Chapitre Un

Structures algébriques usuelles

1.1 Lois de composition internes

1.1.1 Définition

Soit E un ensemble non vide. On appelle loi de composition interne sur E la donnée d'une application de $E \times E$ dans E.

$$* \qquad E \times E \longrightarrow E$$

$$(x, y) \longmapsto x * y$$

Exemples 1.1. *L'addition et la multiplication dans $\mathbb{N}$, la loi de composition dans l'ensemble des fonctions affines à coefficient dans $\mathbb{R}$, la réunion et l'intersection sur l'ensemble des parties d'un ensemble E, l'exponentiation sur $\mathbb{N}$. (On peut donner aussi des contre exemples).*

Notations 1.2. *On note souvent les lois par les symboles $*$, $\perp$, $\top$, $f \ldots$.*

1.1.2 Qualité d'une loi

Soit $*$ une loi de composition interne définie sur un ensemble non vide E. $*$ est dite associative si et seulement si :

$$\forall \quad x, y, z \in E; \qquad x * (y * z) = (x * y) * z.$$

Soit $*$ une loi de composition interne définie sur un ensemble non vide E. $*$ est dite commutative si et seulement si :

$$\forall \quad x, y \in E; \qquad x * y = y * x.$$

On dit qu'une loi de composition interne $*$ définie sur un ensemble non vide E admet un élément neutre si et seulement si :

$$\exists\, e \in E, \forall\, x \in E, x * e = e * x = x.$$

Propriété 1.3. *Soit $*$ une loi de composition interne définie sur un ensemble non vide E. Si $*$ admet un élément neutre dans E alors cet élément neutre est unique.*

Soit $*$ une loi de composition interne définie sur un ensemble non vide E. On suppose que $*$ admet dans E un élément neutre notée e. Un élément x de E a un symétrique (ou

est inversible) pour la loi $*$ si et seulement si :

$$\exists\, x' \in E / x * x' = x' * x = e.$$

Dans ce cas, x' est appelé un symétrique de x ou inverse de x.

Propriété 1.4. *Soit $*$ une loi de composition interne définie sur un ensemble non vide E. On suppose que $*$ est associative. Si un élément x de E a un symétrique alors ce symétrique est unique.*

(Un peu de commentaire sur les notations additives et multiplicatives)

Exercice 1.5. *(1) On considère l'ensemble E défini par $E = \{a + b\sqrt{3}, a,\ b\ \in \mathbb{Z}\}$. Sur E, on définit la loi $*$ sur E par :*

$$(a + b\sqrt{3}) * (c + d\sqrt{3}) = (a + b\sqrt{3}) \times (c + d\sqrt{3}).$$

Démontrer que $*$ est une loi de composition interne sur E.
Démontre $*$ admet un élément neutre dans E.
Détermine l'ensemble E^* des éléments de E qui ont un symétrique dans E pour la loi $*$.

(2) On définit sur $]-1, 1[$ la loi $*$ par $a * b = \frac{a+b}{1+ab}$.
Démontre que $*$ est une loi de composition interne sur $]-1, 1[$ (On pourra remarquer que $a + b - ab - 1 = -(1 - a)(1 - b)$).
Etudie les qualités de cette loi.

(3) Soit E un ensemble non vide muni d'une loi de composition interne notée $*$. On suppose que dans E, $*$ admet un élément neutre notée e. Un élément a de E est régulier si et seulement si pour tout couple (x, y) d'élément de E, on a :

$$a * x = a * y \Longrightarrow x = y \text{ et } x * a = y * a \Longrightarrow x = y.$$

Démontre que tout élément symétrisable de E pour la loi $*$ est régulier. La réciproque est-elle vraie ?

Soit E un ensemble non vide muni de deux lois de composition internes $\perp$, et $\top$. La loi $\perp$ est dite distributive par rapport à la loi $\top$ si et seulement si

$$\forall a,\ b,\ c \in\ E,\ ona$$

$$a\perp(b\top c) = (a\perp b)\top(a\perp c) \text{ et } (b\top c)\perp a = (b\perp a)\top(c\perp a).$$

Soit E un ensemble muni d'une loi de composition interne notée $*$ et A un sous-ensemble de E. A est dit stable pour la loi $*$ si et seulement si :

$$\forall\ a,\ b \in A,\ a * b \in A.$$

Exercice 1.6. *Soit E un ensemble non vide muni d'une loi de composition interne notée $*$. On suppose que $*$ est associative et qu'elle admet dans E un élément neutre notée e. On désigne par A l'ensemble des éléments inversibles de A.*
Démontre que A est une partie non vide de E stable pour la loi $*$.

1.2 Structure de groupe

1.2.1 Définition

Soit G un ensemble non vide muni d'une loi de composition interne notée $*$.
On dit que $(G,*)$ est un groupe si et seulement si :

(1) $*$ admet un élément neutre,

(2) $*$ est associative,

(3) tout élément de G admet un symétrique pour la loi $*$ dans G.

