**Proposition** : Soit $(G,\cdot)$ un groupe fini et $x \in G$ un élément d'ordre $m$.

1) Soit $k$ un entier tels que $x^k = 1$. Alors $m$ divise $k$.

2) Pour tout entier $k$, l'ordre de $x^k$ est $\frac{m}{\text{pgcd}(m,k)}$.

**Preuve** :

1) Il existe des entiers $q, r$ tels que $k = mq + r$ avec $0 \leq r < m$

déduit

Donc on a $x^k = x^{mq+r} = (x^m)^q x^r = 1^q x^r = x^r = 1$

Comme $m$ est le plus petit entier strictement positif tels que $x^m = 1$, on obtient que $r = 0$.

2) Posons $d = \text{pgcd}(m,k)$. On a d'abord $(x^k)^{m/d} = (x^m)^{k/d} = e$.

Considérons un $u \geq 1$ tels que $(x^k)^u = 1$. D'après 1), $m$ divise $uk$ et donc $m/d$ divise $uk/d$. Les entiers $m/d$ et $k/d$ étant premiers entre eux, on déduit du lemme de Gauss que $m/d$ divise $u$. En particulier, on a $m/d \leq u$, d'où le résultat. ∎

**Corollaire** : Soit $n \in \mathbb{N}^*$ et $a$ un entier tels que $0 \leq a \leq n-1$. Dans le groupe additif $(\mathbb{Z}/n\mathbb{Z}, +)$, l'ordre de $\bar{a}$ est $\frac{n}{\text{pgcd}(n,a)}$

**Preuve** : Comme l'ordre de $\bar{1}$ est $n$, et que $\bar{a} = \underbrace{\bar{1} + \cdots + \bar{1}}_{a \text{ fois}}$, on

déduit du 2) de la proposition précédente que l'ordre de $\bar{a}$ est $\frac{n}{pgcd(n,a)}$. (attention ici, on utilise la notation additive)

## Groupes cycliques

**Définition** : Soit $(G,\cdot)$ un groupe fini. On dit que $G$ est cyclique s'il existe un élément $x \in G$ tel que $G = \langle x \rangle$.
Un tel élément $x$ est appelé un générateur de $G$.

Un groupe cyclique est en particulier abélien.

**Exemple** :

- Le groupe $(\mathbb{Z}/n\mathbb{Z}, +)$ est cyclique d'ordre $n$ (engendré par $\bar{1}$).
- Le groupe $(\mathbb{Z}/2\mathbb{Z} \times \mathbb{Z}/3\mathbb{Z}, +)$ est cyclique d'ordre 6, dont un générateur est $(\bar{1}, \bar{1})$.

# Chapitre : Anneaux :

**Définition** : On appelle anneau un triplet $(A, +, \cdot)$ formé d'un ensemble $A$ et de deux applications :

$$+ : A \times A \longrightarrow A \qquad \text{(addition)}$$
$$(a,b) \longmapsto a+b$$

$$\cdot : A \times A \longrightarrow A \qquad \text{(multiplication)}$$
$$(a,b) \longmapsto ab$$

tels que les conditions suivantes soient vérifiées :

1) Le groupe $(A,+)$ est un groupe commutatif.

2) La multiplication est associative et possède un élément neutre.

3) La multiplication est distributive par rapport à l'addition :

$$x(y+z) = xy + xz \quad \text{et} \quad (x+y)z = xz + yz \qquad \forall x,y,z \in A.$$

Si de plus la multiplication est commutative, (i.e $xy = yx$) on dit que $A$ est un anneau commutatif.

On note par $0$ l'élément neutre de $(A,+)$ et $1$ (ou $1_A$) l'élément neutre de $A$ par la multiplication.

**Lemme** : $\forall x, y, z \in A$, on a

$$x(y-z) = xy - xz \quad \text{et} \quad (y-z)x = yx - zx$$

**Preuve** : D'après la condition 3), on a

$$x(y-z) + xz = x(y-z+z) = xy$$

et $$(y-z)x + zx = (y-z+z)x = yx$$

d'où le lemme.

**Corollaire** : $\forall x, y \in A$, on a

$x \cdot 0 = 0 \cdot x = 0$, $\quad x(-y) = -xy$ et $(-y)x = -yx$

En particulier, on a $(-1) \cdot x = -x$.

Par convention, on a $\quad x^0 = 1 \quad \forall x \in A$

**Exemples** :

- $(\mathbb{Z}, +, \cdot)$, $(\mathbb{Q}, +, \cdot)$, $(\mathbb{R}, +, \cdot)$, $(\mathbb{C}, +, \cdot)$ sont des anneaux.
- $(M_n(A), +, \cdot)$ si $A$ est un anneau est un anneau.

- L'anneau $A[X]$ :

Soit $A$ un anneau commutatif. On considère l'anneau des polynômes :

$$A[X] = \{ P(X) = a_0 + a_1 X + \dots + a_n X^n \mid a_0, \dots a_n \in A \}$$

Si $P(X) = a_0 + a_1 X + \dots + a_n X^n$

$Q(X) = b_0 + b_1 X + \dots + b_m X^m$

on définit l'addition par :

$$(P+Q)(X) = a_0+b_0 + (a_1+b_1)X + \dots + (a_i+b_i)X^i + \dots$$

$$(P \cdot Q)(X) = a_0 b_0 + (a_1 b_0 + a_0 b_1)X + \dots + \left(\sum_{k=0}^{i} a_k b_{i-k}\right) X^i + \dots$$

On vérifie que l'ensemble des polynômes à coefficients dans A est aussi muni d'une structure d'anneau commutatif.

- Produit direct d'anneaux :

Soient $A_1, \dots, A_n$ des anneaux. Il existe sur le produit cartésien

$$A = A_1 \times \dots \times A_n$$

une structure d'anneau, l'addition et la multiplication étants données par la formule :

$$(x_1, \dots, x_n) + (y_1, \dots, y_n) = (x_1+y_1, \dots, x_n+y_n)$$

$$(x_1, \dots, x_n) \cdot (y_1, \dots, y_n) = (x_1 y_1, \dots, x_n y_n)$$

Si tous les anneaux $A_i$ sont commutatifs, il en est de même de $A$.

On dit que $A$ est le produit direct des $A_i$.

Notons que l'élément neutre multiplicatif de $A$ est $(1_{A_1}, \dots, 1_{A_n})$

## Sous-anneaux - Idéaux :

Soit $A$ un anneau et $B$ une partie de $A$.

**Définition** : On dit que $B$ est un sous-anneau de $A$ si les conditions suivantes sont vérifiées :

1) $B$ est un sous-groupe additif de $A$
2) $\forall x, y \in B, \quad xy \in B$
3) L'élément neutre multiplicatif $1$ appartient à $B$.

On vérifie que si $B$ est un sous-anneau de $A$, alors $B$ muni de l'addition et la multiplication induites par $A$ est un anneau.

**Exemple** :

1) $\mathbb{Z}$ est un sous-anneau de $\mathbb{R}$, qui est un sous anneau de $\mathbb{C}$.
2) $A$ est un sous anneau de $A[X]$.

**Définition** : Supposons que $A$ est un anneau commutatif et soit $B$ une partie de $A$. On dit que $B$ est un idéal de $A$ si les deux conditions suivantes sont vérifiées.

1) $B$ est un sous-groupe additif de $A$
2) $\forall x \in B$ et $y \in A$, le produit $yx$ est dans $B$.