Université François-Rabelais de Tours
Licence de Mathématiques

Chapitre 1 : Anneaux de polynômes

UE 6-3 Algèbre — Semestre 6

Dans ce chapitre, on introduit la notion de polynôme sur un corps ou un anneau. Tout au long du chapitre, $\mathbb{K}$ désigne un corps et A un anneau commutatif unitaire.

1 Premières définitions

Définition 1.1.

On appelle polynôme à une indéterminée à coefficients dans A toute suite $P = (a_n)_{n\in\mathbb{N}}$ d'éléments de A tous nul à partir d'un certain rang.

Les polynômes sont munis des opérations usuelles d'addition, de produit de polynômes et de multliplication par un scalaire $\lambda \in \mathbb{K}$: soient $P = (a_n)_{n\in\mathbb{N}}$, $Q = (b_n)_{n\in\mathbb{N}}$ deux polynômes à une indéterminée à coefficients dans A. On a alors :

- $P + Q = (a_n + b_n)_{n\in\mathbb{N}}$,
- $PQ = (c_n)_{n\in\mathbb{N}}$ avec $c_n = \sum_{0\leq k\leq n} a_k b_{n-k}$,
- $\lambda P = (\lambda a_n)_{n\in\mathbb{N}}$.

On vérifie que le produit de deux polynômes est bien un polynôme (voir Td1). On pose

$$X = (0, 1, 0\ldots) \quad \text{et} \quad X^0 = (1, 0, 0, \ldots)$$

On montre alors que $X^i = (0, \ldots, 0, 1, 0\ldots)$ où le 1 est situé à la $(i+1)^{\text{ième}}$ place et que

$$X^i \cdot X^j = X^{i+j}.$$

Soit $P = (a_n)_{n\in\mathbb{N}}$ et $\lambda \in A$. On définit le polynôme $\lambda P := (\lambda a_n)_{n\in\mathbb{N}}$. Tout polynôme $P = (a_n)_{n\in\mathbb{N}}$ à une indéterminée à coefficients dans A s'écrit sous la forme

$$P = \sum_{i\in\mathbb{N}} a_i X^i = (a_0, a_1, \ldots, a_n, 0, \ldots).$$

Les polynômes constants sont ceux de la forme $P = (a, 0, \ldots)$: dans ce cas, on note simplement $P = a$. Le degré de P, noté $\deg(P)$, est le plus grand entier n tel que $a_n \neq 0$. Par convention $\deg(0) = -\infty$.

Définition 1.2.

L'ensemble des polynômes à une indéterminée à coefficients dans A muni de l'addition et de la multiplication définies ci-dessus est un anneau commutatif. On le note $A[X]$.

On vérifiera que l'ensemble des polynômes constants est un sous-anneau de $A[X]$ isomorphe à A.

Définition 1.3.

Un polynôme P est dit unitaire si il est non nul et si son coefficient dominant, c'est-à-dire le coefficient du terme de plus haut degré, est égale à 1.

Proposition 1.4. *Si A est intègre alors pour tout $P, Q \in A[X]$ on a*

$$\deg(PQ) = \deg(P) + \deg(Q) \quad \textit{et} \quad \deg(P + Q) \leq \deg(P) + \deg(Q).$$

Démonstration. Si un des deux polynômes est nul alors $PQ = 0$ et l'égalité devient $-\infty = -\infty$ ce qui est « vrai ». On suppose donc que P et Q sont non nuls. Soit $n = \deg(P)$ et $m = \deg(Q)$. On pose $P = \sum a_i X^i$ et $Q = \sum b_i X^i$ où $a_i, b_i \in A$. Alors le coefficient du terme dominant de PQ est $a_n \cdot b_m$. Or $a_n \neq 0$ et $b_m \neq 0$ et donc, puisque A est intègre, $a_n \cdot b_m \neq 0$. Ce qui implique $\deg(PQ) = n + m$. □

On rappelle que $\mathbb{U}(A)$ désigne les éléments inversibles de A.

Proposition 1.5. *Si A est intègre, alors les éléments inversibles de $A[X]$ sont les polynômes constants $P = a$ où $a \in \mathbb{U}(A)$.*

Démonstration. Soit P inversible dans $A[X]$. Il existe $Q \in A[X]$ tel que $PQ = 1$. On a alors $\deg(P) + \deg(Q) = 0$ et $\deg(P) = \deg(Q) = 0$. Ainsi P et Q sont des constantes inversibles. □

2 Arithmétique des polynômes

2.1 Polynômes associés

Définition 2.1.

Deux polynômes P et Q de $A[X]$ sont dits associés s'il existe $a \in \mathbb{U}(A)$ tel que $P = aQ$.

Exemple 2.2. L'ensembles des polynômes associés à $X^2 + 1$ dans $\mathbb{Z}[X]$ est

$$\{X^2 + 1, -(X^2 + 1)\}$$

puisque les seuls inversibles de $\mathbb{Z}$ sont 1 et -1.

Proposition 2.3. *1) La relation « être associé » est une relation d'équivalence sur $A[X]$.*

2) Si P et Q sont associés et ont le même coefficient dominant alors $P = Q$.

