

# Arithmétique

## 1. Divisibilité dans un anneau intègre

Soit  $(A, +, \times)$  un anneau intègre.

**Définition.**— Soient  $(a, b) \in A^2$ .

On dit que  $a$  divise  $b$  dans  $A$ , et on note  $a | b$ , si et seulement si :  $\exists q \in A \mid b = aq$ .

On dit que  $a$  et  $b$  sont associés dans  $A$  si et seulement si :  $a | b$  et  $b | a$ .

**Proposition.**— Soient  $(a, b) \in A^2$ .

$$1) \quad a | b \Leftrightarrow bA \subset aA.$$

$$2) \quad a \text{ et } b \text{ sont associés si et seulement si } aA = bA.$$

$$3) \quad a \text{ et } b \text{ sont associés si et seulement si il existe } u \in A^\times \text{ tel que } b = au.$$

Les associés de  $a$  sont donc les éléments de  $A$  de la forme  $au$ ,  $u$  décrivant  $A^\times$ .

### Exemples

➤ Dans l'anneau  $(\mathbb{Z}, +, \times)$  les associés de l'entier relatif  $a$  sont  $a$  et  $-a$ .

➤ Dans l'anneau  $(K[X], +, \times)$  les associés du polynôme  $P$  sont les  $\lambda P$ ,  $\lambda \in K^\times$ .

**Proposition.**— Soient  $a, b, c$  et  $b_1, \dots, b_n$  des éléments de  $A$ .

- 1) Un élément inversible de  $A$  divise tout élément de  $A$ .  
 $0_A$  est le seul élément de  $A$  à être divisible par tout élément de  $A$ .
- 2) Si  $a | b$  et  $b | c$  alors  $a | c$ .

$$3) \quad \text{Si pour tout } i \text{ dans } [1, n], a | b_i \text{ alors pour tout } (\lambda_1, \dots, \lambda_n) \in A^n, a | \sum_{i=1}^n \lambda_i b_i.$$

### 1.1 Notion de pgcd et de ppcm

**Définition.**— Soit  $(a, b) \in A^2$ .

On appelle plus grand commun diviseur (pgcd) de  $a$  et  $b$  tout élément  $d$  de  $A$  vérifiant :

$$d | a \text{ et } d | b \text{ et } \forall \delta \in A, (\delta | a \text{ et } \delta | b) \Rightarrow \delta | d.$$

On appelle plus petit commun multiple (ppcm) de  $a$  et  $b$  tout élément  $m$  de  $A$  vérifiant :  
 $a | m$  et  $b | m$  et  $\forall \mu \in A, (a | \mu \text{ et } b | \mu) \Rightarrow m | \mu$ .

Remarque : L'existence d'au moins un pgcd (resp un ppcm) n'est pas garantie. Nous verrons néanmoins que cette existence est garantie si l'anneau  $(A, +, \times)$  est principal. Nous verrons d'autre part que si  $a$  et  $b$  admettent un pgcd (resp un ppcm) alors il n'est pas unique.

**Définition.**— Des éléments  $a$  et  $b$  de  $A$  sont dits premiers entre eux ssi  $1_A$  est un pgcd de  $a$  et  $b$ .

**Proposition.**— Deux éléments  $a$  et  $b$  de  $A$  sont premiers entre eux si et seulement si l'ensemble des diviseurs communs à  $a$  et  $b$  est égal à l'ensemble des éléments inversibles de  $A$ .

### 1.2 Notion d'élément irréductible

**Définition.**— Un élément  $p$  de  $A$  est dit irréductible si et seulement si  $p$  est non nul, non inversible et si les seuls diviseurs de  $p$  dans  $A$  sont les inversibles et les associés de  $p$ .

**Proposition.**— Un élément  $p$  de  $A$  est irréductible si et seulement si  $p$  est non nul, non inversible et vérifie :  $\forall (a, b) \in A^2, p = ab \Rightarrow a \in A^\times \text{ ou } b \in A^\times$ .

**Proposition.**— Soient  $p$  un élément irréductible de  $A$  et  $a \in A$ .

$p$  et  $a$  sont premiers entre eux si et seulement si  $p$  ne divise pas  $a$ .

## 2. Arithmétique dans un anneau principal (HP)

**Définition.**— Un anneau  $(A, +, \times)$  est dit principal si et seulement si  $(A, +, \times)$  est un anneau intègre dans lequel tout idéal est de la forme  $aA$  avec  $a \in A$ .

### 2.1 Plus grand commun diviseur, plus petit commun multiple

**Théorème.**— Soient  $(A, +, \times)$  un anneau principal,  $(a, b) \in A^2$  et  $d \in A$ .

- 1) Les éléments  $a$  et  $b$  admettent au moins un pgcd.
- 2)  $d$  est un pgcd de  $a$  et  $b$  si et seulement si  $aA + bA = dA$ .
- 3) Si  $d$  est un pgcd de  $a$  et  $b$  alors les autres pgcd de  $a$  et  $b$  sont les associés de  $d$ .
- 4) Si  $d$  est un pgcd de  $a$  et  $b$  alors il existe  $(u, v) \in A^2$  tel que  $d = au + bv$ .

**Théorème.** Soient  $(A, +, \times)$  un anneau principal,  $(a, b) \in A^2$  et  $m \in A$ .

- 1) Les éléments  $a$  et  $b$  admettent au moins un ppcm.
- 2)  $m$  est un ppcm de  $a$  et  $b$  si et seulement si  $aA \cap bA = mA$ .
- 3) Si  $m$  est un ppcm de  $a$  et  $b$  alors les autres ppcm de  $a$  et  $b$  sont les associés de  $m$ .

## 2.2 Théorèmes de Bezout et de Gauss

**Théorème.** (Bezout)

Soient  $(A, +, \times)$  un anneau principal et  $(a, b) \in A^2$ .

$a$  et  $b$  sont premiers entre eux si et seulement si il existe  $(u, v) \in A^2$  tel que  $1_A = au + bv$ .

**Théorème.** (Gauss)

Soient  $(A, +, \times)$  un anneau principal et  $(a, b, c) \in A^3$ .

Si  $a$  et  $b$  sont premiers entre eux et si  $a \mid bc$  alors  $a \mid c$ .

**Corollaire.** Soient  $(A, +, \times)$  un anneau principal,  $(a, b, c) \in A^3$  et  $(p, q) \in \mathbb{N}^2$ .

- 1) On suppose  $(a, b) \neq (0, 0)$  et on considère un pgcd  $d$  de  $a$  et  $b$ .  
 $d \neq 0_A$ , il existe  $(a', b') \in A^2$  tel que  $a = da'$  et  $b = db'$  et  $a'$  et  $b'$  sont premiers entre eux.
- 2) Si  $a$  et  $b$  sont premiers entre eux et si  $a$  et  $c$  sont premiers entre eux alors  $a$  et  $bc$  sont premiers entre eux.
- 3) Si  $b$  et  $c$  sont premiers entre eux, si  $b \mid a$  et si  $c \mid a$  alors  $bc \mid a$ .
- 4) Si  $a$  et  $b$  sont premiers entre eux alors  $a^p$  et  $b^q$  sont premiers entre eux.

**Théorème.** Soient  $(A, +, \times)$  un anneau principal,  $p$  un élément irréductible de  $A$  et  $(a, b) \in A^2$ .

Si  $p \mid ab$  alors  $p \mid a$  ou  $p \mid b$ .

## 3. Arithmétique entière

### 3.1 Divisibilité dans $(\mathbb{Z}, +, \times)$

L'anneau  $(\mathbb{Z}, +, \times)$  est intègre.

Tout ce qui a été vu dans le paragraphe 1 s'applique donc intégralement. On dispose donc de la notion de divisibilité dans  $\mathbb{Z}$ , de la notion d'association ainsi que de leurs caractérisations via les idéaux. On dispose aussi de la notion d'élément irréductible. Concernant cette dernière notion on peut préciser les choses.