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

Exemples 1.7. *Donner des exemples et aussi des contres exemples.*

Exercice 1.8. *(1) Soit n un entier naturel supérieur où égal à 2. On pose $\mathbb{U}_n = \{z \in \mathbb{C}/z^n = 1\}$. Démontre que $(\mathbb{U}_n, \times)$ est groupe.*

(2) On pose $\mathbb{U} = \{z \in \mathbb{C}/\,|z| = 1\}$. Démontre que $(\mathbb{U}_n, \times)$ est un groupe.

(3) Démotre que $\mathbb{U}_n \subset \mathbb{U}$.

Propriété 1.9. *Soit $(G,*)$ un groupe. Alors pour tous éléments a, b et x de G :*

(1) Si $a * x = b * x$, alors $a = b$,

(2) Si $x * a = x * b$, alors $a = b$,

(3) Le symétrique de $a * b$ est $b' * a'$ où a' est le symétrique de a et b' le symétrique de b.

1.2.2 Sous-groupe

Soit $(G,*)$ un groupe d'élément neutre e et H un sous-ensemble de G. $(H,*)$ est un sous groupe de $(G,*)$ si et seulement si H muni de la restriction de $*$ à $H \times H$ a une structure de groupe. Autrement dit, $(H,*)$ est un sous groupe de $(G,*)$ si et seulement si :

(1) $\forall\ x,\ y \in H,\ x * y \in H$,

(2) $e \in H$,

(3) $\forall\ x \in H$ son symétrique $x' \in H$.

Exercice 1.10. *Montre que ces deux définitions sont équivalentes.*

Propriété 1.11. *Soit $(G,*)$ un groupe. Un sous-ensemble H de G muni de la loi $*$ est un sous-groupe de $(G,*)$ si et seulement si les deux conditions suivantes sont vérifiées :*

(1) L'ensemble H n'est pas vide.

(2) Pour tous a et b de H, le produit $a * b^{-1}$ est aussi dans H.

Définition 1.12. *Soit G un groupe de loi de composition $*$ d'élément neutre e et soit a un élément de G. L'ordre de a est le plus petit entier $k \geq 1$, s'il existe, tel que $a^k = e$. Sinon on dit que l'ordre de a est infini.*

Définition 1.13. *Soit E un ensemble non vide. On appelle permutation ou substitution de E, toute bijection de E dans E. L'ensemble de toute les bijections de E dans E muni de la loi de la loi de composition des applications a une structure de groupe appelé symétrique de E noté $S(E)$. Si $E = \{1, 2, 3, ..., n\}, \quad n \in \mathbb{N}^*$, alors $S(E)$ est simplement noté S_n.*

Notations 1.14. *On dispose de plusieurs notations pour désigner une permutation s élément de S_n. Une notation souvent utlisée est*

$$\begin{pmatrix} 1 & 2 & ... & n \\ s(1) & s(2) & ... & s(n) \end{pmatrix}$$

(Donner quelques exemples).

Remarque 1.15. *On peut ne pas écrire les points fixes de s i.e les i tels que $s(i) = i$. (Donner des exemples dans $s_{...}$.)*

Quelques calculs pratiques(Faire des calculs sur les composées, les inverses...

Définition 1.16. *Soit $p \in \mathbb{N}/0 \leq p \leq n$. On appelle p-cycle, toute permutation $\sigma \in S_n$ telle qu'il existe $x_1, x_2, ..., x_p \in \{x_1, x_2, ..., x_n\}$ deux à deux distincts tels que*

$$\sigma(x_1) = x_2, \sigma(x_2) = x_3, ..., \sigma(x_{p-1} = x_p, \sigma(x_p) = x_1$$
$$\forall \quad k \in \{x_1, x_2, ..., x_n\} \backslash \{x_1, ..., x_p\}, \sigma(k) = k.$$

L'ensemble $\{x_1, x_2, ..., x_p\}$ est appelé le support de σ et p est appelé la longueur de σ.

Propriété 1.17. *Card$(S_n) = n!$.*

Définition 1.18. *Soit $(G, *)$ un groupe. On appelle ordre d'un élément x de G, le plus petit entier naturel n strictement positif vérifiant $x^n = e_G$. Dans ce cas on note $O(x) = n$.*

Propriété 1.19. *Tout p-cycle est d'ordre p.*

Propriété 1.20. *Tout élément σ de S_n s'écrit de façon unique (à l'odre des facteurs près) comme produit de cycles de support disjoints. Ces cycles commutent entre eux et le ppcm des longueurs de ces derniers est l'ordre de la permutation σ.*

Définition 1.21. *On appelle transposition, tout 2-cycles c'est à dire une permutation qui échange deux éléments i et j $(i \neq j)$ et qui laisse fixe chacun des $n-2$ autres. On la note τ_{ij}. Ainsi*

$$\tau_{ij} = \begin{pmatrix} 1 & 2 & ...i & ...j & ... & n \\ 1 & 2 & ...j & ...i & ... & n \end{pmatrix}$$

