Chapitre 4 – Structures algébriques

1 Structure de groupe

1.1 Définitions et propriétés générales

1.1.1 Groupes et sous-groupes

Définition 1. Groupe
Soit un ensemble G muni d'une loi de composition interne notée $*$.
$(G, *)$ est un groupe si les trois propriétés suivantes sont vérifiées :

i. la loi $*$ est associative ;

ii. la loi $*$ admet un élément neutre dans G ;

iii. tout élément de G admet un symétrique dans G pour la loi $*$.

Si de plus la loi $*$ est commutative, le groupe G est dit commutatif (ou abélien).

Notations usuelles pour des lois dites additives ou multiplicatives :

i. lorsque la loi sur G est notée $+$ on parle de groupe additif, cela suppose toujours que cette loi $+$ est commutative, le neutre est alors en général noté 0 et pour un élément $a \in G$ le symétrique est noté $-a$, de plus pour un entier $n \in \mathbb{N}^*$ on note $\underbrace{a + \cdots + a}_{n \text{ fois}} = n\ a$;

ii. lorsque la loi sur G est notée $\cdot$ ou on parle de groupe multiplicatif, cela ne suppose pas que cette loi soit commutative, le neutre est alors en général noté e (ou 1) et pour un élément $a \in G$ le symétrique est noté a^{-1}, de plus pour un entier $n \in \mathbb{N}^*$ on note $\underbrace{a \cdot \cdots \cdot a}_{n \text{ fois}} = a^n$.

Proposition 1.
Dans un groupe, tout élément est simplifiable à gauche et à droite, i.e. :
si $(G, \cdot)$ est un groupe alors, pour tout $(a, b, c) \in G^3$, on a

$$(a.b = a.c) \Rightarrow (b = c) \quad et \quad (b.a = c.a) \Rightarrow (b = c)$$

Définition 2. Sous-groupe
Soit un groupe $(G, \cdot)$ et soit H une partie de G.
On dit que $(H, \cdot)$ est un sous-groupe de $(G, \cdot)$ (ou plus simplement que H est un sous-groupe de G si aucune confusion sur la loi n'est possible) si $(H, \cdot)$ est lui-même un groupe

Proposition 2.
Soit un groupe $(G, \cdot)$, une partie H de G est un sous-groupe de G si, et seulement, si les trois propriétés suivantes sont vraies :

i. H est non vide ;

ii. H est stable par la loi $\cdot$ (i.e. $\forall (x, x') \in H^2, x \cdot x' \in H$) ;

iii. H est stable par passage au symétrique (i.e. $\forall x \in H, x^{-1} \in H$).

Proposition 3. Intersection de sous-groupes
Soit un groupe $(G, \cdot)$ et soit $(H_i)_{i \in I}$ une famille de sous-groupes de G, $\bigcap_{i \in I} H_i$ est alors un sous-groupe de G.

Définition 3. Sous-groupe engendré par une partie
Soit un groupe $(G, \cdot)$ et soit A une partie de G. L'ensemble des sous-groupes de G contenant A admet un plus petit élément H, appelé sous-groupe de G engendré par A.

Notation : groupe engendré par un élément a (i.e par la partie $\{a\}$) ;

— dans un groupe G, le sous-groupe engendré par un élément a de G se note $\langle a \rangle$;

— si le groupe G est noté additivement on a donc $\langle a \rangle = \{na \mid n \in \mathbb{Z}\}$;

— si le groupe G est noté multiplicativement on a donc $\langle a \rangle = \{a^n \mid n \in \mathbb{Z}\}$;

Proposition 4. Sous-groupes de $\mathbb{Z}$
Les sous-groupes de $(\mathbb{Z}, +)$ sont exactement les sous-groupes engendrés par un élément, i.e les $\langle a \rangle = \{ka | k \in \mathbb{Z}\}$ pour $a \in \mathbb{Z}$.
Dans le cas de $\mathbb{Z}$, on note plus usuellement $a\mathbb{Z}$ ce sous-groupe $\{ak | k \in \mathbb{Z}\}$ engendré par a.

1.1.2 Groupe produit

Définition 4. Groupe produit
Soient deux groupes $(G, \diamond)$ et $(G', \vee)$.
On définit sur $G \times G'$ la loi de composition interne $\cdot$ par :

$$\forall (x, y) \in G^2, \forall \left(x', y'\right) \in G'^2, \left(x, x'\right) \cdot \left(y, y'\right) = \left(x \diamond y, x' \vee y'\right)$$

$(G \times G', \cdot)$ est alors un groupe appelé groupe produit de $(G, \diamond)$ et $(G', \vee)$.