**Théorème.** Les irréductibles de  $(\mathbb{Z}, +, \times)$  sont les nombres premiers et leurs opposés, étant entendu qu'un nombre premier est par définition un entier naturel distinct de 1 dont les seuls diviseurs dans  $\mathbb{N}$  sont 1 et lui-même. On note  $\mathcal{P}$  l'ensemble des nombres premiers.

**Proposition (Mpsi).** L'ensemble  $\mathcal{P}$  des nombres premiers est un ensemble infini.

**Théorème (Mpsi).** (Décomposition en nombres premiers)

Tout entier  $n \geq 2$  s'écrit de manière unique sous la forme  $n = p_1^{\alpha_1} \cdots p_r^{\alpha_r}$  où  $r$  est un entier naturel non nul, où  $p_1, \dots, p_r$  sont des nombres premiers tels que  $0 < p_1 < \cdots < p_r$  et où  $\alpha_1, \dots, \alpha_r$  sont des entiers naturels non nuls. Cette décomposition de l'entier  $n$  est appelée décomposition en nombres premiers.

### Valuation p-adique

Soit  $p \in \mathcal{P}$  un nombre premier. On lui associe l'application  $v_p : \mathbb{N}^* \rightarrow \mathbb{N}$  définie de la façon suivante :

Supposons  $n \geq 2$  et considérons la décomposition  $n = p_1^{\alpha_1} \cdots p_r^{\alpha_r}$  de  $n$  en nombres premiers.

Si il existe  $i \in [1, r]$  tel que  $p = p_i$  alors on pose  $v_p(n) = \alpha_i$  et si  $p \notin \{p_1, \dots, p_r\}$  alors on pose  $v_p(n) = 0$ . On pose enfin  $v_p(1) = 0$ .

L'application  $v_p$  ainsi définie est appelée valuation p-adique.

**Théorème (Mpsi).** Tout entier non nul s'écrit de manière unique sous la forme  $n = \prod_{p \in \mathcal{P}} p^{v_p(n)}$ .

**Remarque :**

L'ensemble  $\mathcal{P}$  des nombres premiers étant infini il est important de noter que le symbole  $\prod_{p \in \mathcal{P}} p^{v_p(n)}$  représente un produit fini d'entiers naturels.

Si  $n = 1$  alors tous les  $v_p(n)$  valent 0 et par définition  $\prod_{p \in \mathcal{P}} p^{v_p(n)} = 1$ .

Si  $n \geq 2$  et si  $n = p_1^{\alpha_1} \cdots p_r^{\alpha_r} = p_1^{v_{p_1}(n)} \cdots p_r^{v_{p_r}(n)}$  est la décomposition de  $n$  en nombres premiers alors les  $v_p(n)$  valent 0 pour  $p \in \mathcal{P} \setminus \{p_1, \dots, p_r\}$  et par définition  $\prod_{p \in \mathcal{P}} p^{v_p(n)} = p_1^{v_{p_1}(n)} \cdots p_r^{v_{p_r}(n)}$ .

Autrement dit, dans tous les cas de figure,  $\Sigma_n = \{p \in \mathcal{P} \mid v_p(n) \neq 0\}$  est fini et  $\prod_{p \in \mathcal{P}} p^{v_p(n)} = \prod_{p \in \Sigma_n} p^{v_p(n)}$ .

**Proposition (Mpsi).**— Si  $a = \prod_{p \in P} p^{v_p(a)}$  et  $b = \prod_{p \in P} p^{v_p(b)}$  sont des entiers naturels non nuls alors :

$$a | b \Leftrightarrow \forall p \in P, v_p(a) \leq v_p(b).$$

### 3.2 Pgcd, Ppcm, Bezout et Gauss

L'anneau  $(\mathbb{Z}, +, \times)$  est principal.

On dispose donc des notions de pgcd, de ppcm, d'éléments premiers entre eux et tout ce qui a été vu dans le second paragraphe s'applique intégralement.

Là encore on peut préciser les choses.

**Théorème 1.**— Soient  $a$  et  $b$  deux entiers relatifs.

- 1)  $a$  et  $b$  admettent un unique pgcd positif. Il est noté  $a \wedge b$ .

Les pgcd de  $a$  et  $b$  sont alors  $a \wedge b$  et  $-(a \wedge b)$ .

- 2)  $a \wedge b = 0$  si et seulement si  $a = 0$  et  $b = 0$ .
- 3)  $a\mathbb{Z} + b\mathbb{Z} = (a \wedge b)\mathbb{Z}$  et ainsi il existe  $(u, v) \in \mathbb{Z}^2$  tel que  $a \wedge b = au + bv$ .
- 4) Si  $a$  et  $b$  sont dans  $\mathbb{N}^*$ , si  $a = \prod_{p \in P} p^{v_p(a)}$  et  $b = \prod_{p \in P} p^{v_p(b)}$  alors  $a \wedge b = \prod_{p \in P} p^{\min(v_p(a), v_p(b))}$ .

**Théorème 2.**— Soient  $a$  et  $b$  deux entiers relatifs.

- 1)  $a$  et  $b$  admettent un unique ppcm positif. Il est noté  $a \vee b$ .

$a \vee b = 0$  si et seulement si  $a = 0$  ou  $b = 0$ .

- 2) Les ppcm de  $a$  et  $b$  sont  $a \vee b$  et  $-(a \vee b)$ .
- 3) Si  $a$  et  $b$  sont dans  $\mathbb{N}^*$ , si  $a = \prod_{p \in P} p^{v_p(a)}$  et  $b = \prod_{p \in P} p^{v_p(b)}$  alors  $a \vee b = \prod_{p \in P} p^{\max(v_p(a), v_p(b))}$ .
- 4)  $(a \wedge b) \times (a \vee b) = |ab|$ .

## 4. Arithmétique polynomiale

Soit  $K$  un sous corps de  $(\mathbb{C}, +, \times)$ .

### 4.1 Divisibilité dans $(K[X], +, \times)$

L'anneau  $(K[X], +, \times)$  est intègre.

Tout ce qui a été vu dans le paragraphe 1 s'applique donc intégralement. On dispose donc de la notion de divisibilité dans  $K[X]$ , de la notion d'association ainsi que de leurs caractérisations via les idéaux. On dispose aussi de la notion d'élément irréductible. Concernant cette notion on peut préciser les choses.

**Théorème.**— Soit  $P$  un polynôme de  $K[X]$ . Les assertions suivantes sont équivalentes :

- 1)  $P$  est irréductible dans  $K[X]$ .
- 2)  $P$  est non constant et les seuls diviseurs de  $P$  dans  $K[X]$  sont les polynômes constants non nuls et les associés de  $P$ .
- 3)  $\deg P \geq 1$  et  $\forall (A, B) \in K[X]^2$ ,  $P = AB \Rightarrow \deg A = 0$  ou  $\deg B = 0$ .

**Théorème (Mpsi).**—

- 1) Les irréductibles de  $\mathbb{C}[X]$  sont les polynômes de degré un.
- 2) Les irréductibles de  $\mathbb{R}[X]$  sont les polynômes de degré un et les polynômes de degré deux à discriminant strictement négatif.

**Proposition.**—

- 1) Tout polynôme de  $K[X]$  de degré 1 est irréductible dans  $K[X]$ .
- 2) Tout polynôme de  $K[X]$  de degré 2 ou 3 et sans racines dans  $K$  est irréductible dans  $K[X]$ .  
(HP)

**Exemples**

- $X^3 + 3X + 1$  est irréductible dans  $\mathbb{Q}[X]$  mais ne l'est pas dans  $\mathbb{R}[X]$ .
- $X^4 + 1$  est sans racines dans  $\mathbb{R}$  mais n'est pas irréductible dans  $\mathbb{R}[X]$ .

**Théorème.**— (Décomposition en polynômes irréductibles dans  $K[X]$ )

Soit  $P$  un polynôme non constant de  $K[X]$ .