Propriété 1.22. *Soit σ un p-cycle de S_n. On pose $\sigma = (a_1...a_p)$. Alrs σ se décompose en produit de $p-1$ transpositions. On a*

$$\sigma = (a_1a_2)(a_2a_3)...(a_{p-1}a_p).$$

Propriété 1.23. *Tout élément σ de S_n est oduit de transpositions.*

Exercice 1.24. *Trouve la décomposition en produit de transpositions de la permutation*

$$\sigma = \begin{pmatrix} 1 & 2 & 3 & 4 & 5 & 6 & 7 & 8 & 9 & 10 \\ 3 & 4 & 6 & 2 & 5 & 1 & 8 & 10 & 7 & 9 \end{pmatrix} \in S_{10}.$$

Définition 1.25. *On dit qu'un couple (i, j) présente une inversion pour $\sigma \in S_n$ lorsque $i < j$ et $\sigma(i) > \sigma(j)$.*

On note

$$I(\sigma) = card\{(i, j) \in E_n^2 / i < j \text{ et } \sigma(i) > \sigma(j)\}$$

le nom d'inversion de σ où E_n^2 est l'ensemble des pairs d'éléments de $\{1, 2, ..., n\}$.

Définition 1.26. *On appelle signature de $\sigma \in S_n$ le nombre noté $\Sigma(\sigma)$ défini par*

$$\Sigma(\sigma) = (-1)^{I(\sigma)}.$$

Propriété 1.27. *Si $\sigma \in S_n$ est le produit de p transpositions alors*

$$\Sigma(\sigma) = (-1)^p.$$

Exercice 1.28. *Déterminer de deux façons différentes la signature de la permutation*

$$\sigma = \begin{pmatrix} 1 & 2 & 3 & 4 & 5 & 6 & 7 & 8 & 9 & 10 \\ 3 & 4 & 6 & 2 & 5 & 1 & 8 & 10 & 7 & 9 \end{pmatrix} \in S_{10}.$$

1.3 Anneaux et corps

Définition 1.29. *Soit A un ensemble muni de deux lois de composition internes notées $+$ et $\times$. On dit que $(A, +, \times)$ est un anneau si*

—$(A, +)$ est un groupe commutatif

—la loi $\times$ est associative et distributive par rapport à l'addition

—Il existe un élément neutre pour la loi $\times$.

Propriété 1.30. *Soit $(A, +, \times)$ un anneau. L'ensemble des éléments de A qui sont inversibles pour le produit est un groupe pour la loi $\times$.*

1.3.1 Calcul dans les anneaux

Soit $(A, +, \times)$ un anneau, $n \in \mathbb{N}^*$ et $(a, b, c) \in A^3$.

—On note $a + (-b) = a - b$

—$na = a + a + ... + a$ (n fois).

Propriété 1.31. *Soit $(A, +, \times)$ un anneau, a et b deux éléments de A. On suppose que $ab = ba$. Alors*

—Pour tout $n \in \mathbb{N}^*$, on a :

$$a^n - b^n = (a - b)(\sum_{k=0}^{n-1} a^k b^{n-1-k})$$

. —*Pour tout* $n \in \mathbb{N}$ *on a :*

$$(a+b)^n = \sum_{k=0}^{n} \binom{n}{k} a^k b^{n-k}$$

Chapitre Deux

Arithmétique dans l'ensemble des entiers relatifs

Rappels 2.1. *1. Toute partie non vide de $\mathbb{N}$ admet un plus petit élément.*

2. Toute partie non vide et majoré de $\mathbb{Z}$ admet un plus grand élément.

3. Toute partie non vide et minorée de $\mathbb{Z}$ admet un plus petit élément.

2.1 Divisibilité et division euclidienne

Définition 2.2. *Soient a et b deux entiers relatifs.*

On dit que a est un multiple de b si et seulement s'il existe un entier q tel que $a = bq$.

Si $b \neq 0$ alors on dit que b divise a si et seulement si a est un multiple de b.

L'ensemble des diviseurs de a est noté $D(a)$ et l'ensemble des multiples de a est noté $a\mathbb{Z}$.

Proposition 2.3. *Soient a, b deux entiers relatifs non nuls et c un entier relatif.*

- *a divise a.*
- *Si a divise b et b divise c alors a divise c.*
- *Si a divise b et a divise c alors pour tout entiers relatifs p, q a divise $bp + cq$.(ici b peut être nul)*
- *Si a divise b alors $|a| \leq |b|$.*
- *Si a divise b et si b divise a alors $a = b$ ou $a = -b$.*

Théorème 2.4. *Soit a et b deux entiers relatifs avec $b \neq 0$. Il existe un unique couple $(q, r) \in \mathbb{Z} \times \mathbb{N}$ avec $0 \leq r < |b|$ tel que $a = bq + r$.*

2.2 PGCD et algorithme d'Euclide

Définition 2.5. *Soit a et b deux entiers relatifs non tous nuls. On appelle $PGCD$ de a et b et on $pgcd(a, b)$ ou $a \wedge b$ le plus grand élément $D(a) \cap D(b)$.*

Proposition 2.6. *Soient a et b deux entiers non tous nuls et k un entiers relatif non nul.*

1. $pgcd(a, b) = pgcd(|a|, |b|)$.
2. $pgcd(ka, kb) = |k| \, pgcd(a, b)$.

