

STRUCTURES

B. Landelle

Table des matières

I	Structure de groupe	2
1	Définition, propriétés	2
2	Sous-groupe	3
3	Morphismes de groupes	3
II	Structure d'anneaux	4
1	Définition, propriétés	4
2	Groupe des inversibles	5
3	Idéaux d'un anneau commutatif	6
4	Divisibilité dans un anneau commutatif intègre	7
III	Anneau de polynômes à une indéterminée	7
1	Idéaux de $(\mathbb{K}[X], +, \times)$	7
2	Plus grand commun diviseur	8
3	Polynômes premiers entre eux	9
4	Irréductibles	11
IV	Algèbres	12
1	Définition	12
2	Sous-algèbre	12
3	Morphisme d'algèbres	13

Avertissement : Ce chapitre ne constitue qu'un bref aperçu des notions d'algèbre générale au programme, le strict minimum pour introduire les notions utiles au chapitre de **Réduction** (idéaux, morphismes d'algèbres). Les structures de groupes et anneaux seront étudiées plus en détail dans des chapitres ultérieurs.

Dans ce qui suit, le corps des scalaires $\mathbb{K}$ est $\mathbb{R}$ ou $\mathbb{C}$.

I Structure de groupe

1 Définition, propriétés

Définition 1. On appelle groupe un couple $(G, \star)$ avec G un ensemble (non vide) et $\star$ une loi de composition interne sur G vérifiant :

1. la loi $\star$ est associative, i.e.

$$\forall (a, b, c) \in G^3 \quad (a \star b) \star c = a \star (b \star c)$$

2. la loi $\star$ admet un élément neutre (souvent noté e), i.e.

$$\exists e \in G \quad | \quad \forall x \in G \quad e \star x = x = x \star e$$

3. tout élément de G admet un symétrique, i.e.

$$\forall x \in G \quad \exists y \in G \quad | \quad x \star y = e = y \star x$$

Si la loi $\star$ est commutative, la groupe est dit abélien ou commutatif.

Remarque : L'associativité signifie que l'on met les parenthèse où bon nous semble.

Proposition 1. Soit $(G, \star)$ un groupe. On a :

1. tout élément x de G admet un unique symétrique noté x^{-1} et $(x^{-1})^{-1} = x$;
2. l'élément neutre est unique et est son propre symétrique ;
3. $\forall (x, y) \in G^2 \quad x \star y = e \quad \text{ou} \quad y \star x = e \implies y = x^{-1}$;
4. $\forall (x, y) \in G^2 \quad (x \star y)^{-1} = y^{-1} \star x^{-1}$;
5. $\forall (x, y) \in G^2 \quad x \star y = y \star x \implies x^{-1} \star y = y \star x^{-1}$.

Démonstration. 1. Soit $x \in G$ et y des z des symétriques de x . On a par associativité

$$z = (y \star x) \star z = y \star (x \star z) = y$$

2. Soient e et u éléments neutres de G . On a

$$u = u \star e \quad \text{et} \quad u \star e = e$$

d'où $u = e$ et $e \star e = e$.

3. Soit $(x, y) \in G^2$ tel que $x \star y = e$. On a

$$y = (x^{-1} \star x) \star y = x^{-1} \star (x \star y) = x^{-1}$$

De même pour l'autre sens.

4. Soit $(x, y) \in G^2$. Par associativité, on a

$$(x \star y) \star (y^{-1} \star x^{-1}) = x \star (y \star y^{-1}) \star x^{-1} = x \star x^{-1} = e$$

5. Soit $(x, y) \in G^2$ tel que $x \star y = y \star x$. On opère à droite et à gauche par x^{-1} et il vient

$$x^{-1} \star (x \star y) \star x^{-1} = y \star x^{-1} = x^{-1} \star (y \star x) \star x^{-1} = x^{-1} \star y$$

□

Notations : En général, on note $(G, +)$ un groupe abélien, l'élément neutre 0 et $-x$ le symétrique de x . On note $(G, \times)$ un groupe non abélien, l'élément neutre 1 et x^{-1} le symétrique de x .

Exemples : $(\mathbb{Z}, +)$ est un groupe abélien, $(\mathbb{R}^*, \times)$ est un groupe abélien, $(GL_n(\mathbb{K}), \times)$ avec $n > 1$ est un groupe non commutatif.

2 Sous-groupe

Définition 2. On appelle sous-groupe d'un groupe $(G, \star)$ une partie H de G vérifiant

1. $e \in H$,
2. $\forall (x, y) \in H^2 \quad x \star y^{-1} \in H$.

Remarque : Il est parfois judicieux de séparer la deuxième propriété en vérifiant

$$\forall x \in H \quad x^{-1} \in H \quad \text{et} \quad \forall (x, y) \in H^2 \quad x \star y \in H$$

Exemples : Pour n entier, $n\mathbb{Z}$ est un sous-groupe de $(\mathbb{Z}, +)$.

Proposition 2. Soit H un sous-groupe de $(G, \star)$. Alors $(H, \star)$ possède une structure de groupe.

Démonstration. Immédiate. □

Remarque : En pratique, pour vérifier la structure de groupe d'un ensemble (pour la loi induite), on cherche en général à établir que celui-ci est sous-groupe d'un groupe connu.

3 Morphismes de groupes

Définition 3. Soient $(G_1, \star_1)$ et $(G_2, \star_2)$ des groupes. On appelle morphisme du groupe $(G_1, \star_1)$ vers le groupe $(G_2, \star_2)$ une application $\varphi : G_1 \rightarrow G_2$ vérifiant

$$\forall (x, y) \in G_1^2 \quad \varphi(x \star_1 y) = \varphi(x) \star_2 \varphi(y)$$

Proposition 3. Soit φ un morphisme du groupe $(G_1, \star_1)$ vers le groupe $(G_2, \star_2)$. On a

$$\varphi(e_1) = e_2 \quad \text{et} \quad \forall x \in G_1 \quad \varphi(x^{-1}) = \varphi(x)^{-1}$$

Démonstration. On a $\varphi(e_1) = \varphi(e_1 \star_1 e_1) = \varphi(e_1) \star_2 \varphi(e_1) \implies \varphi(e_1) = e_2$

Puis $\forall x \in G_1 \quad e_2 = \varphi(e_1) = \varphi(x \star_1 x^{-1}) = \varphi(x) \star_2 \varphi(x^{-1})$

□

Théorème 1. Soit φ morphisme du groupe $(G_1, \star_1)$ vers le groupe $(G_2, \star_2)$. Le noyau $\text{Ker } \varphi = \varphi^{-1}(\{e_2\})$ du morphisme de groupes φ est un sous-groupe de $(G_1, \star_1)$.

