{Z}/n\mathbb{Z}$.
Par exemple, dans l'anneau $\mathbb{Z}/6\mathbb{Z} = \{\bar{0}\,;\,\bar{1}\,;\,\bar{2}\,;\,\bar{3}\,;\,\bar{4}\,;\,\bar{5}\}$ l'élément unité est $\bar{1}$.
Le groupe $\mathbb{Z}/6\mathbb{Z}$ est un groupe cyclique d'ordre 6.

| $\dot{+}$ | $\bar{0}$ | $\bar{1}$ | $\bar{2}$ | $\bar{3}$ | $\bar{4}$ | $\bar{5}$ |
|---|---|---|---|---|---|---|
| $\bar{0}$ | $\bar{0}$ | $\bar{1}$ | $\bar{2}$ | $\bar{3}$ | $\bar{4}$ | $\bar{5}$ |
| $\bar{1}$ | $\bar{1}$ | $\bar{2}$ | $\bar{3}$ | $\bar{4}$ | $\bar{5}$ | $\bar{0}$ |
| $\bar{2}$ | $\bar{2}$ | $\bar{3}$ | $\bar{4}$ | $\bar{5}$ | $\bar{0}$ | $\bar{1}$ |
| $\bar{3}$ | $\bar{3}$ | $\bar{4}$ | $\bar{5}$ | $\bar{0}$ | $\bar{1}$ | $\bar{2}$ |
| $\bar{4}$ | $\bar{4}$ | $\bar{5}$ | $\bar{0}$ | $\bar{1}$ | $\bar{2}$ | $\bar{3}$ |
| $\bar{5}$ | $\bar{5}$ | $\bar{0}$ | $\bar{1}$ | $\bar{2}$ | $\bar{3}$ | $\bar{4}$ |

| $\dot{\times}$ | $\bar{0}$ | $\bar{1}$ | $\bar{2}$ | $\bar{3}$ | $\bar{4}$ | $\bar{5}$ |
|---|---|---|---|---|---|---|
| $\bar{0}$ | $\bar{0}$ | $\bar{0}$ | $\bar{0}$ | $\bar{0}$ | $\bar{0}$ | $\bar{0}$ |
| $\bar{1}$ | $\bar{0}$ | $\bar{1}$ | $\bar{2}$ | $\bar{3}$ | $\bar{4}$ | $\bar{5}$ |
| $\bar{2}$ | $\bar{0}$ | $\bar{2}$ | $\bar{4}$ | $\bar{0}$ | $\bar{2}$ | $\bar{4}$ |
| $\bar{3}$ | $\bar{0}$ | $\bar{3}$ | $\bar{0}$ | $\bar{3}$ | $\bar{0}$ | $\bar{3}$ |
| $\bar{4}$ | $\bar{0}$ | $\bar{4}$ | $\bar{2}$ | $\bar{0}$ | $\bar{4}$ | $\bar{2}$ |
| $\bar{5}$ | $\bar{0}$ | $\bar{5}$ | $\bar{4}$ | $\bar{3}$ | $\bar{2}$ | $\bar{1}$ |

Il admet que deux sous-groupes propres $H = \{\bar{0}\,;\,\bar{2}\,;\,\bar{4}\}$ et $K = \{\bar{0}\,;\,\bar{3}\}$
$H$ et $K$ sont stables pour la multiplication donc sont des sous-anneaux :
Le sous-anneau $H = \{\bar{0}\,;\,\bar{2}\,;\,\bar{4}\}$ a pour élément unité $\bar{4}$

| $\dot{\times}$ | $\bar{0}$ | $\bar{2}$ | $\bar{4}$ |
|---|---|---|---|
| $\bar{0}$ | $\bar{0}$ | $\bar{0}$ | $\bar{0}$ |
| $\bar{2}$ | $\bar{0}$ | $\bar{4}$ | $\bar{2}$ |
| $\bar{4}$ | $\bar{0}$ | $\bar{2}$ | $\bar{4}$ |

Le sous-anneau $K = \{\bar{0}\,;\,\bar{3}\}$ a pour élément unité $\bar{3}$

| $\dot{\times}$ | $\bar{0}$ | $\bar{3}$ |
|---|---|---|
| $\bar{0}$ | $\bar{0}$ | $\bar{0}$ |
| $\bar{3}$ | $\bar{0}$ | $\bar{3}$ |

## 5.6 Exercices

### 5.6.1 Exercice

Soit $(a,b) \in \mathbb{Z}^2$.

