CHAPITRE 8

ARITHMÉTIQUE ET POLYNÔMES

8.1 Arithmétique des entiers

8.1.1 Généralités

Définition 8.1

Soit $(a, b) \in \mathbb{Z}^2$. On dit que a est un **diviseur** de b ou que b est un **multiple** de a s'il existe $k \in \mathbb{Z}$ tel que $b = ka$.

Notation. On dit que a divise b et on note $a|b$.

Théorème et définition 8.2

Soit $(a, b) \in \mathbb{Z} \times \mathbb{N}^*$. Alors il existe un unique couple $(q, r) \in \mathbb{Z}^2$ tel que

- $a = bq + r$,
- $0 \leq r < b$.

Cette opération s'appelle **division euclidienne** de a par b , dont q est le **quotient** et r le **reste**.

Définition 8.3

On dit que $p \in \mathbb{N}$ est un nombre **premier** s'il admet exactement deux diviseurs : 1 et p . Un nombre qui n'est pas premier est dit **composé**.

Théorème 8.4

L'ensemble des nombres premiers est infini.

Théorème 8.5 (Décomposition en produit de facteurs premiers)

Soit $n \in \mathbb{N} \setminus \{0, 1\}$. Alors n s'écrit de manière unique sous la forme

$$p_1^{\alpha_1} \cdots p_k^{\alpha_k},$$

avec $p_1 < \dots < p_k$ des nombres premiers et $\alpha_1, \dots, \alpha_k \in \mathbb{N}^*$.

Remarque. Chaque α_i est appelé **valuation** de p_i dans la décomposition de n

8.1.2 Ensembles et parties finis

Notation. On notera désormais $\llbracket m, n \rrbracket$ l'ensemble des entiers compris entre m et n .

On admet pour ce chapitre le résultat suivant dont la démonstration est accessible mais difficile.

Lemme 8.6

Soit $(m, n) \in \mathbb{N}^2$. S'il existe une bijection entre $\llbracket 1, m \rrbracket$ et $\llbracket 1, n \rrbracket$, alors $m = n$.

Définition 8.7

On dit que l'ensemble E est un **ensemble fini** s'il est vide ou s'il existe $n \in \mathbb{N}$ et une bijection entre E et $\llbracket 1, n \rrbracket$.

D'après le lemme ci-dessus, si un tel entier existe, il est unique ; on l'appelle **cardinal** de E , noté $\text{Card } E$ ou $\#E$, ou $|E|$. Par extension, l'ensemble vide a un cardinal nul.

Deux ensembles de même cardinal sont dits **équipotents**.

Proposition 8.8

Soit E un ensemble fini et F une partie de E . Alors

- (i) $\text{Card } F \leq \text{Card } E$;
- (ii) $\text{Card } F = \text{Card } E \Leftrightarrow F = E$.

Théorème 8.9 (Parties finies de $\mathbb{N}$)

- (i) Une partie de $\mathbb{N}$ est finie si et seulement si elle est majorée.
- (ii) Si P est une partie non vide de $\mathbb{N}$, de cardinal n , alors il existe une unique bijection strictement croissante de $\llbracket 1, n \rrbracket$ dans P .

Proposition 8.10

Soit $f : E \rightarrow F$ avec E et F ensembles finis. Alors

- (i) $\text{Card}(f(E)) \leq \text{Card } E$;
- (ii) $\text{Card}(f(E)) = \text{Card } E \Leftrightarrow f$ est injective.

Théorème 8.11

Soit $f : E \rightarrow F$ avec E et F deux ensembles finis de même cardinal. Alors on a équivalence entre

- (i) f est injective,
- (ii) f est surjective,
- (iii) f est bijective.

Opérations

Proposition 8.12

Soient E et F deux ensembles finis.

- (i) $E \cup F$ est fini et $\text{Card}(E \cup F) = \text{Card } E + \text{Card } F - \text{Card}(E \cap F)$.
- (ii) $E \times F$ est fini et $\text{Card}(E \times F) = \text{Card } E \times \text{Card } F$.

Remarque. Si E et F sont finis et disjoints, alors $\text{Card}(E \cup F) = \text{Card } E + \text{Card } F$. Dans ce cas on note $E \cup F = E \sqcup F$.