Démonstration. On a $\varphi(e_1) = e_2$ et pour $(x, y) \in \varphi^{-1}(\{e_2\})$, on a

$$\varphi(x \star_1 y^{-1}) = e_2 \star_2 e_2^{-1} = e_2$$

d'où le résultat. □

Exemple : L'ensemble $SL_n(\mathbb{K}) = \{M \in \mathcal{M}_n(\mathbb{K}) \mid \det(M) = 1\}$ muni de la loi $\times$ est un groupe. L'application $\varphi : (GL_n(\mathbb{K}), \times) \rightarrow (\mathbb{K}^*, \times), M \mapsto \det(M)$ est un morphisme de groupes. Ainsi, le noyau $SL_n(\mathbb{K}) = \text{Ker } \varphi$ est un sous-groupe de $(GL_n(\mathbb{K}), \times)$.

II Structure d'anneaux

1 Définition, propriétés

Définition 4. On appelle anneau un triplet $(A, +, \times)$ avec A un ensemble (non vide) muni de deux lois de composition interne $+$ et $\times$ telles que :

1. $(A, +)$ est un groupe abélien de neutre 0_A ;
2. $\times$ est associative ;
3. $\times$ possède un neutre 1_A ;
4. $\times$ est distributive sur $+$, i.e.

$$\forall (x, y, z) \in A^3 \quad x(y + z) = xy + xz \quad \text{et} \quad (x + y)z = xz + yz$$

Si la loi $\times$ est commutative, l'anneau $(A, +, \times)$ est dit commutatif.

Exemples : $(\mathbb{K}, +, \times)$, $(\mathbb{K}[X], +, \times)$ sont des anneaux commutatifs.

$(\mathcal{L}(E), +, \circ)$, $(\mathcal{M}_n(\mathbb{K}), +, \times)$ avec $\dim E > 1$ et $n > 1$ sont des anneaux non commutatifs.

Remarques : Soit $x \in A$. On a $0_A x = x 0_A = 0_A$ (en écrivant $0_A + 0_A = 0_A$) et $(-1_A)x = x(-1_A) = -x$ (en écrivant $1_A + (-1_A) = 0_A$).

Notations : Soit $x \in A$. On pose $0x = 0_A$ puis $(k+1)x = kx + x$ et $-(k+1)x = (-k)x - x$ pour k entier. Puis, on pose $x^0 = 1_A$ et $x^{n+1} = x^n x$ pour n entier. Pour $(a, b) \in A^2$, on note $a - b = a + (-b)$ et on a $-ab = (-a)b = a(-b)$ (en écrivant $(a - a)b = 0_A$ et $a(b - b) = 0_A$). On note simplement 0 et 1 les éléments neutres de $(A, +, \times)$ quand il n'y a pas de confusion possible.

Proposition 4. Soit $(A, +, \times)$ un anneau et $(x, y) \in A^2$ avec $xy = yx$. On a

$$\forall (m, n) \in \mathbb{N}^2 \quad x^m y^n = y^n x^m$$

Démonstration. On procède par récurrence pour établir $xy^n = y^n x$ avec n entier. Supposant le résultat vrai au rang n , il vient $xy^{n+1} = xy^n y = y^n xy = y^n yx = y^{n+1}x$. On applique alors ce premier résultat avec y^n pour n fixé et x . $\square$

Remarque : En particulier, pour $x \in A$ et n entier, on a $x^{n+1} = xx^n = x^n x$.

Théorème 2. Soit $(A, +, \times)$ un anneau et a, b éléments de A qui commutent. On a pour tout n entier :

1. $(ab)^n = a^n b^n$;
2. $(a + b)^n = \sum_{k=0}^n \binom{n}{k} a^k b^{n-k}$ (binôme de Newton) ;
3. $a^n - b^n = (a - b) \sum_{k=0}^{n-1} a^k b^{n-1-k}$ avec commutation du produit (identité de Bernoulli).

Démonstration. La première propriété se montre par récurrence en utilisant la proposition 4. Avec la convention $\binom{n}{n+1} = \binom{n}{-1} = 0$, il vient

$$\begin{aligned} (a + b)(a + b)^n &= \sum_{k=0}^n \binom{n}{k} a^{k+1} b^{n-k} + \sum_{k=0}^n \binom{n}{k} a^k b^{n+1-k} \\ &= \sum_{k=0}^{n+1} \binom{n}{k-1} a^k + b^{n+1-k} + \sum_{k=0}^{n+1} \binom{n}{k} a^k b^{n+1-k} = \sum_{k=0}^{n+1} \left[\binom{n}{k-1} + \binom{n}{k} \right] a^k b^{n+1-k} \end{aligned}$$

L'hérédité suit d'après la relation de Pascal. En distribuant, on trouve par télescopage

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

et le résultat vaut aussi en commutant. $\square$

Définition 5. On appelle sous-anneau de l'anneau $(A, +, \times)$ une partie B de A vérifiant :

1. $1_A \in B$;
2. $\forall (x, y) \in B^2 \quad x - y \in B$;
3. $\forall (x, y) \in B^2 \quad xy \in B$.

Proposition 5. Si B est un sous-anneau de $(A, +, \times)$, alors $(B, +, \times)$ possède une structure d'anneau.

Démonstration. Immédiate. $\square$

Remarque : En pratique, pour vérifier la structure d'anneau d'un ensemble, on cherche souvent à établir que celui-ci est sous-anneau d'un anneau connu.

Exemples : $(\mathbb{Z}, +, \times)$ est un sous-anneau de $(\mathbb{Q}, +, \times)$ qui est un sous-anneau de $(\mathbb{R}, +, \times)$ qui est un sous-anneau de $(\mathbb{C}, +, \times)$.

Définition 6. Un anneau commutatif $(A, +, \times)$ est dit intègre s'il est non réduit à $\{0_A\}$ et si

$$\forall (a, b) \in A^2 \quad ab = 0 \implies a = 0 \quad \text{ou} \quad b = 0$$

Exemples : 1. L'anneau $(\mathbb{Z}, +, \times)$ est intègre.

2. L'anneau $(A, +, \times)$ avec $A = \{\alpha I_2 + \beta M, (\alpha, \beta) \in \mathbb{K}^2\}$ et $M = \begin{pmatrix} 0 & 1 \\ 0 & 0 \end{pmatrix}$ n'est pas intègre puisque $M^2 = 0$. On verra ultérieurement que $A = \mathbb{K}[M]$.