1.2 Morphismes de groupes

1.2.1 Définitions et propriétés générales

Définition 5. Morphisme de groupes
Soient deux groupes $(G, \diamond)$ et $(G', \vee)$, on appelle morphisme (de groupe) de $(G, \diamond)$ dans $(G', \vee)$ toute application f de G dans G' telle que, pour tout $(x, y) \in G^2, f(x \diamond x') = f(x) \vee f(x')$

Vocabulaire :

— si f est un morphisme de G dans lui-même, on dit que f est en endomorphisme de G ;

— si f est un morphisme bijectif de G dans G', on dit que f est un isomorphisme de G dans G', sa réciproque f^{-1} est alors un morphisme de G' dans G ;

— si f est un isomorphisme de G dans lui-même, on dit que f est un automorphisme de G.

Proposition 5.
Soient deux groupes $(G, \cdot)$ et $(G', \cdot)$ de neutres e et e', et soit f un morphisme de G dans G', on a alors :

i. $f(e) = e'$;

ii. $\forall x \in G, f\left(x^{-1}\right) = f(x)^{-1}$;

iii. $\forall x \in G, \forall n \in \mathbb{N}, f\left(x^n\right) = f(x)^n$.

Proposition 6. Composition de morphismes
La composée de deux morphismes de groupes est un morphisme de groupes.

1.2.2 Noyau et image d'un morphisme de groupes

Proposition 7. image ou image réciproque d'un sous-groupe par un morphisme
Soient deux groupes $(G,\cdot)$ et $(G',\cdot)$ de neutres e et e', et soit f un morphisme de G dans G'.

- Soit H un sous-groupe de G, l'ensemble $f(H) = \{f(x)|x \in H\}$ est alors un sous-groupe de G'.
- Soit H' un sous-groupe de G', l'ensemble $f^{-1}(H') = \{x \in G|f(x) \in H'\}$ est alors un sous-groupe de G.

Définition 6. Noyau d'un morphisme de groupes
Soient deux groupes $(G,\cdot)$ et $(G',\cdot)$ de neutres e et e'.
Soit f un morphisme de G dans G', on appelle noyau de f et on note $\ker(f)$ le sous-groupe de G défini par :

$$\ker(f) = f^{-1}(\{e'\}) = \{x \in G|f(x) = e'\}$$

Proposition 8. Caractérisation de l'injectivité
Soient deux groupes $(G,\cdot)$ et $(G',\cdot)$ de neutres e et e' et soit f un morphisme de G dans G'.
Ce morphisme f est alors injectif si, et seulement si, $\ker(f) = \{e\}$.

Définition 7. Image d'un morphisme de groupes
Soient deux groupes $(G,\cdot)$ et $(G',\cdot)$.
Soit f un morphisme de G dans G', on appelle image de f et on note $Im(f)$ le sous-groupe de G' défini par :

$$Im(f) = f(G) = \{f(x)|x \in G\}$$

Proposition 9. Caractérisation de la surjectivité
Soient deux groupes $(G,\cdot)$ et $(G',\cdot)$ et soit f un morphisme de G dans G'.
Ce morphisme f est alors surjectif si, et seulement si, $Im(f) = G'$.

1.3 Groupes monogènes et groupes cycliques

1.3.1 Définitions

Définition 8. Groupe monogène et groupe cyclique
Un groupe $(G,\cdot)$ est dit :

- monogène s'il est engendré par un élément, i.e. s'il existe $a \in G$ tel que $G = \langle a\rangle = \{a^n|n \in \mathbb{Z}\}$;
- cyclique s'il est monogène et fini.

Proposition 10. Caractérisation des groupes cycliques parmi les groupes monogènes
Soit un groupe monogène $(G,\cdot)$ engendré par a et de neutre e, les trois propriétés suivantes sont alors équivalentes :

i. G est cyclique ;

ii. il existe deux entiers distincts m et n tels que $a^m = a^n$;

iii. il existe un entier non nul k tel que $a^k = e$.