3) Si A est un corps alors tout polynôme P est associé à un unique polynôme unitaire.

Démonstration. Voir Td. □

2.2 Division

Définition 2.4.

Soient $P, Q \in A[X]$. On dit que P divise Q et on note $P \mid Q$ s'il existe $R \in A[X]$ tel que $Q = PR$.

Exemple 2.5. 1) Le polynôme $X - 1$ divise $X^n - 1$ pour tout $n \geq 1$ dans $\mathbb{Z}[X]$.

2) Soient $A = X^3 + X + 1$ et $B = X + 1$ dans $\mathbb{Z}[X]$. On peut montrer que B ne divise pas A.

Proposition 2.6. *Soient $P, Q, R, S \in A[X]$.*

1) Si $P \mid Q$ et $Q \mid R$ alors $P \mid R$.

2) Si $P \mid Q$ et $P \mid R$ alors $P \mid Q + R$.

3) Si $P \mid Q$ et $Q \neq 0$ alors $\deg(P) \leq \deg(Q)$.

4) Si $P \mid Q$ et $R \mid S$ alors $PR \mid QS$.

5) Si $P \mid Q$ alors $P^n \mid Q^n$ pour tout $n \geq 1$.

Démonstration. Voir Td. □

Proposition 2.7. *Soient $P, Q, R, S \in A[X]$.*

1) Si $P \mid Q$ et $Q \mid P$ alors P et Q sont associés.

2) Si P est associé à R et Q est associé à S alors $P \mid Q \iff R \mid S$.

Démonstration. Voir Td. □

2.3 Division euclidienne

Théorème 2.8 (division euclidienne)**.**

Soit $A, B \in \mathbb{K}[X]$ deux polynômes à coeffcients dans **un corps** $\mathbb{K}$ et tels que $B \neq 0$. Alors il existe un unique couple (Q, R) de $\mathbb{K}[X]$ tels que $A = BQ + R$ et $\deg(R) < \deg(B)$.

Démonstration. Supposons qu'ils existent Q_1, R_1, et Q_2, R_2 tels que $A = BQ_1 + R_1$, $A = BQ_2 + R_2$ et $\deg(R_1), \deg(R_2) < \deg B$. On a alors $B \cdot (Q_1 - Q_2) = R_2 - R_1$. Cette égalité n'est possible que si $Q_1 - Q_2 = 0$ puisque $\deg(R_2 - R_1) < \deg(B)$. On a donc $Q_1 = Q_2$ et $R_1 = R_2$. Ce qui prouve l'unicité.

Pour l'existence, on procède par récurrence. On fixe le polynôme $B \neq 0$ et on pose $m = \deg(B) \geq 0$. Soit (H_n) la propriété

$$\text{Pour tout } A \in \mathbb{K}[X] \text{ tel que } \deg(A) \leq n-1, \text{ il existe un unique } (Q, R) \text{ tel que } A = BQ + R$$

La propriété H_m est vraie puisque si $n = m$ alors $Q = 0$ et $R = A$ conviennent. Soit $n \geq m$. On suppose que (H_n) est vraie et on souhaite montrer que (H_{n+1}) est vraie. Autrement dit, il faut montrer que pour tout polynôme de degré n il existe un couple (Q, R) tel que $A = BQ + R$. On pose

$$A = a_n X^n + a_{n-1} X^{n-1} + \cdots + a_0 \text{ et } B = b_m X^m + b_{m-1} X^{m-1} + \cdots + b_0.$$

et $T(X) = \dfrac{a_n}{b_m} X^{n-m}$, ce qui est possible puisque $b_m \neq 0$ (le polynôme B est non nul) et $n \geq m$. Alors T est un polynôme de degré $n - m$. Par conséquent, le polynôme $A - TB$ a un degré inférieur ou égal à n. De plus, son terme de degré n vaut :

$$a_n - \frac{a_n}{b_m} b_m = 0.$$

Il s'ensuit que $\deg(A - TB) < n$. On peut donc appliquer l'hypothèse de récurrence à ce polynôme et il vient :

$$A - TB = BQ_0 + R \text{ avec } \deg(R) < \deg(B) \text{ d'où } A = B(Q_0 + T) + R.$$

En posant $Q = Q_0 + T$, on obtient le résultat au rang n, ce qui achève notre récurrence. □

Exemple 2.9. Soit $A = X^3 + X + 1$ et $B = X + 1$. On a alors $A = B \cdot (X^2 - X + 2) - 1$. Dans ce cas ■

On rappelle qu'un sous ensemble I d'un anneau A est un idéal si les deux conditions suivantes sont vérifiées :

1) $(I, +)$ est un sous-groupes de $(A, +)$
2) Pour tout $a \in A$, on a $aI \subset I$. En d'autres termes $\forall a \in A, \forall x \in I, ax \in I$.

Théorème 2.10.

L'anneau $\mathbb{K}[X]$ est principal.