2 Groupe des inversibles

Définition 7. Un élément a d'un anneau $(A, +, \times)$ est dit inversible s'il existe $b \in A$ tel que

$$ab = ba = 1_A$$

Cet élément b est unique, on l'appelle inverse de a et on le note a^{-1} .

Remarque : L'unicité de l'inverse s'obtient, comme dans le cas d'un groupe, par associativité.

Notation : On note $U(A)$ ou $A^\times$ l'ensemble des éléments inversibles de A .

Proposition 6. Soit $(A, +, \times)$ un anneau. On a

1. 1_A inversible d'inverse lui même ;
2. $\forall x \in U(A) \quad x^{-1} \in U(A) \quad \text{et} \quad (x^{-1})^{-1} = x$;
3. $\forall (x, y) \in U(A)^2 \quad xy \in U(A) \quad \text{et} \quad (xy)^{-1} = y^{-1}x^{-1}$.

Démonstration. Immédiate. $\square$

Proposition 7. Soit $(A, +, \times)$ un anneau. Le couple $(U(A), \times)$ est un groupe.

Démonstration. La loi $\times$ une loi de composition interne d'après le résultat de la proposition précédente, associative par hypothèse, avec pour élément neutre 1_A et tout élément admet un symétrique qui est son inverse. $\square$

Exemples : $U(\mathbb{Z}) = \{-1, 1\}$, $U(\mathbb{K}) = \mathbb{K}^*$, $U(\mathcal{M}_n(\mathbb{K})) = GL_n(\mathbb{K})$.

3 Idéaux d'un anneau commutatif

Définition 8. Soit $(A, +, \times)$ un anneau commutatif. On appelle idéal de cet anneau une partie I de A vérifiant :

1. l'ensemble I est un sous-groupe de $(A, +)$;
2. propriété d'absorption : $\forall (a, x) \in A \times I \quad ax \in I$

Exemple : Pour n entier, l'ensemble $n\mathbb{Z}$ est un idéal de $(\mathbb{Z}, +, \times)$.

Proposition 8. Soient I, J des idéaux d'un anneau $(A, +, \times)$ commutatif. Alors, l'ensemble $I + J$ (ou $J + I$) défini par

$$I + J = \{x + y, (x, y) \in I \times J\}$$

est un idéal de $(A, +, \times)$ contenant I et J .

Démonstration. Pour $x \in I$, on a $x + 0 \in I + J$ d'où $I \subset I + J$ et de même avec J . On a $0 \in I + J$ et pour $(x, y) \in I^2$ et $(z, t) \in J^2$, on a

$$x + z - (y + t) = (x - y) + (z - t) \in I + J$$

d'où $I + J$ sous-groupe de $(A, +)$. Enfin pour $(x, y, a) \in I \times J \times A$, on a

$$a(x + y) = ax + ay \in I + J$$

ce qui prouve le résultat attendu. $\square$

Proposition 9. Une somme finie d'idéaux d'un anneau $(A, +, \times)$ commutatif est un idéal contenant chacun des idéaux de la somme.

Démonstration. Récurrence immédiate. $\square$

Remarque : L'ordre dans la somme est sans incidence.

Définition 9. Soit $(A, +, \times)$ un anneau commutatif et $x \in A$. On appelle idéal engendré par x l'ensemble noté xA défini par

$$xA = \{xy, y \in A\}$$

Exemples : On a $0A = \{0\}$, $1A = A$. Si $A = \mathbb{Z}$, pour n entier, on note $n\mathbb{Z}$.

Proposition 10. Soit $(A, +, \times)$ anneau commutatif et $x \in A$. L'ensemble xA est un idéal contenant x .

Démonstration. Immédiate. $\square$

4 Divisibilité dans un anneau commutatif intègre

Dans cette partie, le triplet $(A, +, \times)$ désigne un anneau commutatif intègre.

Définition 10. Soient a, b dans A . On dit que a divise b s'il existe $c \in A$ tel que $b = ac$. On note $a|b$.

Proposition 11. Soient a, b dans A . On a

$$a|b \iff b \in aA \iff bA \subset aA$$

Démonstration. Immédiate. □

Proposition 12. Soient a, b, c dans A . On a

$$a|b \text{ et } b|c \implies a|c$$

$$a|b \text{ et } a|c \implies a|b+c$$

Démonstration. Immédiate. □

Proposition 13. Soient a, b, c dans A . On a

$$ab = ac \text{ et } a \neq 0 \implies b = c$$

$$ab|ac \text{ et } a \neq 0 \implies b|c$$

Démonstration. Immédiate avec l'intégrité. □

Définition 11. Soient a, b dans A . On dit que a et b sont associés si a divise b et b divise a .

Proposition 14. Soient a, b dans A . On a

$$a, b \text{ associés} \iff aA = bA \iff \exists c \in U(A) \mid b = ac$$

Démonstration. La première équivalence est immédiate. Supposons a, b associés. On dispose de c, d dans A tels que $a = bd$ et $b = ac$. Si $a = 0$, alors $b = ac = 0$ donc $b = 1 \times a$. Si $a \neq 0$, on a $a = bd = acd$ d'où $cd = 1$. Si $b = ac$ avec $c \in U(A)$ alors $a|b$ et comme il existe d tel que $cd = 1$, on a $bd = acd = a$ d'où $b|a$. □

Remarque : L'association est une relation d'équivalence (immédiat avec la première équivalence de la proposition précédente).

III Anneau de polynômes à une indéterminée

1 Idéaux de $(\mathbb{K}[X], +, \times)$

Proposition 15. Le triplet $(\mathbb{K}[X], +, \times)$ est un anneau commutatif intègre de neutres 0 et 1 dont les éléments inversibles sont les polynômes constants non nuls.

Démonstration. On sait déjà que $(\mathbb{K}[X], +, \times)$ est anneau commutatif de neutres 0 et 1. Soient P et Q dans $\mathbb{K}[X]$. On a

$$PQ = 0 \implies \deg PQ = \deg P + \deg Q = -\infty \implies \deg P = -\infty \text{ ou } \deg Q = -\infty$$

ce qui prouve l'intégrité de $\mathbb{K}[X]$. Puis

$$PQ = 1 \implies \deg PQ = 0 \implies \deg P + \deg Q = 0$$

Les polynômes inversibles sont donc constants non nuls et la réciproque est immédiate. □

Remarque : On peut donc parler de divisibilité dans $\mathbb{K}[X]$. Pour A, B dans $\mathbb{K}[X]$, on a

$$A|B \iff \exists C \in \mathbb{K}[X] \quad | \quad B = AC$$

$$A, B \text{ associés} \iff \exists \lambda \in \mathbb{K}^* \quad | \quad B = \lambda A$$

On utilisera fréquemment le fait suivant : deux polynômes associés unitaires ou nuls sont égaux.