Proposition 11. Écriture d'un groupe cyclique noté multiplicativement
Soit un groupe cyclique $(G,\cdot)$ engendré par a et de neutre e.
Soit $d = \min\left\{k \in \mathbb{N}^*|a^k = e\right\}$, G est alors de cardinal d et s'écrit :

$$G = \left\{e, a, \ldots, a^{d-1}\right\} = \left\{a^k|k \in [\![0, d-1]\!]\right\}.$$

1.3.2 Le groupe $(\mathbb{Z}/n\mathbb{Z}, +)$

Définition 9. groupe $(\mathbb{Z}/n\mathbb{Z}, +)$
Soit $n \in \mathbb{N}^*$, on note $\mathbb{Z}/n\mathbb{Z}$ l'ensemble des classes d'équivalence de la relation d'équivalence R définie sur $\mathbb{Z}$ par aRb lorsque $a \equiv b[n]$.
Pour tout $k \in \mathbb{Z}$, en notant $\bar{k}$ la classe d'équivalence de k, on a donc $\mathbb{Z}/n\mathbb{Z} = \left\{\bar{0}, \bar{1}, \ldots, \overline{n-1}\right\}$.
On définit alors sur $\mathbb{Z}/n\mathbb{Z}$ la loi de composition interne $+$ induite par la loi $+$ sur $\mathbb{Z}$, i.e. :

$$\forall (i,j) \in \mathbb{Z}^2,\ \bar{i} + \bar{j} = \overline{i+j}.$$

$(\mathbb{Z}/n\mathbb{Z}, +)$ est alors un groupe abélien de neutre $\bar{0}$.

Proposition 12. Générateurs de $\mathbb{Z}/n\mathbb{Z}$
Soit $n \in \mathbb{N}^*$, $\mathbb{Z}/n\mathbb{Z}$ est un groupe cyclique engendré par tout élément $\bar{k}$ tel que $k \wedge n = 1$.

Proposition 13. Caractérisation des groupes monogènes infinis et des groupes cycliques
Soit un groupe $(G, \cdot)$, alors :

- G est cyclique si, et seulement si, il existe $n \in \mathbb{N}^*$ tel que G soit isomorphe à $(\mathbb{Z}/n\mathbb{Z}, +)$;
- G est monogène infini si, et seulement si, G est isomorphe à $(\mathbb{Z}, +)$.

1.3.3 Ordre d'un élément

Définition 10. Élément d'ordre fini
Soit un groupe $(G, \cdot)$ et soit a un élément de G, on dit que a est d'ordre fini si le sous groupe engendré par a est fini, le cardinal de $\langle a \rangle$ est alors appelé ordre de cet élément a de G.

Proposition 14.
Soit un groupe $(G, \cdot)$ de neutre e et soit a un élément de G d'ordre fini égal à d, alors :

- $d = \min\{n \in \mathbb{N}^* | a^n = e\}$;
- pour tout entier n, on a l'équivalence suivante : $a^n = e \Leftrightarrow d|n$.

Théorème 1. Une version simple du théorème de Lagrange
Soit un groupe fini $(G, \cdot)$ de cardinal n.
Tout élément a de G est d'ordre fini et de plus cet ordre divise n.

2 Anneaux et corps

2.1 Définitions générales

Définition 11. Anneau
Soit un ensemble A muni de deux loi de composition interne notées $+$ et $\times$.
$(A, +, \times)$ est un anneau si les quatre propriétés suivantes sont vérifiées :

i. $(A, +)$ est un groupe abélien (dont on note l'élément neutre 0_A) ;

ii. la loi $\times$ est associative ;

iii. la loi $\times$ est distributive par rapport à la loi $+$;

iv. A admet un élément neutre pour la loi $\times$ (on note 1_A cet élément neutre).

Si de plus la loi $\times$ est commutative, A est dit être un anneau commutatif.

Proposition 15. Groupe des éléments inversibles
Soit un anneau $(A,+,\times)$, l'ensemble des éléments inversibles de A (i.e. admettant un symétrique pour $\times$) forme un groupe pour la loi $\times$ appelé groupe des éléments inversible de A.