- 1) Il existe  $r$  polynômes irréductibles unitaires et deux à deux distincts  $P_1, \dots, P_r$ ,  $r$  entiers naturels non nuls  $\alpha_1, \dots, \alpha_r$  et un scalaire non nul  $\lambda$  tels que :  $P = \lambda P_1^{\alpha_1} \dots P_r^{\alpha_r}$ .
- 2) On a unicité de la décomposition au sens suivant : si  $P$  s'écrit  $P = \lambda P_1^{\alpha_1} \dots P_r^{\alpha_r} = \mu Q_1^{\beta_1} \dots Q_s^{\beta_s}$  où  $\lambda, \mu$  sont des scalaires non nuls,  $\alpha_1, \dots, \alpha_r, \beta_1, \dots, \beta_s$  des entiers naturels non nuls et  $P_1, \dots, P_r, Q_1, \dots, Q_s$  des polynômes irréductibles unitaires et deux à deux distincts alors  $r = s$  et  $\exists \sigma \in S_r \mid \forall i \in [1, r], P_i = Q_{\sigma(i)}$  et  $\alpha_i = \beta_{\sigma(i)}$ . Pour résumer cette dernière propriété on dit que l'on a unicité de la décomposition en polynômes irréductibles à l'ordre près des facteurs.

**Remarques**

- ✓ Il est toujours possible d'écrire un polynôme non nul  $A$  de  $K[X]$  sous la forme :  $A = \alpha P_1^{\alpha_1} \dots P_r^{\alpha_r}$  où  $P_1, \dots, P_r$  sont des polynômes irréductibles unitaires deux à deux distincts,  $\alpha_1, \dots, \alpha_r$  des entiers naturels (éventuellement nuls) et  $\alpha$  un scalaire non nul.

- ✓ Si  $A$  et  $B$  sont deux polynômes non nuls de  $K[X]$  alors il est toujours possible d'écrire  $A$  et  $B$  sous la forme :  $A = \alpha P_1^{\alpha_1} \cdots P_r^{\alpha_r}$  et  $B = \beta P_1^{\beta_1} \cdots P_r^{\beta_r}$ , où  $P_1, \dots, P_r$  sont des polynômes irréductibles unitaires deux à deux distincts,  $\alpha_1, \dots, \alpha_r, \beta_1, \dots, \beta_r$  des entiers naturels (éventuellement nuls) et  $\alpha, \beta$  des scalaires non nuls. Dans ces conditions on a :
- $$A | B \Leftrightarrow \forall i \in [1, r], \alpha_i \leq \beta_i.$$

**Théorème.** Pour  $n \geq 1$ , la décomposition en polynômes irréductibles dans  $C[X]$  de  $X^n - 1$  est donnée par :  $X^n - 1 = \prod_{\zeta \in U_n} (X - \zeta) = (X - 1)(X - \omega_n)(X - \omega_n^2) \cdots (X - \omega_n^{n-1})$  où  $\omega_n = e^{i\frac{2\pi}{n}}$ .

#### 4.2 Pgcd, Ppcm, Bezout et Gauss

L'anneau  $(K[X], +, \times)$  est principal.

On dispose donc des notions de pgcd, de ppcm, d'éléments premiers entre eux et tout ce qui a été vu dans le paragraphe 2 s'applique intégralement.

Là encore on peut préciser les choses.

**Théorème 1.** Soient  $A$  et  $B$  deux polynômes de  $K[X]$ .

- 1)  $A$  et  $B$  admettent un unique pgcd normalisé. Il est noté  $A \wedge B$ .  
Les pgcd de  $A$  et  $B$  sont alors les  $\lambda(A \wedge B)$ ,  $\lambda$  décrivant  $K \setminus \{0\}$ .
- 2) Si  $A = B = 0$  alors  $A \wedge B = 0$  et sinon  $A \wedge B$  est unitaire.
- 3)  $AK[X] + BK[X] = (A \wedge B)K[X]$  et ainsi :  $\exists (U, V) \in K[X]^2 \mid A \wedge B = AU + BV$ .
- 4) Si  $A = \alpha P_1^{\alpha_1} \cdots P_r^{\alpha_r}$  et  $B = \beta P_1^{\beta_1} \cdots P_r^{\beta_r}$  où  $P_1, \dots, P_r$  sont des polynômes irréductibles unitaires deux à deux distincts, où  $\alpha_1, \dots, \alpha_r, \beta_1, \dots, \beta_r$  sont des entiers naturels et où  $\alpha, \beta$  des scalaires non nuls alors  $A \wedge B = P_1^{\min(\alpha_1, \beta_1)} \cdots P_r^{\min(\alpha_r, \beta_r)}$ .

**Théorème 2.** Soient  $A$  et  $B$  deux polynômes de  $K[X]$ .

- 1)  $A$  et  $B$  admettent un unique ppcm normalisé. Il est noté  $A \vee B$ .  
Si  $AB = 0$  alors  $A \vee B = 0$  et sinon  $A \vee B$  est unitaire.
- 2) Les ppcm de  $A$  et  $B$  sont les  $\lambda(A \vee B)$ ,  $\lambda$  décrivant  $K \setminus \{0\}$ .
- 3) Si  $A = \alpha P_1^{\alpha_1} \cdots P_r^{\alpha_r}$  et  $B = \beta P_1^{\beta_1} \cdots P_r^{\beta_r}$  où  $P_1, \dots, P_r$  sont des polynômes irréductibles unitaires deux à deux distincts, où  $\alpha_1, \dots, \alpha_r, \beta_1, \dots, \beta_r$  sont des entiers naturels et où  $\alpha, \beta$  des scalaires non nuls alors  $A \vee B = P_1^{\max(\alpha_1, \beta_1)} \cdots P_r^{\max(\alpha_r, \beta_r)}$ .
- 4) Si  $A$  et  $B$  sont unitaires alors  $(A \wedge B)(A \vee B) = AB$ .

#### 5. Résolution de $ax + by = c$ dans $A^2$ avec $(A, +, \times)$ anneau principal (HP)

On fixe  $a, b, c$  dans  $A$  avec  $a \neq 0_A$  et  $b \neq 0_A$ .

On se propose de résoudre dans  $A^2$  l'équation (E) :  $ax + by = c$  d'inconnue  $(x, y)$ .

On considère un pgcd  $d$  de  $a$  et  $b$ .

$d \neq 0_A$ , il existe  $(a', b') \in A^2$  tel que  $a = da'$  et  $b = db'$  et  $a'$  et  $b'$  sont premiers entre eux.

Remarque : si  $A = \mathbb{Z}$  ou si  $A = K[X]$  alors on prend  $d = a \wedge b$ .

Si  $d$  ne divise pas  $c$  alors l'équation (E) n'admet pas de solutions.

Si  $d$  divise  $c$  alors l'équation (E) admet au moins une solution et si  $(x_0, y_0)$  est une solution de (E) alors l'ensemble de toutes les solutions de l'équation (E) est égal à  $\{(x_0 + kb', y_0 - ka'), k \in A\}$ .

#### Etienne Bézout (1730-1783)

Étienne Bézout, né à Nemours le 31 mars 1730 est un mathématicien français. Il est passé à la postérité pour le théorème de Bachet-Bézout en arithmétique, pour le Bézoutien, utilisé en algorithmique, et pour son théorème sur le nombre de points d'intersection de deux courbes algébriques, résultat crucial en géométrie algébrique. Il est nommé en 1763 examinateur des gardes de la marine, puis est chargé dans la foulée de la rédaction d'un cours de mathématiques. Il est ensuite nommé examinateur des élèves du corps de l'artillerie et rédige le « Cours complet de mathématiques à l'usage de la marine et de l'artillerie » qui devient plus tard le livre de référence des candidats au concours d'entrée à l'École polytechnique. Il est également l'auteur d'une Théorie générale des équations algébriques, publiée en 1779, consacrée à la théorie de l'élimination et aux fonctions symétriques des racines d'une équation algébrique. Élu adjoint de mécanique à l'Académie des sciences en 1758, il y devient associé en 1768, puis pensionnaire en 1770.