Théorème 3. Soient A, B dans $\mathbb{K}[X]$ avec $B \neq 0$. Il existe un unique couple $(Q, R) \in \mathbb{K}[X]^2$ tel que

$$A = BQ + R \quad \text{et} \quad \deg R < \deg B$$

On appelle Q le quotient et R le reste de la division euclidienne de A par B .

Démonstration. En annexe. □

Théorème 4. Les idéaux de $(\mathbb{K}[X], +, \times)$ sont exactement de la forme $P \mathbb{K}[X]$ avec $P \in \mathbb{K}[X]$.

Démonstration. Soit I un idéal de $(\mathbb{K}[X], +, \times)$ distinct de $\{0\}$. L'ensemble $\{\deg P, P \in I \setminus \{0\}\}$ est une partie non vide de $\mathbb{N}$ donc admet un plus petit élément. Soit $B \in I \setminus \{0\}$ de degré minimal. Par absorption, on a $B \mathbb{K}[X] \subset I$. Réciproquement, soit $A \in I$. D'après le théorème de la division euclidienne, il existe $(Q, R) \in \mathbb{K}[X]^2$ tel que $A = BQ + R$ avec $\deg R < \deg B$. Or, on a $R = A - BQ \in I$ d'où $R = 0$ par minimalité de $\deg B$ ce qui prouve que B divise A d'où $I \subset B \mathbb{K}[X]$ et le résultat suit. □

Remarque : On dit que l'anneau $(\mathbb{K}[X], +, \times)$ est *principal*, à savoir un anneau intègre dont tous les idéaux sont engendrés par un élément.

Corollaire 1. Soit I un idéal de $(\mathbb{K}[X], +, \times)$. Il existe un unique polynôme P unitaire ou nul tel que $I = P \mathbb{K}[X]$.

Démonstration. Si $I = \{0\}$, c'est immédiat. Supposons $I \neq \{0\}$. D'après le résultat précédent, quitte à normaliser, on a l'existence. Supposons $I = P \mathbb{K}[X] = Q \mathbb{K}[X]$ avec P et Q unitaires. Ainsi, les polynômes P et Q sont associés et unitaires donc égaux. □

2 Plus grand commun diviseur

Définition 12. Soient P, Q dans $\mathbb{K}[X]$. On appelle plus grand commun diviseur de P et Q noté $P \wedge Q$ le polynôme unitaire ou nul engendrant l'idéal $P \mathbb{K}[X] + Q \mathbb{K}[X]$.

Remarque : Ce pgcd est bien défini comme unique polynôme unitaire ou nul engendrant un idéal de $(\mathbb{K}[X], +, \times)$. On a clairement $P \wedge Q = Q \wedge P$ pour $(P, Q) \in \mathbb{K}[X]^2$.

Proposition 16 (Relation de Bézout). Soient P, Q dans $\mathbb{K}[X]$. Il existe U, V dans $\mathbb{K}[X]$ tels que

$$UP + VQ = P \wedge Q$$

Démonstration. Immédiate par définition de $P \wedge Q$. □

Remarque : Les polynômes U et V de la relation de Bézout ne sont pas uniques. On a

$$\forall R \in \mathbb{K}[X] \quad P(U - RQ) + Q(V + RP) = P \wedge Q$$

Proposition 17. Soient P, Q dans $\mathbb{K}[X]$. On a $P \wedge Q$ divise P et Q et

$$S|P \quad \text{et} \quad S|Q \quad \implies \quad S|P \wedge Q$$

Démonstration. On a P, Q dans $(P \wedge Q)\mathbb{K}[X]$ d'où $P \wedge Q$ divise P et Q . On dispose de U et V dans $\mathbb{K}[X]$ tels que $PU + QV = P \wedge Q$. Si S divise P et S divise Q , alors S divise $PU + QV$. On peut aussi raisonner sur les idéaux

$$P\mathbb{K}[X] \subset S\mathbb{K}[X], Q\mathbb{K}[X] \subset S\mathbb{K}[X] \quad \text{d'où} \quad P\mathbb{K}[X] + Q\mathbb{K}[X] = (P \wedge Q)\mathbb{K}[X] \subset S\mathbb{K}[X]$$

□

Remarque : Ceci justifie l'appellation de *pgcd*.

Théorème 5 (Théorème d'Euclide). Soient A, B, Q et R dans $\mathbb{K}[X]$. Si $A = BQ + R$, alors $A \wedge B = B \wedge R$.

Démonstration. On a $A \wedge B$ qui divise A, B et donc $A - BQ = R$. Puis $B \wedge R$ divise B et divise $A - BQ$ donc divise $A - BQ + BQ = A$. Ainsi, les deux pgcd sont associés, unitaires ou nuls donc égaux. □

Commentaire : On peut alors envisager une implémentation de l'algorithme d'Euclide pour la détermination du pgcd de deux polynômes.

3 Polynômes premiers entre eux

Définition 13. Deux polynômes P, Q de $\mathbb{K}[X]$ sont dits premiers entre eux si $P \wedge Q = 1$.

Théorème 6 (Théorème de Bézout). Soient P, Q dans $\mathbb{K}[X]$. On a

$$P \wedge Q = 1 \iff \exists (U, V) \in \mathbb{K}[X]^2 \mid UP + VQ = 1$$

Démonstration. Le sens direct est immédiat par définition de $P \wedge Q$. Réciproquement, si $1 \in P\mathbb{K}[X] + Q\mathbb{K}[X]$, alors $1\mathbb{K}[X] = P\mathbb{K}[X] + Q\mathbb{K}[X] = (P \wedge Q)\mathbb{K}[X]$ d'où 1 et $P \wedge Q$ associés, unitaires et donc égaux. □

Proposition 18. Soient P, Q dans $\mathbb{K}[X]$. On a P et Q premiers entre eux si et seulement s'ils n'ont aucune racine complexe commune.