Proposition 16. Règles de calcul dans un anneau
Soit un anneau $(A,+,\times)$, on a alors :

- $\forall a \in A, a \times 0_A = 0_A \times a = 0_A$;
- $\forall (a,b) \in A^2, a \times (-b) = (-a) \times b = -(a \times b)$;
- $\forall (a,b) \in A^2$ tels que $a \times b = b \times a$, $\forall n \in \mathbb{N}$:

$$(a+b)^n = \sum_{k=0}^{n} \binom{n}{k} a^k \times b^{n-k} \quad \text{et} \quad a^n - b^n = (a-b) \times \sum_{k=0}^{n-1} a^{n-1-k} \times b^k.$$

Définition 12. Anneau intègre
Un anneau non trivial $(A,+,\times)$ est dit intègre s'il n'admet aucun diviseur de 0, i.e :

$$\forall (a,b) \in A^2, a \times b = 0_A \Rightarrow (a = 0_A \text{ ou } b = 0_A) \ .$$

Définition 13. Corps
On appelle corps tout anneau non trivial $(A,+,\times)$ commutatif et tel que tout élément non nul de A admette un symétrique pour la loi $\times$.

Définition 14. Sous-anneau et sous-corps
Soit un anneau $(A,+,\times)$ et soit B une partie de A, on dit que B est un sous anneau de A si $(B,+,\times)$ est lui-même un anneau.
Soit un corps $(\mathbb{K},+,\times)$ et soit B une partie de $\mathbb{K}$, on dit que B est un sous anneau de $\mathbb{K}$ si $(B,+,\times)$ est lui-même un corps.

Proposition 17. Caractérisation

- Soit un anneau $(A,+,\times)$ et soit B une partie de A, B est alors un sous anneau de A si et seulement si B contient 1 et est stable par $+$, par passage à l'opposé et par $\times$.
- Soit un corps $(\mathbb{K},+,\times)$ et soit B une partie de $\mathbb{K}$, B est alors un sous-corps de $\mathbb{K}$ si et seulement si B contient 1 et est stable par $+$, par passage à l'opposé, par $\times$ et par passage à l'inverse de tout élément non nul.

Définition 15. Anneau produit
Soient deux anneaux $(A,+,\times)$ et $(A',+,\times)$.
On définit sur $A \times A'$ les lois de composition interne $+$ et $\times$ par :

$$\forall (x,y,x',y') \in A^2 \times A'^2, \begin{cases} (x,x') + (y,y') = (x+y, x'+y') \\ (x,x') \times (y,y') = (x \times y, x' \times y') \end{cases}$$

$(A \times A', +, \times)$ est alors un anneau d'élément nul $(0_A, 0_{A'})$ et d'élément unité $(1_A, 1_{A'})$, cet anneau est appelé anneau produit de A et A' .

2.2 Morphismes d'anneaux

Définition 16. Morphisme d'anneaux
Soient deux anneaux $(A,+,\times)$ et $(A',+,\times)$, et soit f une application de A dans A'.
On dit que f est un morphisme d'anneaux de A dans A' si :

$$f(1_A) = 1_{A'} \quad et \quad \forall (x,y) \in A^2, \begin{cases} f(x+y) = f(x) + f(y) \\ f(x \times y) = f(x) \times f(y) \end{cases}$$

.

2.3 Idéaux

2.3.1 Définition et propriétés générales

Définition 17. Idéal d'un anneau commutatif
Soit un anneau commutatif $(A,+,\times)$, on appelle idéal de A toute partie I de A qui vérifie les deux conditions suivantes :

i. $(I,+)$ est un sous-groupe de $(A,+)$;

ii. I est stable par produit **externe** i.e. : $\forall a \in I, \forall x \in A, a \times x \in I$.

Proposition 18. Intersection d'idéaux
Soit un anneau commutatif $(A,+,\times)$, l'intersection de toute famille d'idéaux de A est un idéal de A.

Proposition 19. Somme d'idéaux
Soit un anneau commutatif $(A,+,\times)$ et soient I et J deux idéaux de A.
On note $I + J = \{a, b \mid a \in I, b \in J\}$.
Alors $I + J$ est le plus petit idéal de A qui contienne I et J.

Définition 18. Idéal engendré par un élément
Soit un anneau commutatif $(A,+,\times)$ et soit un élément a de A, alors l'ensemble $a \times A = \{a \times x | x \in A\}$ est un idéal de A appelé idéal engendré par a, c'est le plus petit idéal de A contenant a.

Proposition 20. Noyau d'un morphisme d'anneaux
Soit f un morphisme d'anneau de l'anneau $(A,+,\times)$ dans l'anneau $(A',+,\times)$, le noyau de f est alors un idéal de A.