Proposition 2.7. *Soient a, b, q trois entiers relatifs.*

$$D(a) \cap D(b) = D(b) \cap D(a - bq).$$

Proposition 2.8. *Soita et b deux entiers naturels avec $b > 0$. Soit $a = bq + r$ la division euclidienne de a par b. Alors $D(a) \cap D(b) = D(b) \cap D(r)$.*

Proposition 2.9. *Soit a et b deux entiers relatifs non tous nuls. On pose $\delta = pgcd(a, b)$. $D(a) \cap D(b) = D(\delta)$.*

Proposition 2.10. *Soient a et b deux entiers relatifs dont l'un au moins est non nul. Alors il existe des entiers relatifs u_0 et v_0 tel que $a \wedge b = au_0 + bv_0$.*

Une telle égalité s'appelle une relation de Bézoutentre a et b. On dit que le couple (u_0, v_0) constitue un couple de coefficient du Bézout de a et b.

Corollaire 2.11. *Soient a et b deux entiers relatifs, dont l'un au moins est non nul. L'ensemble $\{au + bv / u \in \mathbb{Z}, v \in \mathbb{Z}\}$ est exactement égal à l'ensemble des multiples de $a \wedge b$.*

Définition 2.12. *Soient a et b deux entiers relatifs tous non nuls. On appelle ppcm de a et b et on note $ppcm(a, b)$ ou $a \vee b$ le plus petit élément de $a\mathbb{Z} \cap b\mathbb{Z} \cap \mathbb{N}^*$*

Proposition 2.13. *Soient a et b deux entiers relatifs tous non nuls. On a :*

$$a\mathbb{Z} \cap b\mathbb{Z} = (a \vee b)\mathbb{Z}.$$

Proposition 2.14. *Soient a, b et k trois entiers relatifs tous non nuls.*

$$(ka \vee kb) = |k| (a \vee b).$$

Proposition 2.15. *Soient a et b deux entiers relatifs tous non nuls. On a :*

$$ab = (a \wedge b)(a \vee b).$$

2.3 Entiers premiers entre eux

Définition 2.16. *Soient a et b deux entiers relatifs non tous nuls. On dit que a et b sont premiers entre eux si et seulement si $a \wedge b = 1$.*

Proposition 2.17. *Soient a et b deux entiers relatifs non tous nuls. a et b sont premiers entre eux si et seulement si il existe deux entiers u_0 et v_0 tels que $au_0 + bv_0 = 1$.*

Lemme 2.18 (Lemme de Gauss)**.** *a, b, c sont des entiers relatifs.*

Si a divise bc et si a et b sont premiers entre eux alors a divise c.

Proposition 2.19. *a, b, c sont trois entiers relatifs. Les deux propositions suivantes sont équivalentes :*

1. *L'entier a est premier avec l'entier b et avec l'entier c.*
2. *L'entier a est premier avec le produit bc.*

Proposition 2.20. *Soit a, b, c trois entiers relatifs. On a :*

- $(a \wedge b) \wedge c = a \wedge (b \wedge c)$
- $(a \vee b) \vee c = a \vee (b \vee c)$

Proposition 2.21 (Relation de Bézout)**.** *Soit a_1, a_2, ... a_n n entiers relatifs avec $n \geq 2$. On pose $d = pgcd(a_1, a_2, ..., a_n)$. Il existe n entiers relatifs u_1, u_2, ..., u_n tels que*

$$a_1u_1 + a_2u_2 + \cdots + a_nu_n = d$$

Définition 2.22. *Soit a_1, a_2, ... a_n n entiers relatifs avec $n \geq 2$.*
On dit que ces n entiers relatifs sont premiers entre eux si leur pgcd est égal à 1.

Proposition 2.23. *Soit a_1, a_2, ... a_n n entiers relatifs avec $n \geq 2$. Les deux propositions suivantes sont équivalentes :*

- *Les entiers a_1, a_2, ... a_n sont premiers entre eux.*
- *Il existe n entiers relatifs u_1, u_2, ..., u_n tels que $a_1u_1 + a_2u_2 + \cdots + a_nu_n = 1$.*

2.4 Nombres premiers

Définition 2.24. *Un entier naturel p est dit premier si $p \geq 2$ et si les seuls diviseurs de p dans $\mathbb{N}$ sont 1 et p.*

Proposition 2.25. *L'ensemble des nombres premiers est infini.*

Soit n un entier relatif non nul et p un entier premier. Il existe un plus grand entier naturel k tel que p^k divise n. Cet entier est noté $v_p(n)$ et est appelé valuation p-adique de n.