Démonstration. Supposons $P \wedge Q = 1$. Il existe U, V dans $\mathbb{K}[X]$ tels que $PU + QV = 1$. Soit α une racine complexe de P (si P n'admet pas de racines, il n'y a pas de racines communes à P et Q). Alors

$$P(\alpha)U(\alpha) + Q(\alpha)V(\alpha) = Q(\alpha)V(\alpha) = 1 \implies Q(\alpha) \neq 0$$

Pour la réciproque, on montre la contraposée. On note $P \wedge Q = D$ et on suppose $D \neq 1$. Si $D = 0$, alors on a $P = Q = 0$. Si $D \neq 0$, alors le pgcd D est non constant (sans quoi on aurait $D = 1$ puisqu'il est unitaire). D'après le théorème de d'Alembert-Gauss, le polynôme D admet une racine complexe et comme $D|P$ et $D|Q$, il s'ensuit que P et Q ont une racine commune. □

Proposition 19 (Lemme de Gauss). Soit $A, B, C \in \mathbb{K}[X]$. On a

$$A|BC \quad \text{et} \quad A \wedge B = 1 \implies A|C$$

Démonstration. Il existe $Q \in \mathbb{K}[X]$ tel que $BC = AQ$. Puis

$$C = C(UA + BV) = CUA + BCV = CUA + AQV = A(CU + QV)$$

d'où le résultat. $\square$

Proposition 20. Soient $A, B, C \in \mathbb{K}[X]$. On a

$$A \wedge BC = 1 \iff A \wedge B = 1 \quad \text{et} \quad A \wedge C = 1$$

Plus généralement, soient $A, B_1, \dots, B_n$ dans $\mathbb{K}[X]$. On a

$$A \wedge \prod_{i=1}^n B_i = 1 \iff \forall i \in \llbracket 1; n \rrbracket \quad A \wedge B_i = 1$$

Démonstration. Supposons $A \wedge BC = 1$. Il existe U, V dans $\mathbb{K}[X]$ tels que $AU + BCV = 1$ et le sens direct suit. Réciproquement, il existe S, T, U, V dans $\mathbb{K}[X]$ tels que

$$AU + BV = 1 \quad \text{et} \quad AS + CT = 1$$

$$\text{D'où} \quad AU + BV(AS + CT) = 1 \iff A(U + BVS) + BC(VT) = 1$$

d'où le résultat. La généralisation se montre par récurrence. $\square$

Proposition 21. Soient $A, B, C \in \mathbb{K}[X]$. On a

$$A \wedge B = 1 \quad \text{et} \quad A|C \quad \text{et} \quad B|C \implies AB|C$$

Plus généralement, soient $A_1, \dots, A_n$ dans $\mathbb{K}[X]$ premiers entre eux deux à deux et $B \in \mathbb{K}[X]$, on a

$$\forall i \in \llbracket 1; n \rrbracket \quad A_i|B \implies \prod_{i=1}^n A_i|B$$

Démonstration. Il existe $S, T \in \mathbb{K}[X]$ tel que $C = AS = BT$. Puis

$$C = C(UA + VB) = CUA + CVB = ABTU + ABSV = AB(TU + SV)$$

d'où le résultat. La généralisation se montre par récurrence en utilisant le résultat de la proposition précédente pour affirmer $A_{n+1} \wedge \prod_{i=1}^n A_i = 1$ avec $A_1, \dots, A_{n+1}$ premiers entre eux deux à deux. $\square$

Proposition 22. Soient $A, B, C \in \mathbb{K}[X]$. On a

$$A \wedge B = 1 \implies A \wedge BC = A \wedge C$$

Démonstration. On a $A \wedge C$ qui divise A et C donc A et BC donc $A \wedge BC$. Puis $D = A \wedge BC$ divise A . On note $A = DS$ avec $S \in \mathbb{K}[X]$. On a $DS \wedge B = 1$ d'où $D \wedge B = 1$ d'après la proposition précédente. Comme D divise BC , on conclut avec le lemme de Gauss. Ainsi, les polynômes D et $A \wedge C$ sont associés, unitaires ou nuls, donc égaux. $\square$

Proposition 23. Soient $P_1, \dots, P_n$ dans $\mathbb{K}[X]$. L'ensemble $\sum_{i=1}^n P_i \mathbb{K}[X]$ est un idéal de $(\mathbb{K}[X], +, \times)$.

Démonstration. Conséquence de la proposition 9. $\square$

Définition 14. Soient $P_1, \dots, P_n$ dans $\mathbb{K}[X]$. On appelle plus grand commun diviseur de $P_1, \dots, P_n$ noté $P_1 \wedge \dots \wedge P_n$ le polynôme unitaire ou nul engendrant l'idéal $\sum_{i=1}^n P_i \mathbb{K}[X]$.

Proposition 24 (Relation de Bézout). Soit $P_1, \dots, P_n \in \mathbb{K}[X]$ et $D = P_1 \wedge \dots \wedge P_n$. Il existe $U_1, \dots, U_n$ dans $\mathbb{K}[X]$ tels que

$$\sum_{i=1}^n P_i U_i = D$$

Démonstration. Immédiate par définition du pgcd. $\square$

Proposition 25. Soient $P_1, \dots, P_n$ dans $\mathbb{K}[X]$ et $D = P_1 \wedge \dots \wedge P_n$. On a $D|P_i$ pour tout $i \in \llbracket 1; n \rrbracket$ et

$$\forall i \in \llbracket 1; n \rrbracket \quad S|P_i \implies S|D$$

Démonstration. On a $P_i \in D \mathbb{K}[X] = \sum_{i=1}^n P_i \mathbb{K}[X]$ d'où D divise P_i . Si S divise les P_i , alors S divise $\sum_{i=1}^n P_i U_i$.

Ou aussi $P_i \mathbb{K}[X] \subset S \mathbb{K}[X]$ d'où $\sum_{i=1}^n P_i \mathbb{K}[X] = D \mathbb{K}[X] \subset S \mathbb{K}[X]$. $\square$

Proposition 26. Soient A, B, C dans $\mathbb{K}[X]$. On a

$$A \wedge B \wedge C = (A \wedge B) \wedge C$$

Démonstration. Notons $D = A \wedge B \wedge C$. On a $D|A$ et $D|B$ donc $D|A \wedge B$ puis $D|C$ d'où $D|(A \wedge B) \wedge C$. Puis $(A \wedge B) \wedge C$ divise C et $A \wedge B$ donc A et B et par conséquent divise D . Ainsi, les polynômes sont associés, unitaires ou nuls, donc égaux. $\square$

Remarque : On peut avoir $P_1 \wedge \dots \wedge P_n = 1$ sans avoir $P_i \wedge P_j = 1$ pour tout $i \neq j$. « Premiers deux à deux » est une condition plus forte. Un exemple simple est donné par

$$A = X \quad B = X + 1 \quad C = X(X + 1)$$

4 Irréductibles

Définition 15. Un polynôme $P \in \mathbb{K}[X]$ non constant est dit irréductible s'il n'est divisible que par les polynômes constants non nuls et ses polynômes associés.