Démonstration. Soit $\mathscr{I}$ un idéal de $\mathbb{K}[X]$ contenant un polynôme non nul. On veut montrer que $\mathscr{I}$ est principal, c'est-à-dire qu'il existe un polynôme P tel que $\mathscr{I}$ soit exactement l'ensemble des multiples de P. Soit $\mathscr{D} = \{\deg(S) \ ; \ S \in \mathscr{I}, \ S \neq 0\}$. Il s'agit d'une partie non vide de $\mathbb{N}$ donc elle admet un minimum n. Soit P un polynôme de degré n dans $\mathscr{I}$. Comme $\mathscr{I}$ est un idéal, tous les multiples de P sont dans $\mathscr{I}$. Réciproquement, nous voulons montrer que tous les éléments de $\mathscr{I}$ sont des multiples de P. Soit donc $A \in \mathscr{I}$. On sait qu'il existe Q, R tels que $A = PQ + R$ avec $\deg(R) < n$. Or $-PQ \in \mathscr{I}$ donc $R = A - PQ \in \mathscr{I}$. Comme $\deg(R) < n$ donc, d'après la définition de n, on a $R = 0$, c'est-à-dire $A = PQ$ et A est bien un multiple de P. □

Remarque 2.11. Il est possible de montrer que, pour tout idéal $\mathscr{I}$ de $\mathbb{K}(X)$, il existe un **unique** polynôme unitaire qui engendre $\mathscr{I}$. Voir exercice 8 du Td1.

2.4 Polynômes irréductibles

On rappelle que les polynômes inversibles de $A[X]$ sont les polynômes constants $P = a \in \mathbb{U}(A)$. Ainsi, comme tous les éléments non-nuls d'un corps sont inversibles, les polynômes inversibles de $\mathbb{K}[X]$ sont les polynômes constants non-nuls.

Définition 2.12.

Un polynôme $P \in \mathbb{K}[X]$ est dit irréductible s'il n'est pas inversible et si l'égalité $P = QR$ implique que Q ou R est inversible.

On dira qu'un polynôme P est réductible s'il n'est pas irréductible.

Exemple 2.13. 1) Le polynôme $P(X) = 3$ est inversible dans $\mathbb{Q}[X]$. Il n'est donc pas irréductible.

2) Le polynôme $P(X) = X^2 + 1$ est irréductible si nous le considérons comme un élément de $\mathbb{R}[X]$ mais il est réductible si nous le considérons comme un élément de $\mathbb{C}[X]$ car $X^2 + 1 = (X - i)(X + i)$.

La notion de polynômes irréductibles **dépend** donc du corps $\mathbb{K}$.

Proposition 2.14. *1) Les polynômes réductibles de $\mathbb{K}[X]$ sont de degré supérieur ou égal à 2.*

2) Tous les polynômes de degré 1 sont irréductibles.

Démonstration. 1. Si nous avons $P = QR$ avec Q et R non inversibles alors $\deg(Q) \geq 1$ et $\deg(R) \geq 1$. Par conséquent, nous avons $\deg(P) = \deg(Q) + \deg(R) \geq 2$.
2. Exercice. □

2.5 Plus grand diviseur commun

Soient $P_1, \ldots, P_n \in \mathbb{K}[X]$. Puisque $\mathbb{K}[X]$ est principal, l'idéal

$$(P_1) + \ldots + (P_n) := \{A_1P_1 + A_2P_2 + \ldots + A_nP_n \mid A_1, \ldots, A_n \in \mathbb{K}[X]\}$$

est engendré par un unique polynôme unitaire P. Ce polynôme s'appelle le **pgcd** des P_i et on note $P = \text{pgcd}(P_1, \ldots, P_n)$.

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

1) Le $\text{pgcd}(P, Q)$ est un diviseur commun de P et Q.
2) Si D est un autre diviseur commun de P et Q alors D divise $\text{pgcd}(P, Q)$.
3) Il existe un couple de polynômes $(U, V) \in \mathbb{K}[X]^2$ tels que $PU + QV = \text{pgcd}(P, Q)$.

Démonstration. L'idéal $\mathscr{I} = (P) + (Q)$ est égal à l'ensemble des multiples de $\text{pgcd}(P, Q)$. Or $P \in \mathscr{I}$ et $Q \in \mathscr{I}$ donc $\text{pgcd}(P, Q)$ est un diviseur de P et de Q.
Si D est un diviseur de P et de Q, alors tout polynôme de la forme $PU + QV$ est aussi un multiple de D donc $\text{pgcd}(P, Q)$ (qui est de la forme $PU + QV$ puisqu'il est dans $\mathscr{I}$) est un multiple de D.
Le troisième point est clair puisque $\text{pgcd}(P, Q) \in (P) + (Q)$. □

Définition 2.15.

Soit $P, Q \in \mathbb{K}[X]$. On dit que P et Q sont **premiers entre eux** lorsque $\text{pgcd}(P, Q) = 1$.

En d'autres termes, si $\text{pgcd}(P, Q) = 1$ alors seules les constantes non nulles divisent à la fois P et Q.