Proposition 2.26 (décomposition en produit de facteurs premiers)**.** *Soit n un entier naturel avec $n > 0$. Alors $n = \prod_{p \in \mathbb{P}} p^{\alpha_p}$ où sont dans $\mathbb{N}$ et tous non nuls sauf un nombre fini d'entre eux. Dans cette écriture, α_p est la valuation p-adique $v_p(n)$ de n.*

2.5 Congruences

Définition 2.27. *Soit $n \in \mathbb{N}^*$. Deux entiers relatifs x et y sont congrus modulo n si et seulement si n divise $x - y$. Dans ce cas, on note $x \equiv y \pmod{n}$.*

Proposition 2.28. *Soit n un entier naturel non nul, a, b, a', b' et c des entiers relatifs.*

- $a \equiv a \pmod{n}$
- $(a \equiv b \pmod{n}$ *et* $b \equiv c \pmod{n}) \Longrightarrow a \equiv c \pmod{n}$.
- $(a \equiv b \pmod{n}$ *et* $a' \equiv b' \pmod{n}) \Longrightarrow a + a' \equiv b + b' \pmod{n}$.
- $(a \equiv b \pmod{n}$ *et* $a' \equiv b' \pmod{n}) \Longrightarrow aa' \equiv bb' \pmod{n}$.
- *Les énoncés suivants sont équivalents*
  - $a \equiv b \pmod{n}$

– *le reste de la division euclidienne de a par n est le même que le que le reste de la division euclidienne de b par n.*

Proposition 2.29 (Petit théorème de Fermat)**.** *Soit p un nombre premier. Pour tout entier relatif a, on a :*

$$a^p \equiv a \pmod{p}.$$

En particulier, si p ne divise pas a alors

$$a^{p-1} \equiv 1 \pmod{p}.$$

Polynômes et fractions rationnelles

Dans ce chapitre $\mathbb{K}$ désigne un corps et plus précisement le corps $\mathbb{Q}$, $\mathbb{R}$ ou $\mathbb{C}$.

3.1 Anneau des polynômes à une indéterminée

Définition 3.1. *Soit n un entier naturel. Un polynôme à coefficients dans $\mathbb{K}$ est une expression de la forme*

$$P(X) = \sum_{i=0}^{n} a_i X^i$$

où les a_i pour $i \in \{0, ..., n\}$ sont des éléments de $\mathbb{K}$.

L'ensemble des polynômes est noté $\mathbb{K}[X]$.

- *Les a_i sont appelés les les coefficientsdu polynômes .*
- *Si tous coefficients sont nuls, P est appelé le polynôme nul, il est noté 0.*
- *On appelle le degré de P le plus grand entier i tel que $a_i \neq 0$; on le note deg$P$.Si k est le degré de P a_k est alors appelé le coefficient dominant et $a_k X^k$ est appelé le terme dominant de P. Si $a_i = 1$ alors P est dit unitaire. Pour le degré du polynôme nul on pose par convention $deg(0) = -\infty$.*
- *Un polynôme de la forme $P = a_0$ avec $a_0 \in \mathbb{K}$ est un polynôme constant. Si $a_0 \neq 0$, son degré est 0.*

Proposition 3.2. *On pose*

$$P = \sum_{i=0}^{n} a_i X^i \text{ et } Q(= \sum_{i=0}^{n} b_i X^i$$

où les a_i et b_i pour $i \in \{0, ..., n\}$ sont des éléments de $\mathbb{K}$.

- *Egalité.*

$$P = Q \Longleftrightarrow a_i = b_i \text{ pour touti.}$$

- *Addition.*

$$P + Q = \sum_{i=0}^{n} (a_i + b_i) X^i.$$

– *Multiplication.Si* $Q = \sum_{i=0}^{m} b_i X^i$ *alors*

$$P \times Q = \sum_{k=0}^{n+m} \left(\sum_{i+j=k} a_i b_j \right) X^k.$$

– *Multiplication par scalaire. Si* $\lambda \in \mathbb{K}$ *alorr* $\lambda \cdot P$ *est le polynôme dont le* i*-ème coefficient est* λa_i.

Proposition 3.3. *Pour* $P, Q, R \in \mathbb{K}[X]$ *alors*

– $0 + P = P, \quad P + Q = Q + P, \quad (P + Q) + R = P + (Q + R)$;

– $1 \cdot P = P \quad P \times Q = Q \times P, \quad (P \times Q) \times R = P \times (Q \times R)$;

– $P \times (Q + R) = P \times Q + P \times R$.