#### Carl-Friedrich Gauss (1777-1855)

Carl Friedrich Gauss, né le 30 avril 1777 à Brunswick, est considéré par ses pairs comme le prince des mathématiciens. Il est à la fois le dernier des classiques, et le premier des modernes, c'est-à-dire qu'il a résolu les problèmes les plus classiques avec les méthodes les plus modernes. Gauss était un génie particulièrement précoce : à 5 ans, le maître demandait de calculer  $1+2+\dots+100$ , et Gauss inscrivit immédiatement le résultat sur son ardoise : ce n'est pas qu'il fut un génial calculateur, mais il avait trouvé une formule générale pour calculer de telles sommes. À l'université, à 19 ans, il fut le premier à démontrer la loi de réciprocité quadratique, ce que ni Euler, ni Legendre n'avaient réussi à établir. Parmi ses autres prouesses, on peut citer la démonstration du théorème fondamental de l'algèbre, dans sa thèse de doctorat en 1799 ainsi que l'invention de la théorie des congruences. Le génie de Gauss se manifesta dans d'autres domaines : on lui doit d'importants travaux en électricité, en optique, en théorie du potentiel. Le "gauss" est ainsi devenu l'unité d'induction magnétique.

## Groupes : le retour

### 1. Sous-groupe engendré par une partie

**Théorème-définition.** Soient  $(G, \times)$  un groupe et  $A$  une partie de  $G$ . La partie  $\langle A \rangle$ , égale à l'intersection de tous les sous-groupes de  $(G, \times)$  qui contiennent  $A$ , est le plus petit sous-groupe de  $(G, \times)$  à contenir  $A$ .  $\langle A \rangle$  est appelé sous-groupe de  $(G, \times)$  engendré par la partie  $A$ .

#### Remarques

✓ On note  $\mathcal{H}_A$  l'ensemble des sous-groupes de  $(G, \times)$  qui contiennent  $A$ .

L'ensemble  $\mathcal{H}_A$  est non vide car  $G \in \mathcal{H}_A$  et par définition on a :  $\langle A \rangle = \bigcap_{H \in \mathcal{H}_A} H$ .

✓ Si  $a \in G$  alors le sous-groupe de  $(G, \times)$  engendré par la partie  $\{a\}$ , alias  $\langle \{a\} \rangle$ , est simplement noté  $\langle a \rangle$  et est appelé sous-groupe de  $(G, \times)$  engendré  $a$ . Plus généralement : si  $a_1, \dots, a_p$  sont des éléments de  $G$  alors le sous-groupe de  $(G, \cdot)$  engendré par la partie  $\{a_1, \dots, a_p\}$ , alias  $\langle \{a_1, \dots, a_p\} \rangle$ , est noté  $\langle a_1, \dots, a_p \rangle$  et est appelé sous-groupe de  $(G, \times)$  engendré par  $a_1, \dots, a_p$ .

**Proposition.**  $\langle \emptyset \rangle = \{1_G\}$ . Si  $A$  est un sous-groupe de  $(G, \times)$  alors  $\langle A \rangle = A$ .

**Théorème.** Si  $(G, \times)$  est un groupe multiplicatif et si  $a \in G$  alors  $\langle a \rangle = \{a^k, k \in \mathbb{Z}\}$ .

Si  $(G, +)$  est un groupe additif et si  $a \in G$  alors  $\langle a \rangle = \{ka, k \in \mathbb{Z}\}$ .

#### Exemples

- Dans  $(\mathbb{Z}, +)$  on a :  $n\mathbb{Z} = \langle n \rangle$ .
- Dans  $(\mathbb{C}^*, \times)$  on a :  $\mathbb{U}_n = \langle \omega_n \rangle$  avec  $\omega_n = e^{i\frac{2\pi}{n}}$ .
- Dans  $(\mathbb{Z} / n\mathbb{Z}, +)$  on a :  $\mathbb{Z} / n\mathbb{Z} = \langle \bar{1} \rangle$ .
- Dans  $(S_3, \circ)$  on a :  $A_3 = \langle (1, 2, 3) \rangle$ .

### 2. Ordre d'un élément dans un groupe

Convention et notation : Si  $E$  est un ensemble alors on définit le symbole  $|E|$  de la façon suivante.

Si  $E$  est un ensemble fini alors  $|E|$  est égal au cardinal de  $E$  et si  $E$  est infini alors  $|E| = +\infty$ .

Le symbole  $|E|$  est appelé cardinal de l'ensemble  $E$ . On notera bien que  $|E| \in \mathbb{N} \cup \{+\infty\}$ .

**Définition.** Soient  $(G, \times)$  un groupe et  $a \in G$ .

L'ordre  $\omega(a)$  de l'élément  $a$  est le cardinal du groupe engendré par  $a$ . On a donc :  $\omega(a) = |\langle a \rangle|$ . Si  $\omega(a) < +\infty$  alors  $a$  est dit d'ordre fini et si  $\omega(a) = +\infty$  alors  $a$  est dit d'ordre infini.

**Proposition.** Soient  $(G, \times)$  un groupe et  $a \in G$ .

$\omega(a) \geq 1$  et  $1_G$  est l'unique élément de  $G$  à être d'ordre un.

**Proposition.** Soient  $(G, \times)$  un groupe et  $a \in G$ . On considère  $\varphi_a : \mathbb{Z} \rightarrow G$  définie par  $\varphi_a(k) = a^k$ .

1)  $\varphi_a$  est un morphisme de groupes de  $(\mathbb{Z}, +)$  dans  $(G, \times)$ .

2)  $\text{Im } \varphi_a = \langle a \rangle$ ,  $\text{Ker } \varphi_a$  est un sous-groupe de  $(\mathbb{Z}, +)$  et par suite :  $\exists! d_a \in \mathbb{N} \mid \text{Ker } \varphi_a = d_a \mathbb{Z}$ .

**Théorème.** Soient  $(G, \times)$  un groupe et  $a \in G$ .

1) Si  $a$  est d'ordre infini alors les  $a^k$ ,  $k \in \mathbb{Z}$  sont deux à deux distincts,  $\langle a \rangle = \{a^k, k \in \mathbb{Z}\}$  est infini et le groupe  $(\langle a \rangle, \times)$  est isomorphe à  $(\mathbb{Z}, +)$ .

2) Si  $a$  est d'ordre fini alors les éléments  $1_G, a, \dots, a^{\omega(a)-1}$  sont deux à deux distincts,  $a^{\omega(a)} = 1_G$ ,  $\langle a \rangle = \{1_G, a, \dots, a^{\omega(a)-1}\}$  est fini de cardinal  $\omega(a)$  et le groupe  $(\langle a \rangle, \times)$  est isomorphe aux groupes  $(\mathbb{Z} / \omega(a)\mathbb{Z}, +)$  et  $(\mathbb{U}_{\omega(a)}, \times)$ .

**Théorème.** Soient  $(G, \times)$  un groupe et  $a$  un élément de  $G$ .

1)  $a$  est d'ordre fini si et seulement si il existe  $k \in \mathbb{Z}^*$  tel que  $a^k = 1_G$ .

2) Si  $a$  est d'ordre fini alors  $a^{\omega(a)} = 1_G$  et pour tout  $k \in \mathbb{Z}$  on a :  $a^k = 1_G \Leftrightarrow \omega(a) | k$ .

#### Exemples :

- Dans le groupe  $(\mathbb{Z}, +)$ ,  $0$  est le seul élément d'ordre fini.
- Dans le groupe  $(\mathbb{C}^*, \times)$  les éléments d'ordre fini sont les racines de l'unité.
- Dans le groupe  $(S_n, \circ)$ , tout  $p$ -cycle est d'ordre  $p$  et toute transposition est d'ordre 2.

**Théorème.** Si  $(G, \times)$  est un groupe fini de cardinal  $n$  alors tout élément  $a$  de  $G$  est d'ordre fini et son ordre  $\omega(a)$  divise  $n$ .

En particulier : si  $(G, \times)$  est un groupe fini de cardinal  $n$  alors :  $\forall a \in G, a^n = 1_G$ .

### 3. Groupes monogènes, groupes cycliques

Définition.— Soit  $(G, \times)$  un groupe.

On dit que  $a \in G$  est un générateur de  $(G, \times)$  si et seulement si  $G = \langle a \rangle$ .

Le groupe  $(G, \times)$  est dit monogène si et seulement si il admet au moins un générateur.