Proposition 2.16. *Si $P \neq Q$ sont deux polynômes unitaires irréductibles, alors P et Q sont premiers entre eux.*

Démonstration. Supposons par l'absurde qu'il y a un diviseur commun D non constant à ces deux polynômes. En divisant au besoin par le coefficient dominant de D, on peut supposer D unitaire. Il existe alors deux polynômes R et S dans $\mathbb{K}[X]$ tels que $P = DR$ et $Q = DS$. Comme P et Q sont irréductibles et D n'est pas constant, les polynômes R et S sont forcément constants. Comme P, Q et D sont unitaires, on voit directement que $R = S = 1$ et donc $P = Q = D$. Ceci contredit l'hypothèse. □

Exemple 2.17. Si $\lambda \neq \mu$ sont deux nombres, alors les polynômes $(X - \lambda)$ et $(X - \mu)$ sont premiers entre eux.

Algorithme d'Euclide pour trouver le pgcd.
Soient $A, B \in \mathbb{K}[X]$ tels que $B \neq 0$. On calcule les divisions euclidiennes successives :

$$\begin{array}{llll} A = & B \cdot Q_1 & +R_1 & \text{où } \deg(R_1) < \deg(B) \\ B = & R_1 \cdot Q_2 & +R_2 & \text{où } \deg(R_2) < \deg(R_1) \\ R_1 = & R_2 \cdot Q_3 & +R_3 & \text{où } \deg(R_3) < \deg(R_2) \\ \vdots & & & \\ R_{k-2} = & R_{k-1} \cdot Q_k & +R_k & \text{où } \deg(R_k) < \deg(R_{k-1}) \\ R_{k-1} = & R_k \cdot Q_{k+1} & +0 & \end{array}$$

Le degré du reste diminue à chaque division, on s'arrête lorsque le reste est nul. Le pgcd est alors le dernier reste non-nul R_k (rendu unitaire). En remontant les lignes de calculs, on peut déterminer U et V tels que $\text{pgcd}(A, B) = AU + BV$.

Exemple 2.18. 1) Calculons le pgcd de $A = X^4 - 1$ et $B = X^3 - 1$. On a

$$\begin{aligned} X^4 - 1 &= (X^3 - 1) \cdot X + X - 1 \\ X^3 - 1 &= (X - 1) \cdot (X^2 + X + 1) + 0 \end{aligned}$$

et donc $\text{pgcd}(A, B) = X - 1$. De plus, on a

$$X - 1 = (X^4 - 1) \cdot 1 + (X^3 - 1) \cdot (-X).$$

Ainsi si on pose $U = 1$ et $V = -X$ on a

$$\text{pgcd}(A, B) = AU + BV.$$

2) Calculons le pgcd de $A = 6X^4 + 8X^3 - 7X^2 - 5X - 2$ et $B = 6X^3 - 4X^2 - X - 1$. On a

$$\begin{aligned} 6X^4 + 8X^3 - 7X^2 - 5X - 2 &= (X + 2) \cdot (6X^3 - 4X^2 - X - 1) + 2X^2 - 2X \\ 6X^3 - 4X^2 - X - 1 &= (3X + 1) \cdot (2X^2 - 2X) + X - 1 \\ 2X^2 - 2X &= 2X \cdot (X - 1) + 0 \end{aligned}$$

et donc $\text{pgcd}(A, B) = X - 1$. On part ensuite du pgcd et on remonte les lignes pour trouver :

$$\begin{aligned} X - 1 &= (6X^3 - 4X^2 - X - 1) - (3X + 1) \cdot (2X^2 - 2X) \\ &= (6X^3 - 4X^2 - X - 1) - (3X + 1) \left[6X^4 + 8X^3 - 7X^2 - 5X - 2) - (X + 2) \cdot (6X^3 - 4X^2 - X - 1)\right] \\ &= -(3X + 1) \cdot (6X^4 + 8X^3 - 7X^2 - 5X - 2) + (3X^2 + 7X + 3) \cdot (6X^3 - 4X^2 - X - 1). \end{aligned}$$

Ainsi , si on pose $U = -3X + 1$ et $V = 3X^2 + 7X + 3$, on a $\text{pgcd}(A, B) = AU + BV$ ■

Théorème 2.19 (Théorème de Bézout).

Soit $(A, B) \in \mathbb{K}[X]^2$ tel que $A \neq 0$ ou $B \neq 0$. Alors A et B sont premiers entre-eux si et seulement si il existe $(A, B) \in \mathbb{K}[X]^2$ tels que $AU + BV = 1$.

Démonstration. Tout diviseur commun de A et B divise $AU + BV = 1$. Donc $\text{pgcd}(A, B) = 1$.
Réciproquement, supposons que $\text{pgcd}(P, Q) = 1$. Comme $\text{pgcd}(P, Q)$ engendre l'idéal $(P) + (Q)$, on a $1 \in (P) + (Q)$. Il existe donc $U, V \in \mathbb{K}[X]$ tels que $PU + QV = 1$. □

Le théorème de Bézout implique les trois résultats importants suivants. La preuve sera faite en Td.