Proposition 3.4. *Soient* P *et* Q *deux polynômes à coefficients dans* $\mathbb{K}$.

$$deg(P \times Q) = degP + degQ.$$

$$deg(P + Q) \leq \max(degP, degQ).$$

3.2 Arithmétique des polynômes

3.2.1 Divisibilité et division euclidienne

Définition 3.5. *Soient* $A, B \in \mathbb{K}[X]$, *on dit que* B *divise* A *s'il existe* $Q \in \mathbb{K}[X]$ *tel que* $A = BQ$. *On note* $B \mid A$. *On dit aussi que* A *est un multiple de* B

Proposition 3.6. *Soient* $A, B, C \in \mathbb{K}[X]$.

– *Si* $A \mid B$ *et* $B \mid A$ *alors il existe* $\lambda \in \mathbb{K}^*$ *tel que* $A = \lambda B$.

– *Si* $A \mid B$ *et* $B \mid C$ *alors* $A \mid C$.

– *Si* $C \mid A$ *et* $C \mid B$ *alors* $C \mid (AU + BV)$, *pour tout* $U, V \in \mathbb{K}[X]$

Théorème 3.7. *Soient* $A, B\mathbb{K}[X]$ *avec* $B \neq 0$, *alors il existe un unique polynôme* Q *et un unique polynôme* R *tels que :*

$$A = BQ + R \text{ et } degR < degB$$

Q *est appelé le quotient et* R *le reste et cette écriture est la division euclidienne de* A *par* B.

3.2.2 Fonctions polynômiales- Racines- Dérivation

Définition 3.8. *Soit* $P = \sum_{i=0}^{n} a_i X^i \in \mathbb{K}[X]$. *Pour un élément* $x \in \mathbb{K}$, *on note* $P(x) = \sum_{i=0}^{n} a_i x^i$. *On associe ainsi au polynôme* P *une fonction polynôme*

$$P : \mathbb{K} \to \mathbb{K}, \quad x \mapsto P(X) = \sum_{i=0}^{n} a_i x^i$$

Définition 3.9. *Soit $P \in \mathbb{K}[X]$ et $a \in \mathbb{K}$. On dit que α est une racine (ou un zéro) de P si $P(\alpha) = 0$.*

Proposition 3.10.

$$P(\alpha) = 0 \Longleftrightarrow X - \alpha \text{ divise } P.$$

Théorème 3.11. *Soit $P \in \mathbb{K}[X]$ de degré $n \geq 1$. Alors P admet au plus n racines dans $\mathbb{K}$.*

Définition 3.12. *Soit $k \in \mathbb{N}^*$. On dit que α est une racine de multiplicité k de P si $(X-\alpha)^k$ divise P alors que $(X-\alpha)^{k+1}$ ne divise pas P Lorque $k = 1$ on parle d'une racine simple, lorsque $k = 2$ on parle de racine double, etc.*

Définition 3.13. *Soit $P(X) = \sum_{i=0}^{n} a_i X^i \in \mathbb{K}[X]$.*
Le polynôme $P'(X) = \sum_{i=1}^{n} i a_i X^{i-1} \in \mathbb{K}[X]$ est le polynôme dérivé de P.

Proposition 3.14. *Soient $P, Q \in \mathbb{K}[X]$, α, β deux éléments de $\mathbb{K}$ et n un entier naturel non nul. On a :*

- $(\alpha P + \beta Q)' = \alpha P' + \beta Q'$.
- $(PQ)' = P'Q + Q'P$.
- $(PQ)^n = \sum_{k=0}^{n} \binom{n}{k} P^{(n-k)} Q^{(k)}$. *C'est la formule de Leibniz.*

Proposition 3.15. *Les énoncés suivants sont équivalents :*

- *α est une racine de multiplicité k de P.*
- *Il existe $Q \in \mathbb{K}[X]$ tel que $P = (X - \alpha)Q$, avec $Q(\alpha) \neq 0$.*
- *$P(\alpha) = P'(\alpha) = \cdots = P^{(k-1)}(\alpha) = 0$ et $P^{(k)}(\alpha) \neq 0$*

3.2.3 PGCD et PPCM

Définition 3.16. *Soient $A, B \in \mathbb{K}[X]$ dont l'un au moins est non nul. Tout diviseur commun de A et B de degré maximal est appelé un $PGCD$ de A et B. Il existe un unique polynôme unitaire de plus grand degré qui divise à la fois A et B. Il est noté $PGCD(A, B)$ ou $A \wedge B$*

Proposition 3.17. *Soient $A, B \in \mathbb{K}[X]$ avec $B \neq 0$, Q et $R \in \mathbb{K}[X]$ tel que $A = BQ + R$ avec $degR < degB$. On a :*

$$PGCD(A, B) = PGCD(B, R)$$

Cette proposition justifie l'algorithme d'Euclide.

Proposition 3.18 (Algorithme d'Euclide)**.** *Soient $A, B \in \mathbb{K}[X]$ avec $B \neq 0$. On calcule les divisions euclidiennes successives,*

$$A = BQ_1 + R_1 \quad degR_1 < degB$$

$$B = R_1Q_2 + R_2 \quad degR_2 < degR_1$$

$$\vdots$$

$$R_{k-2} = R_{k-1}Q_k + R_k \quad degR_k < degR_{k-1}$$

$$R_{k-1} = R_kQ_{k+1}$$

Le degré du reste diminue à chaque division. On arrête l'algorithme lorsque le reste est nul. Le pgcd est le dernier reste non nul R_k rendu unitaire.