Proposition 8.13 (Nombre d'applications)

Soient E et F deux ensembles finis de cardinaux respectifs p et n . Alors

$$\text{Card}(\mathcal{F}(E, F)) = n^p.$$

Proposition 8.14 (Nombres de parties de E)

Soient E un ensemble fini de cardinal p . Alors

$$\text{Card}(\mathcal{P}(E)) = 2^p.$$

8.1.3 Dénombrement

 p -listes**Définition 8.15**

Étant donné un ensemble E et $p \in \mathbb{N}$, on appelle **p -liste** d'éléments de E tout p -uplet d'éléments de E , c'est-à-dire tout élément de E^p .

Remarque. L'ordre des éléments compte et il peut y avoir des répétitions.

Proposition 8.16

Soit E un ensemble fini de cardinal n et $p \in \mathbb{N}$. Le nombre de p -listes d'éléments de E est n^p .

 p -arrangements

Définition 8.17

Soient E un ensemble fini de cardinal n et $p \in \mathbb{N}$, on appelle **p -arrangement** de E toute p -liste d'éléments distincts de E .

Remarque. L'ordre des éléments compte et il ne peut pas y avoir de répétitions.

Proposition 8.18

Avec les mêmes notations,

- (i) le nombre de p -arrangements de E est $A_n^p = \frac{n!}{(n-p)!}$;
- (ii) Le nombre d'injections de E dans $\llbracket 1, p \rrbracket$ est $\frac{n!}{(n-p)!}$.

Définition 8.19

Soit E un ensemble fini de cardinal n . On appelle **permutation** de E toute bijection de E dans lui-même.

Proposition 8.20

Avec les mêmes notations, il existe $n!$ permutations de E

Remarque. Il y a une correspondance entre les permutations et les n -arrangements de E .

 p -combinaisons**Définition 8.21**

Soient E un ensemble fini de cardinal n et $p \in \mathbb{N}$, on appelle **p -combinaison** de E toute partie de cardinal p de E .

Remarque. L'ordre des éléments ne compte pas et il ne peut pas y avoir de répétitions.

Proposition 8.22

Le nombre de p -combinaisons de E est $\binom{n}{p} = \frac{n!}{p!(n-p)!}$.

Proposition 8.23

Pour tout $n \in \mathbb{N}$,

(i) $\forall p \in \llbracket 0, n \rrbracket, \binom{n}{p} = \binom{n}{n-p}$;

(ii) $\sum_{k=0}^n \binom{n}{k} = 2^n$;

(iii) $\forall p \in \llbracket 0, n-1 \rrbracket, \binom{n}{p} + \binom{n}{p+1} = \binom{n+1}{p+1}$ (formule de Pascal) ;

(iv) $\forall x, y \in \mathbb{C}, (x+y)^n = \sum_{k=0}^n \binom{n}{k} x^k y^{n-k}$ (formule du binôme de Newton).

8.2 Arithmétique des polynômes

Dans toute la suite, $\mathbb{K}$ désigne $\mathbb{R}$ ou $\mathbb{C}$.

8.2.1 Définitions

Définition 8.24

On appelle **polynôme** à coefficients dans $\mathbb{K}$ une suite $(a_k)_k$ d'éléments de $\mathbb{K}$ nulle à partir d'un certain rang,

$$(a_k)_k = (a_0, a_1, \dots, a_n, 0, \dots).$$

Notations.

- On note 1 le polynôme $(1, 0, \dots)$.
- On note X le polynôme $(0, 1, 0, \dots)$.
- On note naturellement X^n le produit n fois de X par lui-même, qui donne

$$X^n = (\underbrace{0, \dots, 0}_{n \text{ zéros}}, \underbrace{1}_{a_n}, 0, \dots).$$

- Avec ces notations, $P = (a_0, \dots, a_n, 0, \dots)$ sera noté

$$P = a_0 + a_1X + \dots + a_nX^n$$

Définition 8.25

Soit $P = a_0 + \dots + a_nX^n$ avec $a_n \neq 0$. Alors on appelle

- (i) **degré de P** l'entier p , noté $\deg(P)$.
- (ii) **coefficient dominant** le coefficient a_n et **terme dominant** le monôme a_nX^n ,

Remarque. Par convention, le degré du polynôme nul est $-\infty$.

Définition 8.26

Un polynôme dont le coefficient dominant vaut 1 est appelé **polynôme normalisé**.