Proposition 2.20. *Soient $A, B, C \in \mathbb{K}[X]$ non nuls :*

1) **Lemme de Gauss** *: Si $A \mid BC$ et si $\text{pgcd}(A, B) = 1$ alors $A \mid C$.*
2) **Lemme d'Euclide** *: Si A est irréductible et si $A \mid BC$ alors A divise B ou A divise C.*
3) *A est premier avec BC si et seulement si A est premier avec B et A est premier avec C.*

Remarque 2.21. En utilisant 3), on montre que si A et B sont premier entre-eux alors A^α et B^β sont premiers entre-eux pour tout $\alpha, \beta \geq 1$. En particulier, si $\lambda \neq \mu$ sont deux nombres, alors les polynômes $(X - \lambda)^\alpha$ et $(X - \mu)^\beta$ sont premiers entre eux.

2.6 Factorisation

Théorème 2.22.

Soit $P \in \mathbb{K}[X]$ un polynôme non nul. Alors P se décompose de manière unique à l'ordre des facteurs près sous la forme :

$$P = \alpha P_1^{\alpha_1} P_2^{\alpha_2} \dots P_m^{\alpha_m}$$

où les P_i sont des polynômes distincts, unitaires et irréductibles dans $\mathbb{K}[X]$ et $\alpha \in \mathbb{K}^*$ est le coefficient dominant de P.

Démonstration. On peut supposer sans perdre de généralité que P est unitaire. On cherche alors à décomposer P sous la forme $P = P_1^{\alpha_1} P_2^{\alpha_2} \dots P_m^{\alpha_m}$.

Existence de la décomposition.

On raisonne par récurrence sur $d = \deg(P)$. Si $d = 1$, P est un polynôme de degré 1 donc irréductible. Le résultat est clair.

On suppose le résultat vrai pour tout polynôme de degré $\leq d$. Soit P un polynôme de degré $d+1$. Soit P est irréductible auquel cas le résultat est clair soit P est réductible et il existe deux polynômes unitaires Q et R non constants tels que $P = QR$. Comme Q et R sont de degrés ≥ 1, on a $1 \leq \deg(Q), \deg(R) \leq d$. L'hypothèse de récurrence s'applique donc à Q et à R. Il existe alors des polynômes unitaires irréductibles $P_1, \dots, P_m$ et $P_{m+1}, \dots, P_r$ tels que $Q = P_1 \dots P_m$ et $R = P_{m+1} \dots P_r$. On a alors $P = P_1 \dots P_r$ et on obtient le résultat en regroupant les P_i qui sont égaux.

Unicité de la décomposition.

On suppose que $P = P_1^{\alpha_1} P_2^{\alpha_2} \dots P_m^{\alpha_m} = Q_1^{\beta_1} Q_2^{\beta_2} \dots Q_k^{\beta_k}$ où les P_i (respectivement les Q_i) sont des polynômes distincts, unitaires et irréductibles dans $\mathbb{K}[X]$.

Soit $i \in \{1, \dots, m\}$. Puisque $P_i \mid Q_1^{\beta_1} Q_2^{\beta_2} \dots Q_k^{\beta_k}$ et P_i est irréductible, on voit d'après le lemme d'Euclide que $P_i \mid Q_j$ pour un certain $j \in \{1, \dots, k\}$. Comme P_i et Q_j sont irréductibles et unitaires, on a alors $P_i = Q_j$. Ceci permet de définir une application de $\{1, \dots, m\}$ dans $\{1, \dots, k\}$ tel que $P_i = Q_j$. De plus comme les Q_i sont distincts, cette application est injective. Par symétrie, on peut construire une application injective de $\{1, \dots, k\}$ dans $\{1, \dots, m\}$, ce qui montre que $k = m$ et

$$\{P_1, \dots, P_m\} = \{Q_1, \dots, Q_m\}.$$

Quitte à réordonner les facteurs on supposera que $P = P_1^{\alpha_1} P_2^{\alpha_2} \dots P_m^{\alpha_m} = P_1^{\beta_1} P_2^{\beta_2} \dots P_m^{\beta_m}$. Pour tout $i \neq j$ on a $\operatorname{pgcd}(P_i^{\alpha_i}, Q_j^{\beta_j}) = 1$, ainsi $P_i^{\alpha_i} \mid Q_i^{\beta_i}$ et $\alpha_i \leq \beta_i$. De manière symétrique, on montre que $Q_i^{\beta_i} \mid P_i^{\alpha_i}$ et $\beta_i \leq \alpha_i$. Ainsi $\alpha_i = \beta_i$ pour tout i. □

Exemple 2.23. On considère le polynôme $P = X^2 + 1$. Alors P est à la fois dans $\mathbb{R}[X]$ et $\mathbb{C}[X]$. Mais, **attention**, sa factorisation n'est pas la même dans ces deux anneaux :

1) P se factorise sous la forme $(X - i) \cdot (X + i)$ dans $\mathbb{C}[X]$
2) P est irréductible dans $\mathbb{R}[X]$. ■

Proposition 2.24. *Soit P et Q deux polynômes non nuls. Soit $P = aP_1^{\alpha_1} \dots P_n^{\alpha_n}$ et $Q = bP_1^{\beta_1} \dots P_n^{\beta_n}$ leurs décompositions en facteurs irréductibles où $\alpha_i, \beta_i \geq 0$ pour tout $i \in \{1, \dots, n\}$. Alors*

$$P \mid Q \iff \alpha_j \leq \beta_j \text{ pour tout } 1 \leq j \leq n.$$

Démonstration. Tout d'abord on peut supposer que les mêmes P_j sont utilisés pour P et pour Q quitte à autoriser les α_i et β_i à être nuls.