1. Développer $(a+b)^7$.
2. En déduire que $(a+b)^7 \equiv a^7 + b^7\ [7]$
   et que $(a+b)$ est un multiple de 7 $\iff$ $a^7+b^7$ est un multiple de 7
3. Déterminer tous les $x \in \mathbb{Z}$ tels que

$$\begin{cases} -10 \leq x \leq 10 \\ x^7 + 128 \text{ est un multiple de } 7 \end{cases}$$

**Corrigé**

1. $(a+b)^7 = \sum_{k=0}^{7} \binom{7}{k} a^{n-k}b^k = a^7 + 7a^6b + 21a^5b^2 + 35a^4b^3 + 35a^3b^4 + 21a^2b^5 + 7ab^6 + b^7$

2. (a) $(a+b)^7 = a^7 + b^7 + 7(a^6b + 3a^5b^2 + 5a^4b^3 + 5a^3b^4 + 3a^2b^5 + ab^6) = a^7 + b^7 + 7q$ où $q \in \mathbb{Z}$
   d'où on déduit que $(a+b)^7 \equiv a^7 + b^7\ [7]$

   (b) $(a+b)$ est un multiple de 7 $\iff$ $(a+b) \equiv 0\ [7]$ $\iff$ $(a+b)^7 \equiv 0\ [7]$

      i. $\Longrightarrow$ est évident

      ii. $\Longleftarrow$ l'est moins. On le prouve en raisonnant par l'absurde :
      si $(a+b)^7 \equiv 0\ [7]$ alors on ne peut avoir respectivement
      $a+b \equiv 1\ [7]$ ou $a+b \equiv 2\ [7]$
      ou $a+b \equiv 3\ [7]$ ou $a+b \equiv 4\ [7]$
      ou $a+b \equiv 5\ [7]$ ou $a+b \equiv 6\ [7]$
      car alors on aurait respectivement :
      $(a+b)^7 \equiv 1^7 \not\equiv 0\ [7]$ ou $(a+b)^7 \equiv 2^7 \not\equiv 0\ [7]$
      ou $(a+b)^7 \equiv 3^7 \not\equiv 0[7]$ ou $(a+b)^7 \equiv 4^7 \not\equiv 0\ [7]$
      ou $(a+b)^7 \equiv 5^7 \not\equiv 0\ [7]$ ou $(a+b)^7 \equiv 6^7 \not\equiv 0\ [7]$

   Comme $(a+b)^7 \equiv a^7 + b^7\ [7]$ alors $(a+b)$ est un multiple de 7 $\iff$ $(a+b) \equiv 0\ [7]$ $\iff$ $(a+b)^7 \equiv 0\ [7]$ $\iff$ $a^7 + b^7 \equiv 0\ [7]$

3. $$\begin{cases} -10 \leq x \leq 10 \\ x^7 + 128 \text{ est un multiple de } 7 \end{cases}$$

   $\iff$

   $$\begin{cases} -10 \leq x \leq 10 \\ x^7 + 2^7 \equiv 0\ [7] \end{cases}$$

   $\iff$

   $$\begin{cases} -10 \leq x \leq 10 \\ x + 2 \equiv 0\ [7] \end{cases}$$

$\iff x = -9$ *ou* $x = -2$ *ou* $x = 5$
d'après le tableau suivant

| $x$ | $x+2$ | | $x$ | $x+2$ | | $x$ | $x+2$ | | $x$ | $x+2$ | | $x$ | $x+2$ |
|---|---|---|---|---|---|---|---|---|---|---|---|---|---|
| $-10$ | $-8$ | | $-5$ | $-3$ | | 0 | 2 | | 5 | 7 | | 10 | 12 |
| $-9$ | $-7$ | | $-4$ | $-2$ | | 1 | 3 | | 6 | 8 | | | |
| $-8$ | $-6$ | | $-3$ | $-1$ | | 2 | 4 | | 7 | 9 | | | |
| $-7$ | $-5$ | | $-2$ | 0 | | 3 | 5 | | 8 | 10 | | | |
| $-6$ | $-4$ | | $-1$ | 1 | | 4 | 6 | | 9 | 11 | | | |

### 5.6.2 Théorème de Wilson

Soit $p$ un entier $\geq 2$.

1. Démontrer que si $p$ est premier alors $(p-1)! + 1 \equiv 0\ [mod\ p]$ en calculant le produit des éléments de $\mathbb{Z}/p\mathbb{Z}$
2. Réciproquement démontrer que si $(p-1)! + 1 \equiv 0\ \ [mod\ p]$ alors $p$ est premier

### 5.6.3 Théorème de Fermat

Soient $p$ et $n$ des entiers naturels tels que $p$ est premier et que $pgcd(n,p) = 1$

1. Démontrer que les classes $\overline{n}, \overline{2n}, \overline{3n}, \cdots, \overline{(p-1)n}$ sont toutes distinctes dans $\mathbb{Z}/p\mathbb{Z}$.
2. En déduire que $n^{p-1} \equiv 1\ [p]$
3. Démontrer que pour tout nombre premier $p$ et pour tout entier naturel non nul, l'on a

$$n^p \equiv n\ [p]$$