Définition 8.27

On définit sur $\mathbb{K}[X]$ les deux opérations suivantes : étant donnés $P = (a_0, \dots, a_n, 0, \dots)$ et $Q = (b_0, \dots, b_n, 0, \dots)$, on définit

- $P + Q = (a_0 + b_0, \dots, a_n + b_n, 0, \dots)$;
- $P \times Q = (c_0, \dots, c_n, \dots)$ avec pour tout $p \in \mathbb{N}$, $c_p = \sum_{k=0}^{+\infty} a_k b_{p-k}$.

Définition 8.28

Étant donné un polynôme $P = a_0 + a_1X + \dots + a_nX^n \in \mathbb{K}[X]$, on appelle **fonction polynomiale** associée à P la fonction

$$\begin{aligned} \tilde{P} : \mathbb{K} &\rightarrow \mathbb{K} \\ x &\mapsto a_0 + a_1x + \dots + a_nx^n. \end{aligned}$$

Proposition 8.29

Soient $P, Q \in \mathbb{K}[X]$. Alors

- (i) $\deg(P + Q) \leq \max(\deg P, \deg Q)$,
- (ii) $\deg(P \times Q) = \deg P + \deg Q$.

Définition 8.30 (Divisibilité)

Soient $A, B \in \mathbb{K}[X]$. On dit que A **divise** B et on note $A|B$ s'il existe $Q \in \mathbb{K}[X]$ tel que $B = A \times Q$. On dit alors aussi que B est **multiple** de A .

Théorème 8.31

Soit $(A, B) \in \mathbb{K}[X]^2$. Alors il existe un unique couple $(Q, R) \in \mathbb{K}[X]^2$ tel que

- $A = BQ + R$,
- $\deg R < \deg B$.

8.2.2 Racines d'un polynôme

Définition 8.32

Soient $P \in \mathbb{K}[X]$ et $\alpha \in \mathbb{K}$. On dit que α est une **racine** ou un **zéro** de P si $\tilde{P}(\alpha) = 0$.

Proposition 8.33

Soit $P \in \mathbb{K}[X]$ et $\alpha \in \mathbb{K}$. Alors

$$\alpha \text{ est une racine de } P \iff (X - \alpha) | P.$$

Théorème 8.34

Tout polynôme non nul de degré inférieur ou égal à n admet au plus n racines.

Remarque. On l'utilise souvent sous la forme : tout polynôme de degré n qui admet au moins $n + 1$ racines est le polynôme nul.

Définition 8.35 (Racines multiples)

Soit $P \in \mathbb{K}[X]$. Soient $\alpha \in \mathbb{K}$ et $p \in \mathbb{N}^*$.

- (i) On dit que α est une **racine d'ordre** p (ou **de multiplicité** p) de P si $(X - \alpha)^p$ divise P .
- (ii) Une racine d'ordre 1 est une **racine simple**
- (iii) Une racine d'ordre strictement supérieur à 1 est une **racine multiple**.

Proposition 8.36

Soient $P \in \mathbb{K}[X]$ et $\alpha \in \mathbb{K}$. Alors α est une racine de P d'ordre p si et seulement s'il existe $Q \in \mathbb{K}[X]$ tel que

- $P = (X - \alpha)^p Q$,
- $Q(\alpha) \neq 0$.

8.2.3 Polynômes dérivés

Définition 8.37 (Polynôme dérivé)

- Soit $P = a_0 + a_1X + \dots + a_nX^n$. On définit alors le **polynôme dérivé** de P par

$$P' = a_1 + 2a_2X + \dots + na_nX^{n-1} = \sum_{k=1}^n ka_kX^{k-1}.$$

- Soient $P \in \mathbb{K}[X]$ et $n \in \mathbb{N}$. On définit par récurrence le **polynôme dérivée n -ième** (ou n fois) par
 - $P^{(0)} = P$,
 - $\forall n \in \mathbb{N}, P^{(n+1)} = [P^{(n)}]'$.

Proposition 8.38

Soit $P \in \mathbb{K}[X]$. Alors

- si $\deg P > 0$, $\deg P' = \deg P - 1$,
- P est constant si et seulement si $P' = 0$.