2.3.2 Idéaux de $\mathbb{Z}$

Proposition 21. Idéaux de $\mathbb{Z}$
Les idéaux de $(\mathbb{Z},+,\times)$ sont exactement les parties de la forme $a\mathbb{Z} = \{ak | k \in \mathbb{Z}\}$ pour $a \in \mathbb{N}$.

2.3.3 Divisibilité et idéaux dans un anneau commutatif intègre

Définition 19. Divisibilité
Soit un anneau commutatif intègre $(A,+,\times)$ et soient a et b deux éléments de A.
On dit que a divise b s'il existe un élément q de A tel que $a \times q = b$.

Proposition 22. Interprétation de la divisibilité en termes d'idéaux
Soit un anneau commutatif intègre $(A,+,\times)$ et soient a et b deux éléments de A, alors :

$$a \text{ divise } b \text{ si, et seulement si, } b \times A \subset a \times A.$$

Proposition 23. PGCD et PPCM dans $\mathbb{Z}$
Soient a et b dans $\mathbb{Z}$

i. Pour $(a,b) \neq (0,0)$, le PGCD de a et b est l'unique élément d de $\mathbb{N}^*$ qui engendre l'idéal $a\mathbb{Z} + b\mathbb{Z}$.

ii. Le PPCM de a et b est l'unique élément m de $\mathbb{N}$ qui engendre l'idéal $a\mathbb{Z} \cap b\mathbb{Z}$.

2.4 L'anneau $\mathbb{Z}/n\mathbb{Z}$

2.4.1 Définition

Définition 20. Anneau $(\mathbb{Z}/n\mathbb{Z}, +, \times)$
Soit $n \in \mathbb{N}^*$, on définit sur $\mathbb{Z}/n\mathbb{Z}$ la loi de composition interne $\times$ par :

$$\forall (i,j) \in \mathbb{Z}^2, \bar{i} \times \bar{j} = \overline{i \times j}.$$

$(\mathbb{Z}/n\mathbb{Z}, +, \times)$ est alors un anneau commutatif.

Proposition 24. Inversibilité dans $\mathbb{Z}/n\mathbb{Z}$
Les éléments inversibles de $\mathbb{Z}/n\mathbb{Z}$ sont exactement les $\bar{k}$ pour $k \in \mathbb{Z}$ premier avec n.

Corollaire 1.
$(\mathbb{Z}/n\mathbb{Z}, +, \times)$ est un corps si et seulement si n est un nombre premier.

Notation : pour p nombre premier, le corps $(\mathbb{Z}/p\mathbb{Z}, +, \times)$ est noté $\mathbb{F}_p$.

2.4.2 Arithmétique

Théorème 2. Théorème chinois
Soient deux entiers m et n premiers entre eux.
On définit l'application suivante (où $\bar{k}^{[j]}$ est la classe d'équivalence de k modulo j) :

$$\begin{array}{rccc} \varphi : & \mathbb{Z}/mn\mathbb{Z} & \to & (\mathbb{Z}/m\mathbb{Z}) \times (\mathbb{Z}/n\mathbb{Z}) \\ & \bar{k}^{[mn]} & \mapsto & (\bar{k}^{[m]}, \bar{k}^{[n]}) \end{array}$$

Cette application φ est alors un isomorphisme d'anneaux de $\mathbb{Z}/mn\mathbb{Z}$ dans $(\mathbb{Z}/m\mathbb{Z}) \times (\mathbb{Z}/n\mathbb{Z})$.

Corollaire 2. Interprétation en terme de système de congruences
Soient m et n des entiers premiers entre eux et soit $(a,b) \in \mathbb{Z}^2$.
Il existe alors un unique q dans $[\![0, mn-1]\!]$ tel que $\begin{cases} q \equiv a[m] \\ q \equiv b[n] \end{cases}$.
On a de plus : $\forall p \in \mathbb{Z}, \begin{cases} p \equiv a[m] \\ p \equiv b[n] \end{cases} \Leftrightarrow p \equiv q[mn]$.

Définition 21. Indicatrice d'Euler
On définit sur $\mathbb{N}^*$ la fonction φ , dite indicatrice d'Euler, par :

$$\forall n \in \mathbb{N}^*, \varphi(n) = card\{k \in [\![1,n]\!] | k \wedge n = 1\}.$$

Proposition 25.
Soient m et n deux entiers premiers entre eux, on a alors : $\varphi(mn) = \varphi(m)\varphi(n)$

Proposition 26.
Soit p un nombre premier et soit $k \in \mathbb{N}^*$ alors $\varphi(p^k) = p^k - p^{k-1}$.