Si, pour chaque j, on a $\alpha_j \leq \beta_j$, alors il est clair que P divise Q. Réciproquement, si P divise Q, alors il existe un polynôme R tel que $Q = PR$. Les polynômes qui divisent R divisent également Q donc la décomposition en facteurs irréductibles de R n'utilise que les polynômes $P_1, \dots, P_n$:

$$R = c\, P_1^{\gamma_1} \dots P_n^{\gamma_n}$$

avec c une constante et $\gamma_j \in \mathbb{N}$. On a alors :

$$Q = PR = (ac) P_1^{\alpha_1 + \gamma_1} \dots P_n^{\alpha_n + \gamma_n}.$$

Par unicité de la décomposition en facteurs irréductibles, il vient

$$ac = b \text{ et } \forall j, \quad \alpha_j + \gamma_j = \beta_j$$

et donc en particulier $\alpha_j \leq \beta_j$. □

En particulier, si $P = aP_1^{\alpha_1} \dots P_n^{\alpha_n}$ et $Q = bP_1^{\beta_1} \dots P_n^{\beta_n}$ alors on a

$$\text{pgcd}(P, Q) = P_1^{\min\{\alpha_1,\beta_1\}} \cdot \dots P_n^{\min\{\alpha_n,\beta_n\}}.$$

3 Fonctions polynomiales

Soit $P \in \mathbb{K}[X]$. On désigne par f_P la fonction polynomiale associée à P, c'est-à-dire la fonction :

$$\begin{array}{rccc} f_P : & \mathbb{K} & \longrightarrow & \mathbb{K} \\ & x & \longmapsto & P(x) \end{array}$$

On veillera à ne pas confondre un polynôme $P \in \mathbb{K}[X]$ avec la fonction polynomiale correspondante. En effet, la fonction polynomiale peut en effet être nulle alors que le polynôme P ne l'est pas.

Exemple. Soit $A = \mathbb{Z}/3\mathbb{Z}$, on peut montrer que A est un corps (faites-le !). Soit P le polynôme défini par $P(X) = X(X^2 - 1) \in A[X]$. On a $f_P(x) = 0$ pour tout $x \in A$ et pourtant P n'est pas le polynôme nul ! C'est la suite d'éléments de A définie par $(\bar{0}, \bar{2}, 0, \bar{1}, \bar{0}, \bar{0}, \dots)$

Il est clair que pour tout $P, Q \in \mathbb{K}[X]$ et tout $\lambda \in \mathbb{K}$ on a

- $f_{P+\lambda Q} = f_P + \lambda f_Q$,
- $f_{PQ} = f_P f_Q$.

En d'autre termes, l'application $P \longmapsto f_P$ est un morphisme d'algèbre. Lorsqu'il n'y aura pas d'ambiguité, on désignera, afin d'alléger les notations, la fonction polynomiale simplement par $x \mapsto P(x)$.

Définition 3.1.

Soit $P \in \mathbb{K}[X]$. On dit que $x \in \mathbb{K}$ est une racine de P si $f_P(x) = 0$ (ou $P(x) = 0$).

Proposition 3.2. *Soit $P \in \mathbb{K}[X]$ et $\alpha \in \mathbb{K}$. Alors α est racine de P si et seulement si le polynôme $X - \alpha \mid P$.*

Démonstration. Il existe deux polynômes $Q, R \in \mathbb{K}[X]$ tels que

$$P = Q \cdot (X - \alpha) + R \text{ où } \deg R < 1.$$

Ainsi R est une constante. En évaluant l'expression ci-dessus en α, on trouve $P(\alpha) = R(\alpha)$ et on a :

$$\alpha \text{ est une racine de P} \iff P(\alpha) = 0 \iff R = 0 \iff (X - \alpha) \text{ divise } P.$$

□

Définition 3.3.

Soit $P \in \mathbb{K}[X]$ et soit α une racine de P. On dit que α est de multiplicité k si et seulement si $(X - \alpha)^k$ divise P et $(X - \alpha)^{k+1} \nmid P$.

En d'autres termes α est racine de P de multiplicité k si et seulement si $P = (X - \alpha)^k \cdot Q$ et $Q(\alpha) \neq 0$.

Exemple 3.4. Pour déterminer la multiplicité d'une racine, on peut donc effectuer des divisions euclidiennes successives. Soit $P = X^5 - 2X^4 + 2X^3 - 3X^2 + 3X - 1$. On vérifie facilement que 1 est racine de P. De plus, on trouve

$$\begin{aligned} P &= (X - 1) \cdot Q_1 \quad \text{où} \quad Q_1 = X^4 - X^3 + X^2 - 2X + 1 \\ Q_1 &= (X - 1) \cdot Q_2 \quad \text{où} \quad Q_2 = X^3 + X - 1 \end{aligned}$$

et $Q_2(1) \neq 0$. Ainsi, 1 est racine de multiplicité 2 de P. ■

Le résultat suivant est utile pour déterminer la multiplicité d'une racine dans $\mathbb{R}$ ou $\mathbb{C}$.