Proposition 8.39

Soient $P, Q \in \mathbb{K}[X]$ et $\alpha, \beta \in \mathbb{K}$. Alors

- $(\alpha P + \beta Q)' = \alpha P' + \beta Q'$;
- $(PQ)' = P'Q + PQ'$.
- Soit $n \in \mathbb{N}$. On a la formule de Leibniz :

$$(PQ)^{(n)} = \sum_{k=0}^n \binom{n}{k} P^{(k)} Q^{(n-k)}.$$

Proposition 8.40

Soient $n \in \mathbb{N}$ et $P \in \mathbb{K}$ un polynôme de degré inférieur ou égal à n . Soit $a \in \mathbb{K}$; alors

$$P = \sum_{k=0}^n \frac{P^{(k)}(a)}{k!} (X - a)^k.$$

Théorème 8.41 (Caractérisation des racines)

Soient $P \in \mathbb{K}[X]$, $p \in \mathbb{N}^*$ et $\alpha \in \mathbb{K}$. Alors on a équivalence entre

- (i) α est une racine de P d'ordre p ,
- (ii) $P(\alpha) = P'(\alpha) = \dots = P^{(p-1)}(\alpha) = 0$ et $P^{(p)}(\alpha) \neq 0$.

8.2.4 Factorisation dans $\mathbb{K}[X]$ **Définition 8.42**

Soit $P \in \mathbb{K}[X]$, on note a_n son coefficient dominant. On dit que P est **scindé sur $\mathbb{K}$** s'il existe des scalaires $\alpha_k \in \mathbb{K}$ (pas nécessairement distincts) tels que

$$P = a_n(X - \alpha_1) \dots (X - \alpha_n) = a_n \prod_{k=1}^n (X - \alpha_k).$$

Théorème 8.43

Soit P un polynôme non constant de $\mathbb{C}[X]$. Alors P possède au moins une racine dans $\mathbb{C}$.

Corollaire 8.44

Tout polynôme $P \in \mathbb{C}[X]$ est scindé sur $\mathbb{C}$, c'est-à-dire qu'il s'écrit sous la forme

$$P = a_n(X - \alpha_1) \dots (X - \alpha_n),$$

où les scalaires α_k sont les racines de P comptées avec multiplicités, et a_n son coefficient dominant.

Corollaire 8.45

Soient $P = X^n + a_{n-1}X^{n-1} + \dots + a_1X + a_0$ un polynôme unitaire et $\alpha_1, \dots, \alpha_n$ ses racines complexes. Alors

- (i) $a_0 = (-1)^n \prod_{k=1}^n \alpha_k$,
- (ii) $a_{n-1} = -\sum_{k=1}^n \alpha_k$,

Théorème 8.46 (Factorisation dans $\mathbb{C}[X]$)

Tout polynôme $P \in \mathbb{C}[X]$ de degré n admet n racines dans $\mathbb{C}$, comptées avec leurs multiplicités.

Théorème 8.47 (Factorisation dans $\mathbb{R}[X]$)

Soit $P \in \mathbb{R}[X]$. Alors P peut s'écrire sous la forme

$$P = a \prod_{k=1}^r (X - \alpha_k) \prod_{\ell=1}^s (X^2 + b_\ell X + c_\ell),$$

avec

- $a \in \mathbb{R}^*$ le coefficient dominant de P ,
- $\alpha_1, \dots, \alpha_r \in \mathbb{R}$ les racines réelles de P , non nécessairement distinctes,
- $(b_1, c_1), \dots, (b_s, c_s) \in \mathbb{R}^2$ tels que, pour tout $1 \leq \ell \leq s$, on ait $\Delta_\ell = b_\ell^2 - 4c_\ell < 0$.

Définition 8.48 (irréductibilité)

Soit $P \in \mathbb{K}[X]$ un polynôme non constant. On dit que P est irréductible si

$$P = AB \Rightarrow A \in \mathbb{K} \text{ ou } B \in \mathbb{K}.$$

Proposition 8.49

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

Théorème 8.50

- (i) Dans $\mathbb{C}[X]$, les polynômes irréductibles sont les polynômes de degré 1.
- (ii) Dans $\mathbb{R}[X]$, les polynômes irréductibles sont les polynômes de degré 1 et les polynômes de degré 2 dont le discriminant est strictement négatif.

Théorème 8.51 (Décomposition en produit d'irréductibles)

Soit P un polynôme non nul de $\mathbb{K}[X]$. Alors il existe $\alpha \in \mathbb{K}^*$ et m polynômes $P_1, \dots, P_m \in \mathbb{K}[X]$ irréductibles et unitaires tels que

$$P = \alpha \prod_{k=1}^m P_k.$$

De plus α et l'ensemble des P_k sont uniques.