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

Théorème 7. Soit $P \in \mathbb{K}[X]$ non constant. On a $P = \lambda \prod_{k=1}^r P_k^{\alpha_k}$ avec r entier non nul, $\lambda \in \mathbb{K}^*$, $P_1, \dots, P_r$ irréductibles unitaires deux à deux distincts et les α_k des entiers non nuls. Cette décomposition est unique à l'ordre près.

Idée de la démonstration. Unicité par des arguments de divisibilité et existence par récurrence forte sur $\deg P$. $\square$

Proposition 27. *Les polynômes irréductibles de $\mathbb{R}[X]$ sont exactement les polynômes de degré 1 et de degré 2 avec un discriminant strictement négatif. Les polynômes irréductibles de $\mathbb{C}[X]$ sont exactement les polynômes de degré 1.*

Démonstration. Soit $P \in \mathbb{C}[X]$ irréductible. Comme P est non constant, il admet une racine complexe α . Ainsi, on a $X - \alpha$ diviseur de P d'où P associé à $X - \alpha$. Soit $P \in \mathbb{R}[X]$ de degré 2 avec un discriminant strictement négatif. Le polynôme n'admet pas de racine réelle et donc pas de diviseur de degré 1. Ainsi, les seuls diviseurs de P sont de degré 0 et 2 et sont donc les polynômes constants non nuls et ses polynômes associés. Enfin, soit $P \in \mathbb{R}[X]$ irréductible. Si P admet une racine réelle α , alors $X - \alpha$ est diviseur de P d'où P associé à $X - \alpha$. Supposons enfin que P n'admet pas de racine réelle. Comme P est non constant, il admet une racine complexe non réelle α et $\overline{P(\alpha)} = P(\bar{\alpha}) = 0$. Ainsi, les polynômes premiers entre eux $X - \alpha$ et $X - \bar{\alpha}$ divisent P (dans $\mathbb{C}[X]$) ce qui prouve que leur produit $X^2 - 2\operatorname{Re}(\alpha)X + |\alpha|^2$ divise P dans $\mathbb{C}[X]$ mais aussi dans $\mathbb{R}[X]$. On en déduit que P est associé à ce polynôme dont le discriminant est strictement négatif. $\square$

IV Algèbres

1 Définition

Définition 16. *On appelle $\mathbb{K}$ -algèbre un quadruplet $(A, +, \times, \cdot)$ où $+$, $\times$ sont des lois internes et $\cdot$ un produit extérieur sur $\mathbb{K}$ vérifiant :*

1. $(A, +, \cdot)$ est un $\mathbb{K}$ -espace vectoriel ;
2. $(A, +, \times)$ est un anneau
3. $\forall (\lambda, x, y) \in \mathbb{K} \times A^2 \quad (\lambda \cdot x)y = \lambda \cdot (xy) = x(\lambda \cdot y).$

Si la loi $\times$ est commutative, l'algèbre $(A, +, \times, \cdot)$ est dite commutative.

Remarque : Dans ce qui suit, pour alléger la rédaction, on notera simplement A une algèbre en lieu et place de $(A, +, \times, \cdot)$.

Rappels : $(A, +, \cdot)$ $\mathbb{K}$ -ev signifie : $(A, +)$ est un groupe abélien et pour $(u, v) \in A^2$ et $(\lambda, \mu) \in \mathbb{K}^2$, on a

$$\lambda \cdot (u + v) = \lambda \cdot u + \lambda \cdot v \quad (\lambda + \mu) \cdot u = \lambda \cdot u + \mu \cdot u \quad (\lambda\mu) \cdot u = \lambda \cdot (\mu \cdot u) \quad 1 \cdot u = u$$

Exemples : Les ensembles $\mathbb{K}$, $\mathbb{K}[X]$, $\mathcal{F}(X, \mathbb{K})$ avec X un ensemble non vide, munis des lois idoines, sont des $\mathbb{K}$ -algèbres commutatives.

Les ensembles $\mathcal{L}(E)$, $\mathcal{M}_n(\mathbb{K})$ avec $\dim E > 1$ et $n > 1$, munis des lois idoines, sont des $\mathbb{K}$ -algèbres non commutatives.

Une $\mathbb{C}$ -algèbre est une $\mathbb{R}$ -algèbre. En particulier, $\mathbb{C}$ est une $\mathbb{R}$ -algèbre commutative, intègre, de dimension 2.

2 Sous-algèbre

Définition 17. *On appelle sous-algèbre d'une $\mathbb{K}$ -algèbre A une partie B de A vérifiant :*

1. $1_A \in B$;
2. $\forall (\lambda, x, y) \in \mathbb{K} \times B^2 \quad \lambda \cdot x + y \in B$;
3. $\forall (x, y) \in B^2 \quad xy \in B.$

Remarque : Une sous-algèbre de A est un sev et un sous-anneau de A .

Proposition 28. Une sous-algèbre d'une $\mathbb{K}$ -algèbre possède une structure de $\mathbb{K}$ -algèbre.

Démonstration. Immédiate. □

Exemples : 1. Le corps $\mathbb{R}$ est une sous-algèbre de $\mathbb{C}$.

2. Pour $u \in \mathcal{L}(E)$, on note $\mathcal{C}(u) = \{v \in \mathcal{L}(E) \mid u \circ v = v \circ u\}$ appelé le *commutant* de u . Ce commutant $\mathcal{C}(u)$ est une sous-algèbre de $\mathcal{L}(E)$.

3. L'ensemble $\mathcal{C} = \{(u_n)_n \in \mathbb{K}^{\mathbb{N}} \mid (u_n)_n \text{ converge}\}$ est une sous-algèbre de la $\mathbb{K}$ -algèbre commutative $\mathbb{K}^{\mathbb{N}} = \mathcal{F}(\mathbb{N}, \mathbb{K})$, et est donc elle-même commutative.

3 Morphisme d'algèbres

Définition 18. Soient A et A' deux $\mathbb{K}$ -algèbres. On appelle *morphisme d'algèbres de A vers A'* une application $\varphi : A \rightarrow A'$ vérifiant ;

1. $\varphi(1_A) = 1_{A'}$;
2. $\forall (\lambda, x, y) \in \mathbb{K} \times A^2 \quad \varphi(\lambda \cdot x + y) = \lambda \cdot \varphi(x) + \varphi(y)$;
3. $\forall (x, y) \in A^2 \quad \varphi(xy) = \varphi(x)\varphi(y)$

Proposition 29. Soit $\varphi : A \rightarrow A'$ un morphisme d'algèbres. L'image $\text{Im } \varphi$ est une sous-algèbre de A' et le noyau $\text{Ker } \varphi = \varphi^{-1}(\{0_{A'}\})$ est un sev de A . Si de plus l'algèbre A est commutative, alors $\text{Ker } \varphi$ est un idéal de A et $\text{Im } \varphi$ est une sous-algèbre commutative de A' .