Proposition 3.5. *Soit $P \in \mathbb{K}[X]$ avec $\mathbb{K} = \mathbb{R}$ ou $\mathbb{C}$. Les trois propositions suivantes sont équivalentes :*

1) α est une racine de multiplicité k.

2) $P = (X - \alpha)^k Q$ et $Q(\alpha) \neq 0$.

3) Pour tout $j \in [\![0, k-1]\!]$, on a $P^{(j)}(\alpha) = 0$ et $P^{(k)}(\alpha) \neq 0$.

Démonstration. Voir Td. □

Théorème 3.6.

Soit $P \in \mathbb{K}[X]$ et $\alpha_1, \ldots, \alpha_r$ des racines distinctes deux à deux de multiplicité respective $k_1, \ldots, k_r$. Alors, il existe $Q \in \mathbb{K}[X]$ tel que

$$P = (X-\alpha_1)^{k_1}(X-\alpha_2)^{k_2}\ldots(X-\alpha_r)^{k_r}\cdot Q \quad \text{et} \quad Q(\alpha_i) \neq 0 \text{ pour tout } i$$

En particulier, P est de degré au moins $k_1 + \ldots + k_r$.

Démonstration. Nous savons que P s'écrit $(X-\alpha_1)^{k_1}Q_2(X)$ et que $Q_2(\alpha_1) \neq 0$. Comme $(X-\alpha_2)^{k_2}$ est premier avec $(X-\alpha_1)^{k_1}$ et divise $P = (X-\alpha_1)^{k_1}Q_2(X)$, le lemme de Gauss assure que $(X-\alpha_2)^{k_2}$ divise $Q_2(X)$. On peut donc factoriser également $(X-\alpha_2)^{k_2}$. En recommençant, on finit par écrire $P = (X-\alpha_1)^{k_1}\ldots(X-\alpha_p)^{k_p}Q(X)$ où Q est un polynôme non nul puisque P est non nul et $Q(\alpha_i) \neq 0$ pour tout i. Dès lors, il est évident que $n = \deg(P) = k + \deg(Q) \geq k$. □

Remarque 3.7. On déduit du théorème précédent qu'un polynôme de degré n a au plus n racines. Attention, le résultat précédent n'est pas vrai lorsque sur un anneau ! Regarder par exemple le polynome $4X$ dans $\mathbb{Z}/8\mathbb{Z}$...

Théorème 3.8 (d'Alembert-Gauss).

Un polynôme non constant de $\mathbb{C}[X]$ possède au moins une racine. En particulier, les polynômes irréductibles de $\mathbb{C}[X]$ sont exactement les polynômes de degré 1.

Démonstration. Soit $P = \sum_{i=1}^{n} a_i X^i$ un polynôme à coefficient complexe de degré $n \geq 1$. On a

$$\forall z \in \mathbb{C}^*,\ |P(z)| = |\sum_{i=1}^{n} a_i z^i| = |a_n||z^n|\left|\frac{a_0}{a_n z^n} + \ldots + \frac{a_{n-1}}{a_n z} + 1\right|$$

et donc $|P(z)| \to +\infty$ lorsque $|z| \to +\infty$. Ainsi :

$$\exists R > 0,\ (|z| > R \Longrightarrow |P(z)| > |P(0)|)\,.$$

De plus, l'application $z \mapsto |P(z)|$ est une application continue sur $\mathbb{C}$ et l'ensemble $K = \{z \in \mathbb{C} \mid |z| \leq R\}$ est un compact de $\mathbb{C}$, ainsi cette application admet un minimum sur K :

$$\exists z_0 \in K, \forall z \in K, |P(z)| \geq |P(z_0)|.$$

Puisque $0 \in K$ on a $|P(0)| \geq |P(z_0)|$. On a donc

$$\forall z \in \mathbb{C}, |P(z)| \geq |P(z_0)|.$$

Pour montrer que P s'annule, on va procéder par l'absurde. Supposons que P ne s'annule pas : on a donc

$$(\star) \qquad \forall z \in \mathbb{C}, |P(z)| \geq |P(z_0)| > 0.$$

Il existe $(b_0, \ldots, b_n) \in \mathbb{C}^{n+1}$ tel que

$$P(z_0 + X) = \sum_{i=0}^{n} b_i z^i.$$

De plus $b_0 = P(z_0) > 0$ et $b_n \neq 0$ puisque P est de degré n. Soit $k = \min\{i \in \{1, \ldots, n\} \mid b_i \neq 0\}$ et soit ω une racine $k^{\text{ième}}$ de $-\frac{b_0}{b_k}$. On a alors pour tout $t \in \mathbb{R}$

$$P(z_0 + \omega t) = b_0 + \sum_{i=k}^{n} b_i(\omega t)^i = b_0\left(1 - t^k + t^k\varepsilon(t)\right)$$

où la fonction $\varepsilon(t) \to 0$ lorsque $t \to 0$. Ainsi, on peut trouver $\alpha > 0$ tel que $|t| < \alpha$ implique $|\varepsilon(t)| < 1/2$. Soit $0 < t < \min\{1, \alpha\}$. On a alors

$$|P(z_0 + \omega t)| = \left|b_0\left(1 - t^k + t^k\varepsilon(t)\right)\right| \leq |b_0|\left(\left|1 - t^k\right| + |t^k\varepsilon(t)|\right) < |b_0|(1 - \frac{1}{2}t^k) < |b_0|$$