Corollaire 3.
Soit un entier n supérieur ou égal à 2 dont la décomposition en produit de facteurs premiers est $n = p_1^{\alpha_1} \cdots p_q^{\alpha_q}$
On a alors $\varphi(n) = (p_1^{\alpha_1} - p_1^{\alpha_1 - 1}) \cdots (p_q^{\alpha_q} - p_q^{\alpha_q - 1}) = n\left(1 - \frac{1}{p_1}\right) \cdots \left(1 - \frac{1}{p_q}\right)$

Théorème 3. Théorème d'Euler
Soit $n \in \mathbb{N}^*$ et soit $a \in \mathbb{Z}$ premier avec n, on a alors : $a^{\varphi(n)} \equiv 1[n]$

3 Polynômes à une indéterminée

Dans tout cette partie 3, $\mathbb{K}$ est un corps qui selon le programme doit-être un un sous-corps de $\mathbb{C}$ (par exemple $\mathbb{R}$ ou $\mathbb{Q}$), ce qui a parfois beaucoup d'importance.

3.1 Généralités

Les polynômes de $\mathbb{K}[X]$ sont définis comme ceux de $\mathbb{R}[X]$ ou $\mathbb{C}[X]$: un polynôme $P \in \mathbb{K}[X]$ est une suite presque nulle (i.e. nulle à partir d'un certain rang) $(a_k)_{k\in\mathbb{N}}$ qu'on note usuellement $P = \sum_{k=0}^{+\infty} a_k X^k$ ou $P = \sum_{k=0}^{n} a_k X^k$ à condition que : $\forall k > n, a_k = 0$.

On a sur $\mathbb{K}[X]$ de la même manière que sur $\mathbb{R}[X]$ et $\mathbb{C}[X]$ les notions fondamentales suivantes.

— Les lois de composition interne $+$ et $\times$ confèrent à $(\mathbb{K}[X], +, \times)$ une structure d'anneau commutatif **intègre**.

— Le produit par un scalaire confère à $(\mathbb{K}[X], +, .)$ une structure de $\mathbb{K}$–espace vectoriel (qui nous intéresse peu dans ce chapitre).

— La notion de degré et les règles correspondantes (degré d'un produit, d'une composée, d'une somme).

— La notion de polynôme dérivé :

Pour $P = \sum_{k=0}^{+\infty} a_k X^k$ on définit son polynôme dérivé noté P'

$P' = \sum_{k=1}^{+\infty} k a_k X^{k-1} = \sum_{k=0}^{+\infty} (k+1) a_{k+1} X^k$.

On peut itérer ce principe pour définir, pour tout $j \in \mathbb{N}$, le polynôme $P^{(j)}$:

$P^{(j)} = \sum_{k=j}^{+\infty} k(k-1)\ldots(k-(j-1)) a_k X^{k-j} = \sum_{k=0}^{+\infty} \frac{(k+j)!}{k!} a_{k+j} X^k$.

— La notion de fonction polynomiale associée :

à $P = \sum_{k=0}^{+\infty} a_k X^k$ on associe la fonction $\widetilde{P}$ de $\mathbb{K}$ dans $\mathbb{K}$ définie par

$\widetilde{P} : \alpha \mapsto \widetilde{P}(\alpha) = \sum_{k=0}^{+\infty} a_k \alpha^k$.

Sur un corps infini, notamment sur un sous-corps de $\mathbb{C}$, on identifie usuellement P et $\widetilde{P}$ ce qui est légitime comme on le verra plus bas.

3.2 Divisibilité dans $\mathbb{K}[X]$

• Comme dans tout anneau, pour A et B dans $\mathbb{K}[X]$ on dit que A divise B (ou que B est un multiple de A) s'il existe $Q \in \mathbb{K}[X]$ tel que $B = QA$.

En termes d'idéaux on a : $A|B \Leftrightarrow B \in A\mathbb{K}[X] \Leftrightarrow B\mathbb{K}[X] \subset A\mathbb{K}[X]$.