Démonstration. On a $1_{A'} = \varphi(1_A) \in \text{Im } \varphi$, $\text{Im } \varphi$ stable par combinaison linéaire et stable par produit ce qui prouve que c'est une sous-algèbre de A' . On a $\text{Ker } \varphi$ sev de A en tant que noyau d'application linéaire. Supposons A commutative. On a

$$\forall (x, y) \in A^2 \quad \varphi(x)\varphi(y) = \varphi(xy) = \varphi(yx) = \varphi(y)\varphi(x)$$

ce qui prouve que $\text{Im } \varphi$ est une sous-algèbre commutative de A' . Pour $(a, x) \in A \times \text{Ker } \varphi$, on a $\varphi(ax) = \varphi(a)\varphi(x) = 0$ d'où $ax \in \text{Ker } \varphi$ et $\text{Ker } \varphi$ est un sous-groupe de $(A, +)$ puisque c'est un sev de A vu comme $\mathbb{K}$ -ev. □

Exemples : 1. Soit X un ensemble non vide. L'application $\varphi : \mathcal{F}(X, \mathbb{K}) \rightarrow \mathbb{K}, f \mapsto f(x)$ avec $x \in X$ est un morphisme d'algèbres appelé *morphisme d'évaluation*. Comme $\mathcal{F}(X, \mathbb{K})$ est une $\mathbb{K}$ -algèbre commutative, le noyau $\text{Ker } \varphi$ est un sev et un idéal de $\mathcal{F}(X, \mathbb{K})$.

2. Soit $\mathcal{C} = \{(u_n)_n \in \mathbb{K}^{\mathbb{N}} \mid (u_n)_n \text{ converge}\}$ et $\varphi : \mathcal{C} \rightarrow \mathbb{K}, (u_n)_n \mapsto \lim_{n \rightarrow +\infty} u_n$. L'application φ est un morphisme d'algèbres. Comme $\mathcal{C}$ est une $\mathbb{K}$ -algèbre commutative, le noyau $\text{Ker } \varphi$ est un sev et un idéal de $\mathcal{C}$.

Annexe

Théorème 3. Soient A, B dans $\mathbb{K}[X]$ avec $B \neq 0$. Il existe un unique couple $(Q, R) \in \mathbb{K}[X]^2$ tel que

$$A = BQ + R \quad \text{et} \quad \deg R < \deg B$$

On appelle Q le quotient et R le reste de la division euclidienne de A par B .

Démonstration. Si $B|A$, alors il existe $Q \in \mathbb{K}[X]$ tel que $A = BQ$ et on choisit $R = 0$. Supposons que B ne divise pas A . La partie $\mathcal{D} = \{\deg(A - BS), S \in \mathbb{K}[X]\}$ est une partie non vide de $\mathbb{N}$ donc admet un plus petit élément. Soit $Q \in \mathbb{K}[X]$ tel que $\deg(A - BQ)$ soit minimal. On pose $R = A - BQ$. Supposons $\deg R \geq \deg B$. On note $R = \rho X^r + \dots$ et $B = \beta X^b + \dots$ avec ρ et β non nuls. On a

$$R - \frac{\rho}{\beta} B X^{r-b} = A + \left(Q - \frac{\rho}{\beta} X^{r-b} \right) B \quad \text{avec} \quad \deg \left(R - \frac{\rho}{\beta} B X^{r-b} \right) < \deg R$$

ce qui est absurde par choix de R . On en déduit $\deg R < \deg B$ d'où l'existence. Pour l'unicité, supposons qu'on ait deux couples (Q_1, R_1) et (Q_2, R_2) solutions. Il vient

$$B(Q_2 - Q_1) = R_1 - R_2$$

d'où $\deg(R_1 - R_2) = \deg B + \deg(Q_2 - Q_1)$ et $\deg(R_1 - R_2) < \deg B$. Il en résulte $Q_1 = Q_2$ puis $R_1 = R_2$. $\square$

Proposition 30. Soit $P \in \mathbb{K}[X]$ irréductible unitaire et $A \in \mathbb{K}[X]$. On a

$$P \nmid A \iff P \wedge A = 1$$

Démonstration. On a $P \wedge A | P$ d'où $P \wedge A$ constant ou associé à P . Comme $P \wedge A$ est unitaire, alors $P \wedge A \in \{1, P\}$. Si $P \wedge A = P$, alors $P = P \wedge A | A$. Réciproquement, si $P | A$, alors $P | P \wedge A$ d'où $P \wedge A \neq 1$. $\square$

Proposition 31. Soit $A \in \mathbb{K}[X]$, n entier non nul et $P \in \mathbb{K}[X]$ irréductible unitaire. On a

$$P | A \iff P | A^n$$

Démonstration. Avec la proposition 20, on a par récurrence sur n entier

$$P \wedge A = 1 \iff P \wedge A^n = 1$$

Ainsi $P \nmid A \iff P \wedge A = 1 \iff P \wedge A^n = 1 \iff P \nmid A^n$

d'où le résultat par négation. $\square$

Proposition 32 (Lemme d'Euclide). Soit $(A, B) \in \mathbb{K}[X]^2$ et $P \in \mathbb{K}[X]$ irréductible unitaire. On a

$$P | AB \implies P | A \quad \text{ou} \quad P | B$$

Démonstration. Supposons que P ne divise pas A . Alors, on a $P \wedge A = 1$ et d'après le lemme de Gauss, il vient $P | B$. $\square$

Théorème 7. Soit $P \in \mathbb{K}[X]$ non constant. On a $P = \lambda \prod_{k=1}^r P_k^{\alpha_k}$ avec r entier non nul, $\lambda \in \mathbb{K}^*$, $P_1, \dots, P_r$ irréductibles unitaires deux à deux distincts et les α_k des entiers non nuls. Cette décomposition est unique à l'ordre près.

Démonstration. Pour l'existence, on procède par récurrence forte sur $n = \deg P$. Le cas $n = 1$ est immédiat. Supposons le résultat vrai jusqu'au degré n entier non nul fixé. Soit $P \in \mathbb{K}[X]$ de degré $n + 1$. Si P est irréductible, c'est immédiat. Sinon, le polynôme P admet un facteur irréductible unitaire Q et notant $P = QR$, on applique l'hypothèse de récurrence à R . L'existence suit par principe de récurrence. Supposons qu'on dispose de deux écritures

$$P = \lambda \prod_{k=1}^r P_k^{\alpha_k} = \mu \prod_{j=1}^s Q_j^{\beta_j}$$

avec λ, μ scalaires non nuls, les P_k et Q_j irréductibles unitaires, deux à deux distincts et les α_k et β_j entiers non nuls. Par examen du coefficient dominant à droite et à gauche, il vient $\lambda = \mu$.