Le groupe  $(G, \times)$  est dit cyclique si et seulement si il est à la fois monogène et fini.

Proposition.— Tout groupe monogène est abélien.

#### Exemples

- ✓ Le groupe  $(\mathbb{Z}, +)$  est un groupe monogène infini.
- ✓ Le groupe  $(U_n, \times)$  des racines  $n^{\text{ème}}$  de l'unité est un groupe cyclique de cardinal  $n$ .
- ✓ Le groupe  $(\mathbb{Z} / n\mathbb{Z}, +)$  est un groupe cyclique de cardinal  $n$ .
- ✓ Pour  $n \geq 3$ , Le groupe  $(S_n, \circ)$  n'est pas un groupe monogène car il n'est pas commutatif.

Proposition.— Soient  $(G, \times)$  un groupe et  $a \in G$ .

- 1) Le groupe  $(\langle a \rangle, \times)$  est monogène.
- 2) Si  $a$  est d'ordre fini alors le groupe  $(\langle a \rangle, \times)$  est cyclique de cardinal  $\omega(a)$ .

Théorème.— Soit  $(G, \times)$  un groupe.

- 1) Si  $G$  est un monogène infini alors il existe  $a \in G$  tel que  $G = \{a^k, k \in \mathbb{Z}\}$ , les  $a^k, k \in \mathbb{Z}$  étant deux à deux distincts.
- 2) Si  $G$  est cyclique de cardinal  $n$  alors il existe  $a \in G$  tel que  $G = \{1_G, a, \dots, a^{n-1}\}$  et  $a^n = 1$ , les  $a^k, k \in [0, n-1]$  étant deux à deux distincts.

Théorème.—

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

Tout groupe cyclique de cardinal  $n$  est isomorphe à  $(\mathbb{Z} / n\mathbb{Z}, +)$  et donc à  $(U_n, \times)$ .

## 4. Pour aller plus loin (HP)

### 4.1 Théorème de Lagrange et applications

Théorème.— (De Lagrange)

Si  $(G, \times)$  est un groupe fini alors tout sous-groupe  $H$  de  $(G, \times)$  est fini et  $|H| \mid |G|$ .

Corollaire.— Si  $(G, \times)$  est un groupe fini de cardinal  $n$  alors :  $\forall a \in G, a^n = 1_G$  et  $\omega(a) \mid n$ .

Théorème.— Soient  $m, n, p, q$  des entiers naturels non nuls

- 1)  $U_m \subset U_n \Leftrightarrow m \mid n$ .
- 2)  $U_n$  est l'unique sous-groupe de  $(C^*, \times)$  de cardinal  $n$ .  
Les sous-groupes finis de  $(C^*, \times)$  sont les  $U_k$ ,  $k$  décrivant  $\mathbb{N}^*$ .
- 3)  $U_p \cap U_q = U_{p \wedge q}$  et  $\langle U_p \cup U_q \rangle = U_{p \vee q}$ .

Proposition.— Tout groupe fini  $(G, \times)$  de cardinal un nombre premier  $p$  est cyclique et tout élément de  $G$  distinct du neutre  $1_G$  est un générateur de du groupe  $(G, \times)$ .

### 4.2 Ordre d'un élément

Théorème.— Soient  $(G, \times)$  un groupe multiplicatif et  $a$  un élément de  $G$ .

Si  $a$  est d'ordre fini alors pour tout  $k \in \mathbb{Z}$ ,  $a^k$  est d'ordre fini et  $\omega(a^k) = \frac{\omega(a)}{k \wedge \omega(a)}$ .

Théorème.— Soient  $(G, \times)$  un groupe et  $a, b$  des éléments de  $G$  d'ordre fini.

Si  $ab = ba$  et  $\omega(a) \wedge \omega(b) = 1$  alors  $ab$  est d'ordre fini et  $\omega(ab) = \omega(a)\omega(b)$ .

Théorème.— Soient  $(G, \times)$  un groupe cyclique de cardinal  $n$  engendré par  $a$  et  $k \in \mathbb{Z}$ .  
L'élément  $a^k$  est un générateur de  $(G, \times)$  si et seulement si  $k \wedge n = 1$ .

#### Exemples :

- Si  $k \in \mathbb{Z}$  alors  $\bar{k}$  est un générateur de  $(\mathbb{Z} / n\mathbb{Z}, +)$  si et seulement si  $k \wedge n = 1$ .
- Si  $k \in \mathbb{Z}$  alors  $\omega_n^k$  est un générateur de  $(U_n, \times)$  si et seulement si  $k \wedge n = 1$ .

### 4.3 Générateurs du groupe linéaire et du groupe spécial linéaire

Théorème.— (Générateurs du groupe linéaire)

Toute matrice  $A$  de  $GL_n(\mathbb{K})$  peut s'écrire sous la forme  $A = T_1 \dots T_s D_n(\det A)$  où  $s \in \mathbb{N}$  et où  $T_1, \dots, T_s$  sont des matrices élémentaires de transvection.

En particulier :  $GL_n(\mathbb{K}) = \langle TD \rangle$  où  $TD$  est l'ensemble constitué des matrices élémentaires de transvection et des matrices élémentaires de dilatation.

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

### 1. Construction de l'anneau $(\mathbb{Z}/n\mathbb{Z}, +, \times)$

Dans tout le paragraphe  $n$  désigne un entier naturel non nul.

Pour tout  $x \in \mathbb{Z}$  on pose par définition :  $\bar{a} = a + n\mathbb{Z}$ .

L'ensemble des parties de  $\mathbb{Z}$  de la forme  $\bar{a}$ ,  $a$  décrivant  $\mathbb{Z}$  est noté  $\mathbb{Z}/n\mathbb{Z}$ .

On a donc :  $\mathbb{Z}/n\mathbb{Z} = \{\bar{a} \mid a \in \mathbb{Z}\} = \{x \in \mathcal{P}(\mathbb{Z}) \mid \exists a \in \mathbb{Z} \mid x = \bar{a}\}$ .

On rappelle que pour  $(a, b) \in \mathbb{Z}^2$  on a :  $\bar{a} = \bar{b} \Leftrightarrow a - b \in n\mathbb{Z} \Leftrightarrow a \equiv b \pmod{n}$ .

On en déduit que pour tout  $a \in \mathbb{Z}$ ,  $\bar{a} = \bar{r}$  où  $r$  est le reste de la division euclidienne de  $a$  par  $n$  puis que  $\mathbb{Z}/n\mathbb{Z} = \{\bar{0}, \bar{1}, \dots, \bar{n-1}\}$  où  $\bar{0}, \bar{1}, \dots, \bar{n-1}$  sont deux à deux distincts.

Considérons deux éléments  $x$  et  $y$  de  $\mathbb{Z}/n\mathbb{Z}$ . Par définition il existe  $(a, b) \in \mathbb{Z}^2$  tel que  $x = \bar{a}$  et  $y = \bar{b}$ . On pose alors :  $x \oplus y = \bar{a} + \bar{b}$  et  $x \otimes y = \bar{ab}$ .

Une telle définition semble dépendre du choix que l'on fait des représentants  $a$  et  $b$  de  $x$  et de  $y$ .

En fait il n'en est rien et  $\oplus$  et  $\otimes$  sont bien des lois de composition interne sur  $\mathbb{Z}/n\mathbb{Z}$ .

Pour des raisons de simplicité d'écriture les loi  $\oplus$  et  $\otimes$  sont respectivement notées  $+$  et  $\times$ .

On retiendra que par définition même on a :  $\forall (a, b) \in \mathbb{Z}^2, \bar{a} + \bar{b} = \bar{a+b}$  et  $\bar{a} \times \bar{b} = \bar{ab}$ .

**Théorème.** –  $(\mathbb{Z}/n\mathbb{Z}, +, \times)$  est un anneau commutatif fini de cardinal  $n$ .

L'application  $\pi_n : \mathbb{Z} \rightarrow \mathbb{Z}/n\mathbb{Z}$  définie par  $\pi_n(a) = \bar{a}$  est un morphisme surjectif d'anneaux.