Définition 3.19. *Soient $A, B \in \mathbb{K}[X]$. On dit que A et B sont premiers entre eux si $pgcd(A, B) = 1$.*

Théorème 3.20 (Théorème de Bézout)**.** *Soient $A, B \in \mathbb{K}[X]$ avec $A \neq 0$ ou $B \neq 0$. On note $D = pgcd(A, B)$. Il existe deux polynômes $U, V \in \mathbb{K}[X]$ tels que $AU + BV = D$.*

Corollaire 3.21. *Soient A et B deux polynômes . A et B sont premiers entre eux s'il existe deux polynômes U et V tels que $AU + BV = 1$.*

Corollaire 3.22. *Soient $A, B, C \in \mathbb{K}[X]$ avec $A \neq 0$ ou $B \neq 0$. Si $C \mid A$ et $C \mid B$ alors $C \mid pgcd(A, B)$.*

Corollaire 3.23 (Lemme de Gauss)**.** *Soient $A, B, C \in \mathbb{K}[X]$. Si $A \mid BC$ et $pgcd(A, B) = 1$ alors $A \mid C$.*

Définition 3.24. *Soient $A, B \in \mathbb{K}[X]$ des polynômes non nuls. Il existe un unique polynôme unitaire M de plus petit degré tel que $A \mid M$ et $B \mid M$ Cet unique polynôme est appelé le ppcm de A et B qu'on note $ppcm(A, B)$ ou $A \vee B$.*

Proposition 3.25. *Soient $A, B \in \mathbb{K}[X]$ des polynômes non nuls et $M = ppcm(A, B)$. Si $C \in \mathbb{K}[X]$ est un polynôme tel que $A \mid C$ et $B \mid C$, alors $M \mid C$.*

3.2.4 Polynômes irréductibles

Théorème 3.26 (Théorème de d'Alembert-Gauss)**.** *Tout polynôme à coefficients complexes de degré $n > 0$ a au moins une racine dans $\mathbb{C}$. Il admet exactement n racines si on compte chaque racine avec multiplicité.*

Définition 3.27. *Soit $P \in \mathbb{K}[X]$ un polynôme de degré $n > 0$. On dit que P est irréductible si pour tout $Q \in \mathbb{K}[X]$ divisant P, alors, soit $Q \in \mathbb{K}^*$, soit il existe $\lambda \in \mathbb{K}^*$ tel que $Q = \lambda P$. Si P n'est pas irréductible alors on dit que P est réductible.*

Lemme 3.28. *Soit $P \in \mathbb{K}[X]$ un polynôme irréductible et soient $A, B \in \mathbb{K}[X]$. Si $P \mid AB$ alors $P \mid A$ ou $P \mid B$.*

Théorème 3.29. *Tout polynôme non constant $A \in \mathbb{K}[X]$ s'écrit comme un produit de polynômes irréductibles unitaires :*

$$A = \lambda P_1^{k_1} P_2^{k_2} \dots P_r^{k_r}$$

où $\lambda \in \mathbb{K}^*$, $r \in \mathbb{N}^*$ et les P_i sont des polynônes irréductibles distincts. De plus cette décomposition est unique à l'ordre des facteurs près.

Théorème 3.30. *Les polynômes irréductibles de $\mathbb{C}[X]$ sont les polynômes de degré 1.*

Ainsi, pour $P \in \mathbb{C}[X]$ de degré $n > 0$ la factorisation s'écrit $P = \lambda(X-\alpha_1)^{k_1}(X-\alpha_2)k_2\dots(X-\alpha_r)^{k_r}$, où $\alpha_1,\dots\alpha_r$ sont les racines distinctes de P et $k_1,\dots,k_r$ sont leurs multiplicités.

Théorème 3.31. *Les polynômes irréductibles de $\mathbb{R}[X]$ sont les polynômes de degré 1 ainsi que les polynômes de degré 2 ayant un discriminant $\Delta < 0$.*

Ainsi, pour $P \in \mathbb{R}[X]$ de degré $n > 0$ la factorisation s'écrit $P = \lambda(X-\alpha_1)^{k_1}(X-alpha_2)k_2\dots(X-\alpha_r)^{k_r}Q_1^{l_1}\dots Q_s^{l_s}$, où $\alpha_1,\dots\alpha_r$ sont les racines réelles distinctes de P et $k_1,\dots,k_r$ de multiplicités k_i et les Q_i sont des polynômes irréductibles de degré 2 : $Q_i = X^2+\beta_i X+\gamma_i$ avec $\Delta = \beta_i^2 - 4\gamma_i$.