• $\mathbb{K}[X]$ est muni d'une division euclidienne : pour A et B dans $\mathbb{K}[X]$ avec $A \neq 0$, il existe un unique couple $(Q, R) \in \mathbb{K}[X]$ tel que $\begin{cases} B = AQ + R \\ \text{et} \\ \deg(R) < \deg(A) \end{cases}$.

Avec ces notations : $A \mid B \Leftrightarrow R = 0$.

• Deux polynômes A et B sont dits associés s'ils se divisent mutuellement ($A \mid B$ et $B \mid A$) ce qui équivaut à l'existence de $\lambda \in \mathbb{K}^*$ tel que $A = \lambda B$.

Deux polynômes associés sont substituables l'un à l'autre pour la divisibilité : ils ont les mêmes diviseurs et les mêmes multiples.

A et B sont donc associés si, et seulement si, ils engendrent le même idéal (i.e. $A\mathbb{K}[X] = B\mathbb{K}[X]$).

• Deux polynômes A et B sont dits premiers entre eux si leurs seuls diviseurs communs sont les polynômes constants non nuls.

3.3 Racines

• Pour $a \in \mathbb{K}$ et $A \in \mathbb{K}[X]$ on dit que a est racine de A si $X - a$ divise A.

On a alors : a est racine de A si, et seulement si, $\widetilde{A}(a) = 0$;

• Pour a racine de A on appelle ordre de multiplicité de a la valeur $\alpha = \max\left\{k \in \mathbb{N} | (X-a)^k \text{ divise} A\right\}$ (égal à $+\infty$ si cet ensemble n'est pas majoré).

On rappelle alors la formule de Taylor et la caractérisation de l'ordre de multiplicité qui en découle.

Proposition 27. valide pour $\mathbb{K}$ sous-corps de $\mathbb{C}$ mais pas en toute généralité
Soit $P \in \mathbb{K}[X]$ et soit $a \in A$, alors :

i. $P = \sum_{k=0}^{+\infty} \frac{\widetilde{P}^{(k)}(a)}{k!}(X-a)^k$

ii. a est racine de P d'ordre de multiplicité k si et seulement si $\begin{cases} \forall j \in [\![0, k-1]\!], \widetilde{P}^{(j)}(a) = 0 \\ \text{et} \\ \widetilde{P}^{(k)}(a) \neq 0 \end{cases}$

3.4 Idéaux de $\mathbb{K}[X]$ et arithmétique dans $\mathbb{K}[X]$

Proposition 28.
Les idéaux de $\mathbb{K}[X]$ sont exactement les $P\mathbb{K}[X] = \{PQ | Q \in \mathbb{K}[X]\}$ où $P \in \mathbb{K}[X]$.

Proposition 29. Définition du PGCD
Soit A et B dans $\mathbb{K}[X]$ non tous les deux nuls.
Soit I l'idéal somme des idéaux engendrés par A et B :
$I = A\mathbb{K}[X] + B\mathbb{K}[X] = \{AQ + BR | (Q,R) \in \mathbb{K}[X]^2\}$.
Alors :

i. I est un idéal non trivial de $\mathbb{K}[X]$;

ii. l'unique polynôme unitaire engendrant I est appelé P.G.C.D. de A et B, il est noté $A \wedge B$;

iii. $D = A \wedge B$ est l'unique polynôme unitaire vérifiant l'équivalence :

$$\forall P \in \mathbb{K}[X], (P|A \text{ et } P|B) \Leftrightarrow P|D.$$

iv. $A \wedge B$ est le polynôme unitaire de plus grand degré diviseur à la fois de A et de B.

Proposition 30. Relation de Bezout
Soit A et B dans $\mathbb{K}[X]$ non tous les deux nuls.

i. Soit $C = A \wedge B$, il existe alors U et V dans $\mathbb{K}[X]$ tels que $AU + BV = C$.

ii. Les polynômes A et B sont premiers entre eux si, et seulement, si il existe U et V dans $\mathbb{K}[X]$ tels que $AU + BV = 1$.

Proposition 31. Lemme de Gauss
Soient A et B deux polynômes de $\mathbb{K}[X]$ premiers entre eux, alors :

$$\forall C \in \mathbb{K}[X], A|BC \Rightarrow A|C \ .$$

Proposition 32.
Soient A, B et C trois polynômes de $\mathbb{K}[X]$ alors C est premier avec A et avec B si, et seulement si, C est premier avec AB

3.5 Polynômes irréductibles

3.5.1 Définition et propriétés

Définition 22.
Un polynôme P de $\mathbb{K}[X]$ est dit irréductible s'il est de degré supérieur ou égal à 1 et s'il n'admet comme diviseurs que les polynômes constants non nuls et les polynômes qui lui sont associés.