**Remarques :**

✓  $0_{\mathbb{Z}/n\mathbb{Z}} = \bar{0}$  et  $1_{\mathbb{Z}/n\mathbb{Z}} = \bar{1}$ .

✓  $\mathbb{Z}/1\mathbb{Z}$  est l'anneau nul. Pour  $n \geq 2$ ,  $\mathbb{Z}/n\mathbb{Z}$  est un anneau non nul.

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

1)  $\forall x \in \mathbb{Z}/n\mathbb{Z}, \forall k \in \mathbb{Z}, n \mid k \Rightarrow kx = \bar{0}$ . En particulier :  $\forall x \in \mathbb{Z}/n\mathbb{Z}, nx = \bar{0}$ .

2) Pour tout  $a \in \mathbb{Z}$  on a :  $\bar{a} \in (\mathbb{Z}/n\mathbb{Z})^\times \Leftrightarrow a \wedge n = 1$ .

Par suite :  $(\mathbb{Z}/n\mathbb{Z})^\times = \{\bar{a} \mid a \in \Gamma_n\}$  où  $\Gamma_n = \{k \in [0, n-1] \mid k \wedge n = 1\}$ .

3)  $(\mathbb{Z}/n\mathbb{Z}, +, \times)$  est intègre si et seulement si  $n$  est premier.

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

**Remarque :** Soit  $p$  un nombre premier. Le polynôme  $P = X^p - X$  de  $\mathbb{Z}/p\mathbb{Z}[X]$  est non nul et pourtant sa fonction polynomiale associée, alias  $\tilde{P}$ , est égale à la fonction nulle.

**Théorème.** – (Des restes chinois)

Soient  $m$  et  $n$  deux entiers naturels non nuls.

Si  $m \wedge n = 1$  alors les anneaux  $\mathbb{Z}/mn\mathbb{Z}$  et  $\mathbb{Z}/m\mathbb{Z} \times \mathbb{Z}/n\mathbb{Z}$  sont isomorphes.

**Théorème.** – (Système de congruences)

Soient  $m$  et  $n$  deux entiers naturels non nuls et premiers entre eux. Soit  $(a, b) \in \mathbb{Z}^2$ .

On pose :  $S_{m,n}(a, b) = \{k \in \mathbb{Z} \mid k \equiv a \pmod{m} \text{ et } k \equiv b \pmod{n}\}$ .

$S_{m,n}(a, b) \neq \emptyset$  et si  $k_0 \in S_{m,n}(a, b)$  alors  $S_{m,n}(a, b) = k_0 + mn\mathbb{Z}$ .

### 2. La fonction indicatrice d'Euler

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

**Définition.** – On note  $\varphi(n)$  le nombre d'entiers naturels compris entre 0 et  $n-1$  qui sont premiers avec  $n$ . On a donc :  $\varphi(n) = |\{k \in [0, n-1] \mid k \wedge n = 1\}|$ .

L'application  $\varphi : \mathbb{N}^* \rightarrow \mathbb{N}$  ainsi définie est appelée indicatrice d'Euler.

**Proposition.** –

1)  $\varphi(1) = 1$  et si  $p$  est un nombre premier alors  $\varphi(p) = p-1$ .

2)  $\varphi(n) = |\{k \in [1, n] \mid k \wedge n = 1\}|$ .

**Proposition.** –  $\varphi(n)$  est le nombre d'éléments inversibles de l'anneau  $\mathbb{Z}/n\mathbb{Z}$ .

Autrement dit :  $\varphi(n) = |(\mathbb{Z}/n\mathbb{Z})^\times|$ .

**Proposition.** – (Calcul de l'indicatrice d'Euler)

1)  $\forall (m, n) \in (\mathbb{N}^*)^2, m \wedge n = 1 \Rightarrow \varphi(mn) = \varphi(m)\varphi(n)$ .

2) Si  $p$  est un nombre premier alors et  $\forall \alpha \in \mathbb{N}^*, \varphi(p^\alpha) = p^\alpha - p^{\alpha-1}$ .

3) Soit  $n \in \mathbb{N}$  tel que  $n \geq 2$ .  $n$  s'écrit  $n = p_1^{\alpha_1} p_2^{\alpha_2} \cdots p_r^{\alpha_r}$  où les  $p_i$  sont des nombres premiers deux à deux distincts et où les  $\alpha_i$  sont des entiers naturels non nuls. Dans ces conditions :

$$\varphi(n) = n \left(1 - \frac{1}{p_1}\right) \left(1 - \frac{1}{p_2}\right) \cdots \left(1 - \frac{1}{p_r}\right).$$

**Théorème.** Soient  $n \in \mathbb{N}^*$  et  $p$  un nombre premier.

- 1)  $\forall x \in (\mathbb{Z} / n\mathbb{Z})^\times, x^{\varphi(n)} = 1$ .
- 2)  $\forall x \in (\mathbb{Z} / p\mathbb{Z})^\times, x^{p-1} = 1$  et  $\forall x \in \mathbb{Z} / p\mathbb{Z}, x^p = x$ .

**Théorème.**

- 1) Si  $a \in \mathbb{Z}$  et si  $n \in \mathbb{N}^*$  alors  $a \wedge n = 1 \Rightarrow a^{\varphi(n)} \equiv 1 \pmod{n}$ . (Euler)
- 2) Si  $a \in \mathbb{Z}$  et si  $p$  est un nombre premier qui ne divise pas  $a$  alors  $a^{p-1} \equiv 1 \pmod{p}$ . (Fermat)
- 3) Si  $a \in \mathbb{Z}$  et si  $p$  est un nombre premier alors  $a^p \equiv a \pmod{p}$ . (Fermat)

### 3. Pour aller plus loin (HP)

**Théorème.** Soient  $n \in \mathbb{N}^*$ .

- 1)  $\varphi(n)$  est le nombre de générateurs d'un groupe cyclique de cardinal  $n$ .  $\varphi(n)$  est donc le nombre de générateurs des groupes  $(\mathbb{Z} / n\mathbb{Z}, +)$  et  $(\mathbb{U}_n, \times)$ .
- 2)  $\sum_{d|n} \varphi(d) = n$ .

**Pierre Simon de Fermat (1601-1665)**

Mathématicien français dont les travaux portent sur l'arithmétique, les probabilités et l'étude des courbes. Fermat est notamment l'auteur d'une conjecture célèbre selon laquelle pour  $x, y, z$  et  $n$  dans  $\mathbb{N}^*$  avec  $n \geq 3$  on ne peut avoir  $x^n + y^n = z^n$ . Cette conjecture porte le nom de grand théorème de Fermat. Pour la petite histoire, Fermat énonce cette conjecture dans la marge d'un livre avec l'annotation suivante : « J'ai découvert une démonstration merveilleuse mais je n'ai pas la place de la mettre dans la marge ». Depuis cette époque, de nombreux mathématiciens se sont attaqués à la démonstration de cette conjecture et ce n'est qu'en 1993 que le mathématicien anglais Andrew Wiles a résolu le problème. Il aura donc fallu plus de trois cents ans et beaucoup de mathématiques pour venir à bout de la conjecture de Fermat !!!

**Leonhard Euler (1707-1783)**

Né à Bâle en 1707, Euler étudia les mathématiques sur les conseils de Bernoulli qui était ami avec son père. Son œuvre scientifique est considérable. Il est intervenu de manière décisive en astronomie, en physique et bien sûr en mathématiques. Il a notamment introduit le concept de fonction et découvert une très jolie relation entre le nombre de sommets, d'arêtes et de faces d'un polyèdre convexe. D'une santé fragile il décède d'une hémorragie cérébrale à Saint-Pétersbourg.