Soit $k \in \llbracket 1; r \rrbracket$. On a $P_k \mid \prod_{j=1}^s Q_j^{\beta_j}$ d'où, d'après le lemme d'Euclide, l'existence de $j \in \llbracket 1; s \rrbracket$ tel

que $P_k \mid Q_j^{\beta_j}$ d'où $P_k \mid Q_j$ par irréductibilité de P_k . Comme P_k et Q_j sont irréductibles unitaires, il s'ensuit $P_k = Q_j$. L'indice j correspondant à k est unique puisque les polynômes intervenant dans la décomposition sont deux à deux distincts. Ainsi, pour $k \in \llbracket 1; r \rrbracket$, il existe un unique $j \in \llbracket 1; s \rrbracket$ tel que $P_k = Q_j$. On dispose d'une injection de $\llbracket 1; r \rrbracket$ dans $\llbracket 1; s \rrbracket$ d'où $r \leq s$ et par symétrie des rôles, on trouve $r = s$. Les polynômes irréductibles intervenant dans chacun des produits sont donc les mêmes et en même nombre. Enfin, pour $k \in \llbracket 1; r \rrbracket$ et $\ell \in \llbracket 1; r \rrbracket \setminus \{k\}$, on a $P_k \wedge P_\ell = 1$ et par des récurrences en invoquant la proposition 20, on obtient $P_k^{\alpha_k} \wedge P_\ell^{\beta_\ell} = 1$ d'où

$$P_k^{\alpha_k} \wedge \prod_{\ell \in \llbracket 1; r \rrbracket \setminus \{k\}} P_\ell^{\beta_\ell} = 1$$

D'après le lemme de Gauss, il s'ensuit $P_k^{\alpha_k} \mid P_k^{\beta_k}$ d'où $\alpha_k \leq \beta_k$ et $\alpha_k = \beta_k$ par symétrie des rôles ce qui clôt l'unicité. $\square$

Théorème 8 (d'Alembert-Gauss). *Tout polynôme non constant de $\mathbb{C}[X]$ admet une racine.*

Démonstration. Soit $P = \sum_{k=0}^n a_k X^k \in \mathbb{C}[X]$ avec n entier non nul et $a_n \neq 0$. Par inégalité triangulaire, il vient

$$\begin{aligned} \forall z \in \mathbb{C} \quad |P(z)| &= \left| a_n z^n + \sum_{k=0}^{n-1} a_k z^k \right| \\ &\geq |a_n| |z|^n - \left| \sum_{k=0}^{n-1} a_k z^k \right| \geq |a_n| |z|^n - \sum_{k=0}^{n-1} |a_k| |z|^k \underset{|z| \rightarrow +\infty}{=} |z_n| |z|^n (1 + o(1)) \end{aligned}$$

Par comparaison $|P(z)| \xrightarrow{|z| \rightarrow +\infty} +\infty$

Ainsi, on dispose de $R \geq 0$ tel que

$$\forall z \in \mathbb{C} \quad |z| > R \implies |P(z)| \geq |P(0)|$$

On en déduit $\inf_{z \in \mathbb{C}} |P(z)| = \inf_{|z| \leq R} |P(z)|$

Le disque fermé $D_f(0, R)$ est un fermé borné de $\mathbb{C}$ donc un compact de $\mathbb{C}$ et la fonction $z \mapsto |P(z)|$ continue comme composée de fonctions continues (le module avec $z \mapsto P(z)$) y atteint ses bornes. Ainsi, on dispose de $z_0 \in D_f(0, R)$ tel que

$$|P(z_0)| = \inf_{z \in \mathbb{C}} |P(z)|$$

Supposons $P(z_0) \neq 0$. On pose $Q = \frac{1}{P(z_0)} P(z_0 + X)$. On a

$$Q = \frac{1}{P(z_0)} \sum_{k=0}^n a_k (z_0 + X)^k = \frac{1}{P(z_0)} \sum_{k=0}^n a_k \sum_{\ell=0}^k \binom{k}{\ell} X^\ell z_0^{k-\ell} = \frac{a_n}{P(z_0)} X^n + \dots + 1$$

Ainsi, notant $Q = 1 + \sum_{k=1}^n b_k X^k$, l'ensemble $\{k \in \llbracket 1; n \rrbracket \mid b_k \neq 0\}$ est non vide et admet donc un minimum qu'on note ℓ . Il vient

$$Q(z) = 1 + b_\ell z^\ell (1 + \varphi(z)) \quad \text{avec} \quad \varphi(z) \xrightarrow{z \rightarrow 0} 0$$

On choisit $r > 0$ tel que $|\varphi(z)| \leq \frac{1}{2}$ pour $|z| \leq r$. On précise l'écriture trigonométrique de b_k avec $b_k = |b_k| e^{i\theta}$ où θ réel. Par suite, pour $\rho > 0$, on choisit une direction pour aller à l'opposé de θ afin de descendre plus bas avec

$$Q(\rho e^{-i(\theta+\pi)/\ell}) = 1 - |b_\ell| \rho^\ell - |b_\ell| \rho^\ell \varphi(\dots)$$

et pour $\rho \in]0; r[$, on obtient par inégalité triangulaire

$$|Q(\rho e^{-i(\theta+\pi)/\ell})| \leq |1 - |b_\ell| \rho^\ell| + \frac{1}{2} |b_\ell| \rho^\ell$$

Comme $1 - |b_\ell| \rho^\ell \xrightarrow{\rho \rightarrow 0} 1 > 0$, on dispose de $\varepsilon \in]0; r[$ tel que

$$\forall \rho \in]0; \varepsilon[\quad 1 - |b_\ell| \rho^\ell > 0$$

Par conséquent $\forall \rho \in]0; \varepsilon[\quad |Q(\rho e^{-i(\theta+\pi)/\ell})| \leq 1 - \frac{1}{2} |b_\ell| \rho^\ell < 1$

On peut donc trouver $z \in \mathbb{C}$ tel que

$$|P(z_0 + z)| < |P(z_0)|$$

ce qui est contredit le choix de z_0 . L'hypothèse $P(z_0) \neq 0$ est donc fausse et par conséquent, on a montré $P(z_0) = 0$. $\square$