Proposition 33.
Dans $\mathbb{K}[X]$, deux polynôme irréductibles non associés sont premiers entre eux.

Proposition 34.
Tout polynôme P de $\mathbb{K}[X]$ de degré 1 est irréductible.

3.5.2 Lien aux racines

Théorème 4.
Dans $\mathbb{K}[X]$, tout polynôme P non nul admet un nombre fini de racines.
Plus précisément, la somme des ordres de multiplicité des racines de $P \in \mathbb{K}[X] \setminus \{0\}$ est inférieure ou égale au degré de P.

Corollaire 4.

i. Soit $n \in \mathbb{N}$, tout polynôme de $\mathbb{K}_n[X]$ admettant strictement plus de n racines est nul.

ii. Tout polynôme de $\mathbb{K}[X]$ admettant une infinité de racines est nul.

Corollaire 5.
Si $\mathbb{K}$ est infini l'application qui à un polynôme P de $\mathbb{K}[X]$ associe sa fonction polynomiale associée $\widetilde{P}$ est injective.
On peut donc identifier les polynômes et leurs fonctions polynomiales associées.

3.5.3 Décomposition en produit de facteurs irréductibles

Théorème 5.
Tout polynôme P de $\mathbb{K}[X]$ de degré supérieur ou égal à 1 admet une unique décomposition en produit de facteurs irréductibles.

3.5.4 Cas de $\mathbb{C}$

Théorème 6. Théorème de d'Alembert–Gauss
Tout polynôme non constant de $\mathbb{C}[X]$ admet au moins une racine.

Corollaire 6.

i. Les éléments irréductibles de $\mathbb{C}[X]$ sont exactement les polynômes de degré 1.

ii. Tout polynôme non constant de $\mathbb{C}[X]$ est scindé sur $\mathbb{C}$, i.e. s'écrit comme un produit de facteurs de degré 1.

3.5.5 Cas de $\mathbb{R}$

Proposition 35.
Les éléments irréductibles de $\mathbb{R}[X]$ sont exactement les polynômes de degré 1 et les polynômes de degré 2 de discriminant strictement négatif.

Corollaire 7.
Tout polynôme non nul $P \in \mathbb{R}[X]$ admet une unique décomposition de la forme

$$P = \lambda \prod_{k=1}^{q} (X - a_k)^{\alpha_k} \prod_{k=1}^{r} (X^2 + b_k X + c_k)^{\beta_k}$$

où : $\lambda \in \mathbb{R}^*$; $(q, r) \in \mathbb{N}^2$;
$\forall k \in [\![1, q]\!], a_k \in \mathbb{R}, \alpha_k \in \mathbb{N}^*$;
$\forall k \in [\![1, r]\!], (b_k, c_k) \in \mathbb{R}^2, b_k^2 - 4c_k^2 < 0, \beta_k \in \mathbb{N}^*$.

4 Algèbres

Définition 23. Algèbre
Soit un $\mathbb{K}$–espace vectoriel $(A, +, .)$ et soit $\times$ une loi de composition interne sur A telle que :

i. $(A, +, \times)$ est un anneau ;

ii. $\forall \lambda \in \mathbb{K}, \forall (x, y) \in A^2$, $\lambda.(x \times y) = (\lambda.x) \times y = x \times (\lambda.y)$.

$(A, +, ., \times)$ est alors dit être une $\mathbb{K}$–algèbre.

Définition 24. Sous-algèbre
Soit une $\mathbb{K}$–algèbre $(A, +, ., \times)$ et soit B une partie de A, on dit que B est une sous-algèbre de A si $(B, +, ., \times)$ est une algèbre.

Définition 25. Morphisme d'algèbres
Soient deux $\mathbb{K}$–algèbres $(A, +, ., \times)$ et $(A', +, ., \times)$ et soit f une application de A dans A', on dit que f est un morphisme d'algèbres si les deux conditions suivantes sont satisfaites :

i. f est un morphisme d'anneaux de $(A, +, \times)$ dans $(A', +, \times)$;

ii. f est une application linéaire de $(A, +, .)$ dans $(A', +, .)$.