## Ensembles finis, ensembles dénombrables

On note  $\leq$  la relation d'ordre usuelle de l'ensemble des nombres réels  $\mathbb{R}$ . L'ensemble totalement ordonné  $(\mathbb{R}, \leq)$  possède les propriétés fondamentales suivantes :

- Toute partie non vide de  $\mathbb{N}$  admet un plus petit élément dans  $\mathbb{N}$ .
- Toute partie non vide et majorée de  $\mathbb{N}$  admet un plus grand élément dans  $\mathbb{N}$ .
- Toute partie non vide et majorée de  $\mathbb{Z}$  admet un plus grand élément dans  $\mathbb{Z}$ .
- Toute partie non vide et minorée de  $\mathbb{Z}$  admet un plus petit élément dans  $\mathbb{Z}$ .
- Toute partie non vide et minorée de  $\mathbb{R}$  admet une borne inférieure dans  $\mathbb{R}$ .
- Toute partie non vide et majorée de  $\mathbb{R}$  admet une borne supérieure dans  $\mathbb{R}$ .

### 1. Ensemble fini - Cardinal d'un ensemble fini (Mpsi)

#### 1.1 Notion d'équipotence

**Définition (HP).**— On dit qu'un ensemble  $E$  est équivalent à un ensemble  $F$  si et seulement si il existe une bijection de  $E$  sur  $F$ . *+ sorte de ~*

**Proposition.**— Soit  $E$ ,  $F$  et  $G$  des ensembles.

- 1)  $E$  est équivalent à lui-même.
- 2)  $E$  est équivalent à  $F$  si et seulement si  $F$  est équivalent à  $E$ .
- 3) Si  $E$  est équivalent à  $F$  et si  $F$  est équivalent à  $G$  alors  $E$  est équivalent à  $G$ .

**Remarque** : Pour exprimer que  $E$  est équivalent à  $F$  ou ce qui est équivalent que  $F$  est équivalent à  $E$ , on utilise aussi la terminologie : « les ensembles  $E$  et  $F$  sont équivalents ».

#### 1.2 Notion d'ensemble fini

Pour  $(p, q) \in \mathbb{N}^2$  on pose par définition :  $[p, q] = \{n \in \mathbb{N} \mid p \leq n \leq q\}$ . Si  $p > q$  alors  $[p, q] = \emptyset$  et si  $p \leq q$  alors  $[p, q] = \{p, p+1, \dots, q-1, q\}$ . Il est à noter que  $[1, 0] = \emptyset$  et qu'il s'agit là du prototype de l'ensemble que l'on souhaite qualifier d'ensemble fini à 0 éléments.

Pour  $p \in \mathbb{N}^*$ ,  $[1, p] = \{1, 2, \dots, p-1, p\}$  est, de la même façon, le prototype de l'ensemble que l'on souhaite qualifier d'ensemble fini à  $p$  éléments. Formalisons cette idée.

**Théorème.**— Soient  $p$  et  $q$  des entiers naturels non nuls.

Si il existe une injection de  $[1, p]$  dans  $[1, q]$  alors  $p \leq q$ .

Si il existe une surjection de  $[1, p]$  sur  $[1, q]$  alors  $p \geq q$ .

Si il existe une bijection de  $[1, p]$  sur  $[1, q]$  alors  $p = q$ .

**Remarque** : le dernier point peut se reformuler en : si  $[1, p]$  et  $[1, q]$  sont équipotents alors  $p = q$ .

**Définition.**— On dit qu'un ensemble  $E$  est fini si et seulement si il existe  $p \in \mathbb{N}$  tel que  $E$  soit équipotent à  $[1, p]$ . L'ensemble  $E$  est dit infini si et seulement si  $E$  n'est pas fini.

#### Cardinal d'un ensemble fini

Soit  $E$  un ensemble fini. Par définition il existe un entier naturel  $p$  tel que  $E$  soit équipotent à  $[1, p]$ . Un tel entier  $p$  est en fait unique. En effet, si il existe  $q \in \mathbb{N}$  tel que  $E$  soit équipotent à  $[1, q]$  alors il vient :  $[1, p]$  équipotent à  $E$  et  $E$  équipotent à  $[1, q]$  donc  $[1, p]$  équipotent à  $[1, q]$  puis  $p = q$ . Cet unique entier naturel  $p$  est appelé cardinal de  $E$ . On le note  $|E|$  ou encore Card  $E$ .

#### **Proposition.**—

- 1) L'ensemble vide est le seul ensemble fini à être de cardinal 0.
- 2) Si  $p \in \mathbb{N}$  alors  $[1, p]$  est un ensemble fini de cardinal  $p$ .
- 3) Si  $(p, q) \in \mathbb{N}^2$  est tel que  $p \leq q$  alors  $[p, q]$  est un ensemble fini de cardinal  $q - p + 1$ .
- 4) Un ensemble  $E$  est fini et de cardinal  $p$  si et seulement si il est de la forme  $E = \{a_1, \dots, a_p\}$  où les  $a_k$  sont des éléments de  $E$  deux à deux distincts.
- 5)  $\mathbb{N}$  est un ensemble infini.

#### 1.3 Propriétés des ensembles finis (et infinis)

**Proposition.**— Soit  $E$  un ensemble.

Si  $E$  est équivalent à un ensemble fini  $F$  alors  $E$  est fini et  $|E| = |F|$ .

Si  $E$  est équivalent à un ensemble infini alors  $E$  est infini.

**Proposition.**— Si  $E$  et  $F$  sont deux ensembles finis alors  $E \times F$  est fini et  $|E \times F| = |E| \times |F|$ .

**Proposition.**— Soit  $E$  un ensemble fini.

- 1) Toute partie  $A$  de  $E$  est finie et vérifie :  $|A| \leq |E|$  et  $(|A| = |E| \Rightarrow A = E)$ .
- 2) Si  $A$  et  $B$  sont des parties de  $E$  alors la partie  $A \cup B$  est finie et  $|A \cup B| = |A| + |B| - |A \cap B|$ .  
En particulier : si  $A \cap B = \emptyset$  alors  $|A \cup B| = |A| + |B|$ .
- 3) Tout ensemble qui contient un ensemble infini est un ensemble infini.

Remarque : Le résultat du 2) peut se généraliser : si  $A, B, C$  sont des parties de  $E$  alors  $A \cup B \cup C$  est une partie de  $E$  et  $|A \cup B \cup C| = |A| + |B| + |C| - |A \cap B| - |B \cap C| - |C \cap A| + |A \cap B \cap C|$ .

**Théorème.**— Soient  $E$  et  $F$  deux ensembles et  $f : E \rightarrow F$  une application.

- 1) Si  $f$  est injective et si  $F$  est fini alors  $E$  est fini.
- 2) Si  $f$  est surjective et si  $E$  est fini alors  $F$  est fini.

**Théorème.**— Soient  $E, F$  des ensembles finis de même cardinal et  $f : E \rightarrow F$  une application.

$f$  est bijective  $\Leftrightarrow f$  est injective  $\Leftrightarrow f$  est surjective.

**Théorème.**— (Principe des bergers)

Soient  $E$  et  $F$  deux ensembles. Si  $F$  est fini et si il existe une application  $f : E \rightarrow F$  et un entier  $p$  tels que tout élément de  $F$  admette exactement  $p$  antécédents par  $f$  alors  $E$  est fini et  $|E| = p|F|$ .

## 2. Dénombrements classiques (Mpsi)

### 2.1 Nombre d'applications entre deux ensembles finis

**Théorème.**— Soient  $E$  et  $F$  deux ensembles finis.

- 1) L'ensemble  $F^E$  des applications de  $E$  dans  $F$  est fini et  $|F^E| = |F|^{|E|}$ .
- 2) L'ensemble  $\mathcal{P}(E)$  des parties de  $E$  est fini et  $|\mathcal{P}(E)| = 2^{|E|}$ .

### 2.2 Nombre d'injections entre deux ensembles finis

**Théorème.**— Soient  $E$  et  $F$  deux ensembles finis.

- 1) L'ensemble  $\mathcal{I}(E, F)$  des injections de  $E$  dans  $F$  est un ensemble fini.

Si  $|E| > |F|$  alors  $|\mathcal{I}(E, F)| = 0$ . Si  $|E| \leq |F|$  alors  $|\mathcal{I}(E, F)| = \frac{|F|!}{(|F| - |E|)!}$ .

Dans tous les cas de figure on a la formule :  $|\mathcal{I}(E, F)| = |F|! \binom{|F|}{|E|}$ .