Cette dernière inégalité est en contradiction avec $(\star)$ puisque $b_0 = P(z_0)$. □

Corollaire 3.9. *Les polynômes non constants irréductibles de $\mathbb{R}[X]$ sont ceux de degré 1 et ceux de degré 2 dont le discriminant Δ est strictement négatif.*

Démonstration. Soit P un polynôme à coefficients réels de degré supérieur ou égale à 2. On montre que pour tout $\alpha \in \mathbb{C}$, on a $P(\overline{\alpha}) = \overline{P(\alpha)}$. Ainsi, les racines complexes non-réelles de P vont par deux. On a donc un nombre pair de racines complexes : $\alpha_1, \overline{\alpha_1}, \ldots, \alpha_k, \overline{\alpha_k}$. Soient $\beta_1, \ldots, \beta_r$ les racines réelles de P. Le polynôme P se factorise sous la forme suivante dans $\mathbb{C}$:

$$P = \prod_{i=1}^{k}(X - \alpha_i)(X - \overline{\alpha_i}) \cdot \prod_{i=1}^{r}(X - \beta_i).$$

On remarque que $(X - \alpha_i)(X - \overline{\alpha_i}) = X^2 - 2\mathrm{Re}(\alpha_i)X + |\alpha_i|^2$ est un polynôme à coefficients réels et à discriminant négatif. On peut donc factoriser P de la manière suivante sur $\mathbb{R}$:

$$P = \prod_{i=1}^{k}(X^2 - 2\mathrm{Re}(\alpha_i)X + |\alpha_i|^2) \cdot \prod_{i=1}^{r}(X - \beta_i).$$

Finalement les polynômes de degré 2 dont le discriminant Δ est strictement négatif sont irréductibles sur $\mathbb{R}$ puisqu'ils n'ont pas de racines réelles. □

Exercice 3.10. On considère le polynôme $P = X^4 + 1$. Déterminer la factorisation de Q en irréductibles dans les anneaux $\mathbb{Q}[X]$, $\mathbb{R}[X]$ et $\mathbb{C}[X]$.

Solution. On résoud l'équation $z^4 + 1 = 0$ dans $\mathbb{C}$. On trouve 4 solutions : $e^{i\frac{\pi}{4}}, e^{-i\frac{\pi}{4}}, e^{i\frac{3\pi}{4}}, e^{i\frac{-3\pi}{4}}$. Ainsi on a

$$P = (X - e^{i\frac{\pi}{4}})(X - e^{-i\frac{\pi}{4}})(X - e^{i\frac{3\pi}{4}})(X - e^{-i\frac{3\pi}{4}}).$$

Tous les polynômes qui apparaissent dans cette décomposition sont bien irréductibles, c'est donc bien la factorisation de P en irréductibles dans $\mathbb{C}[X]$.

En regroupant les facteurs conjugués on trouve

$$\begin{aligned} P &= (X - e^{i\frac{\pi}{4}})(X - e^{-i\frac{\pi}{4}})(X - e^{i\frac{3\pi}{4}})(X - e^{-i\frac{3\pi}{4}}) \\ &= (X^2 + \sqrt{2}X + 1)(X^2 - \sqrt{2}X + 1). \end{aligned}$$

Encore une fois, tous les polynômes qui apparaissent dans cette décomposition sont bien irréductibles sur $\mathbb{R}$ (leurs discriminants sont négatifs) on a donc bien trouvé la factorisation de P en irréductibles dans $\mathbb{R}[X]$.

Finalement montrons que Q est irréductibles sur $\mathbb{Q}$. Supposons que le polynôme Q est réductible sur $\mathbb{Q}$. Puisque Q n'a pas de racine dans $\mathbb{Q}$, il se factorise comme un produit de deux polynômes unitaires de degré deux, disons A et B. Alors $Q = AB$ est aussi une factorisation de Q sur $\mathbb{R}$. Puisque Q n'a pas de racine dans $\mathbb{R}$, les polynômes A et B sont aussi irréductibles sur $\mathbb{R}$. Par unicité de la factorisation on a alors $A = X^2 + \sqrt{2}X + 1$ ou $B = X^2 + \sqrt{2}X + 1$. C'est une contradiction. Ainsi Q est irréductible sur $\mathbb{Q}$.

Remarque 3.11. **Attention**, l'argument *P n'a pas de racine dans $\mathbb{K}$ donc P est irréductible* ne marche que si P est de degré 1, 2 ou 3 ! On s'en convaincra aisément en considérant le polynôme $(X^2+1)^2$ dans $\mathbb{R}[X]$.