3.2.5 Fractions rationnelles

Définition 3.32. *Une fraction rationnelle à coefficients dans $\mathbb{K}$ est une expression de la forme*

$$F = \frac{P}{Q}$$

où $P, Q \in \mathbb{K}[X]$ sont deux polynômes et $Q \neq 0$

Décomposition en éléments simples sur $\mathbb{C}$

Soit P/Q une fraction rationnelle avec $P, Q \in \mathbb{C}[X]$, $pgcd(P,Q) = 1$ et $Q = (X-\alpha_1)^{k_1}(X-\alpha_2)k_2\dots(X-\alpha_r)^{k_r}$ Alors il existe une et une seule écriture :

$$\begin{aligned}\frac{P}{Q} &= E + \tfrac{\alpha_{1,1}}{(X-\alpha_1)^{k_1}} + \tfrac{\alpha_{1,2}}{(X-\alpha_1)^{k_1-1}} + \dots + \tfrac{\alpha_{1,k_1}}{(X-\alpha_1)} \\ &\quad + \tfrac{\alpha_{2,1}}{(X-\alpha_2)^{k_2}} + \tfrac{\alpha_{2,2}}{(X-\alpha_2)^{k_2-1}} + \dots + \tfrac{\alpha_{2,k_2}}{(X-\alpha_2)} + \dots\end{aligned}$$

Le polynôme E s'appelle la partie polynomiale (ou partie entière). Les termes $\frac{\alpha}{(X-\alpha)^i}$ sont les éléments simples sur $\mathbb{C}$.

Décomposition en éléments simples sur $\mathbb{R}$

Soit P/Q une fraction rationnelle avec $P, Q \in \mathbb{R}[X]$, $pgcd(P,Q) = 1$. Alors P/Q s'écrit de manière unique comme somme :

- d'une partie polynomiale $E(X)$,
- d'éléments simples du type $\frac{a}{(X-\alpha)^i}$,
- d'éléments simples du type $\frac{ax+b}{(X^2+\alpha X+\beta)^i}$.

Où les $X-\alpha$ et $X^2+\alpha X+\beta$ sont les facteurs irréductibles de $Q(X)$ et les exposants i sont inférieurs ou égaux à la la puissance correspondante dans cette factorisation.

3.2.6 Quelques Théorèmes

Théorème 3.33 (Formule de taylor pour les polynômes). *Soit P un polynôme de $\mathbb{K}[X]$ de degré inférieur ou égal à d et c un élément de $\mathbb{K}$. Alors*

$$P(X) = P(c) + P'(c)(X-c) + \frac{P''(c)}{2}(X-c)^2 + \frac{P^{(3)}(c)}{3!}(X-c)^3 + \cdots + \frac{P^{(d)}(c)}{d!}(X-c)^d.$$

Ainsi, soient $c_1, \cdots, c_p$ des éléments de $\mathbb{K}$. Si c_i est une racine de multiplicité k_i de P, pour $i = 0, \cdots p$, alors $(X-c_1)^{k_1} \cdots (X-c_p)^{k_p}$ divise P.

Théorème 3.34 (Polynôme d'interpolation de Lagrange). *Soient $c_0, c_1, \cdots, c_n$ des éléments distincts de $\mathbb{K}$. Soient $a_0, a_1, \cdots, a_n$ des éléments de $\mathbb{K}$. Alors il existe un unique polynôme P de degré inférieur ou égal à n tel que $P(c_i) = a_i$ pour $i = 0, 1, \cdots, n$. Ce polynôme est donné par*

$$P(X) = \sum_{i=0}^{n} a_i \frac{\prod_{j \neq i}(X - c_j)}{\prod_{j \neq i}(c_i - c_j)}$$

Définition 3.35. *Un polynôme de degré $n > 0$ est dit scindé sur $\mathbb{K}$ s'il a exactement n racines comptées avec multiplicitÃ© dans $\mathbb{K}$*

Théorème 3.36. *Soit $P = a_0 + a_1X + \cdots + a_{n-1}X^{n-1} + X^n$ un polynôme unitaire de degré $n > 0$, scindé sur $\mathbb{K}$. Soit $c_1, \cdots, c_n$ ses racines comptées avec multiplicité. Alors*

$$\bullet\ a_{n-1} = \sum_{1 \leq i \leq n} c_i, \quad a_{n-2} = \sum_{1 \leq i_1 < i_2 \leq n} c_{i_1} c_{i_2}$$

$$\vdots$$

$$\vdots$$

$$\bullet\ (-1)^k a_{n-k} = \sum_{1 \leq i_1 < i_2 < \cdots < i_k \leq n} c_{i_1} c_{i_2} \cdots c_{i_k}$$

$$\bullet (-1)^n a_0 = c_1 c_2 \cdots c_n.$$

Autrement dit $(-1)^k a_{n-k}$ est la somme des produits k à k des racines. En particulier a_{n-1} est l'opposé de la somme des racines et $(-1)^n a_0$ est le produit des racines.