2) L'ensemble  $\mathcal{B}(E, F)$  des bijections de  $E$  sur  $F$  est fini.

Si  $|E| \neq |F|$  alors  $|\mathcal{B}(E, F)| = 0$ . Si  $|E| = |F|$  alors  $|\mathcal{B}(E, F)| = |E|! = |F|!$ .

### 2.3 Nombre de parties à $p$ éléments dans un ensemble fini

**Théorème.**— Soient  $E$  un ensemble fini et  $p$  un entier naturel.

L'ensemble  $\mathcal{P}_p(E)$  des parties de  $E$  ayant  $p$  éléments est fini.

Si  $p > |E|!$  alors  $|\mathcal{P}_p(E)| = 0$  et si  $p \leq |E|$  alors  $|\mathcal{P}_p(E)| = \frac{|E|!}{p!(|E| - p)!}$ .

Dans tous les cas de figure on a la formule :  $|\mathcal{P}_p(E)| = \binom{|E|}{p}$ .

### 2.4 p-listes et combinaisons

**Définition.**— Soient  $E$  un ensemble et  $p$  un entier naturel.

Une  $p$ -liste d'éléments de  $E$  est un élément  $(x_1, \dots, x_p)$  de  $E^p$ .

Une  $p$ -liste d'éléments distincts de  $E$  est un élément  $(x_1, \dots, x_p)$  de  $E^p$  avec  $x_i \neq x_j$  pour  $i \neq j$ .

Une  $p$ -combinaison de  $E$  est une partie de  $E$  de cardinal  $p$ .

**Proposition.**— Soient  $n$  et  $p$  deux entiers naturels.

- 1) Le nombre d'applications d'un ensemble de cardinal  $p$  dans un ensemble de cardinal  $n$  est  $n^p$ .  
Le nombre de  $p$ -listes d'éléments d'un ensemble de cardinal  $n$  est  $n^p$ .
- 2) Le nombre d'applications injectives d'un ensemble de cardinal  $p$  dans un ensemble de cardinal  $n$  est  $p! \binom{n}{p}$ . Le nombre de  $p$ -listes d'éléments distincts d'un ensemble de cardinal  $n$  est  $p! \binom{n}{p}$ .
- 3) Le nombre de parties d'un ensemble de cardinal  $n$  est  $2^n$ .
- 4) Le nombre de parties de cardinal  $p$  (ou  $p$ -combinaison) d'un ensemble de cardinal  $n$  est  $\binom{n}{p}$ .

### 2.5 Obtention de formules via un raisonnement de nature combinatoire

Si  $E$  est un ensemble fini et si  $A_1, \dots, A_n$  sont des parties deux à deux disjointes de  $E$  dont la réunion vaut  $E$  alors on a la formule :  $|E| = \sum_{k=1}^n |A_k|$ .

Ce résultat permet d'établir de nombreuses formules. Examinons cela sur quelques exemples.

**Proposition.-**

- 1)  $\forall (n, p) \in \mathbb{N}^2, \binom{n+1}{p+1} = \binom{n}{p+1} + \binom{n}{p}$ .
- 2)  $\forall n \in \mathbb{N}, \sum_{k=0}^n \binom{n}{k} = \binom{n}{0} + \binom{n}{1} + \dots + \binom{n}{n} = 2^n$ .
- 3)  $\forall (p, q, r) \in \mathbb{N}^3, \sum_{k=0}^r \binom{p}{k} \binom{q}{r-k} = \binom{p+q}{r}$ .

**Proposition (HP).-** Pour  $n \in \mathbb{N}$  on note  $D_n$  le nombre de permutations sans points fixes d'un ensemble fini de cardinal  $n$ . On a alors la formule :  $n! = \sum_{k=0}^n \binom{n}{k} D_k$ .

**Proposition (HP).-** Pour  $(n, p) \in \mathbb{N}^2$  on note  $S_{p,n}$  le nombre de surjections d'un ensemble fini de cardinal  $p$  dans un ensemble fini de cardinal  $n$ . On a alors la formule :  $n^p = \sum_{k=0}^n \binom{n}{k} S_{p,k}$ .

**3. Ensembles dénombrables**

**Définition.-** On dit qu'un ensemble  $E$  est dénombrable si et seulement si  $E$  est équivalent à  $\mathbb{N}$ .

**Proposition.-**

- 1) Un ensemble équivalent à un ensemble fini est fini.
- 2) Un ensemble équivalent à un ensemble dénombrable est dénombrable.
- 3) Un ensemble équivalent à un ensemble fini ou dénombrable (FOD) est FOD.

**Théorème.-** Toute partie infinie de  $\mathbb{N}$  est dénombrable.

**Proposition.-**

- 1) Un ensemble est FOD si et seulement si il est équivalent à une partie de  $\mathbb{N}$ .
- 2) Une partie d'un ensemble dénombrable est FOD.

**Théorème.-**  $\mathbb{N}^2$  est dénombrable

**Proposition.-** Si  $E$  et  $F$  sont des ensembles dénombrables alors  $E \times F$  est dénombrable.

**Proposition.-** Soient  $E$  et  $F$  des ensembles et  $f : E \rightarrow F$  une application.

- 1) Si  $f$  est injective et si  $F$  est FOD alors  $E$  est FOD.
- 2) Si  $f$  est surjective et si  $E$  est FOD alors  $F$  est FOD.

**Proposition.-** Une réunion FOD d'ensembles FOD est un ensemble FOD.

**Théorème.-** Si  $(z_i)_{i \in I}$  est une famille sommable de complexes alors  $\{i \in I \mid z_i \neq 0\}$  est FOD.

**Théorème.-**  $\mathbb{N}$ ,  $\mathbb{N}^*$ ,  $\mathbb{N}^2$ ,  $\mathbb{Z}$  et  $\mathbb{Q}$  sont dénombrables.

**Théorème.-**  $\mathbb{R}$  n'est pas dénombrable.

**4. Pour aller plus loin (HP)****Proposition.- (Formule du crible)**

Si  $E$  est un ensemble fini, si  $A_1, \dots, A_n$  sont des parties de  $E$  alors :

$$\left| \bigcup_{k=1}^n A_k \right| = \sum_{k=1}^n (-1)^{k+1} S_k^{(n)} \text{ avec } S_k^{(n)} = \sum_{J \in \mathcal{P}_k(\{1, \dots, n\})} \left| \bigcap_{j \in J} A_j \right| = \sum_{1 \leq j_1 < \dots < j_k \leq n} |A_{j_1} \cap \dots \cap A_{j_k}|.$$

**Proposition.- (Nombre de solutions dans  $\mathbb{N}^p$  de l'équation  $\alpha_1 + \dots + \alpha_p = n$ .)**

On considère  $n \in \mathbb{N}$  et  $p \in \mathbb{N}^*$ .

Le nombre  $\Gamma_n^p$  de  $p$ -listes  $(\alpha_1, \dots, \alpha_p)$  de  $\mathbb{N}^p$  vérifiant  $\alpha_1 + \dots + \alpha_p = n$  est égal à  $\binom{n+p-1}{p-1}$ .

**Proposition.- (Nombre de dérangements)**

On considère  $n \in \mathbb{N}$  et on note  $D_n$  le nombre de permutations sans points fixes d'un ensemble fini de cardinal  $n$ . Dans ces conditions :

$$D_0 = 1, \quad n! = \sum_{k=0}^n \binom{n}{k} D_k \quad \text{et} \quad D_n = n! \sum_{k=0}^n \frac{(-1)^k}{k!}.$$

**Proposition.- (Nombre de surjections)**

On considère  $(p, n) \in \mathbb{N}^2$  et on note  $S_{p,n}$  le nombre de surjections d'un ensemble de cardinal  $p$  sur un ensemble de cardinal  $n$ .

$$\text{Si } p < n \text{ alors } S_{p,n} = 0, \quad S_{n,n} = n!, \quad n^p = \sum_{k=0}^n \binom{n}{k} S_{p,k} \text{ et } S_{p,n} = (-1)^n \sum_{k=0}^n \binom{n}{k} (-1)^k k^p.$$