CHAPITRE 23

Polynômes

Notations

Soit $\mathbb{K}$ un corps et $P \in \mathbb{K}[X]$.

→ On note $Z_{\mathbb{K}}(P)$ l'ensemble des racines de P dans $\mathbb{K}$. Lorsqu'il n'y a pas ambiguïté sur $\mathbb{K}$, on note simplement $Z(P)$.

→ On note $\operatorname{val} P$ la valuation de P, c'est à dire le coefficient du terme de plus petit degré de P.

I Préambule

Dans tout le chapitre, $\mathbb{K}$ désigne un corps.

Proposition I.1.

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

1. Si $\deg P = 1$, alors P est irréductible.
2. Si $\deg(P) \in \{2, 3\}$, alors P est irréductible si et seulement s'il n'a pas de racine.

Preuve

1. Clair car si $P = QR$ et $\deg P = 1$ alors nécessairement Q ou R est constant.
2. Montrons les deux implications.
   → ($\Rightarrow$) Si P est irréductible de degré $n \geq 2$, il est sans racine (s'il admet une racine a, $P = (X - a)Q$ avec Q non constant, absurde).
   → ($\Leftarrow$) Procédons par contraposée. si $\deg P \in \{2, 3\}$ se factorise de manière non triviale, $P = QR$ avec $1 \leq \deg Q \leq \deg R$ et $\deg P = \deg Q + \deg R$, donc $1 \leq \deg Q \leq \dfrac{\deg(P)}{2} \leq 1.5$, donc $\deg Q = 1$ et Q admet une racine dans $\mathbb{K}$ et finalement P aussi.

Contre exemple : Pour $\deg P \geq 4$, la propriété (2) n'est plus vraie. En effet, $X^4 + 1$ dans $\mathbb{R}[X]$ est réductible car sa factorisation dans $\mathbb{R}[X]$ est $(X^2 + \sqrt{2}X + 1)(X^2 - \sqrt{2}X + 1)$ mais n'admet pas de racine dans $\mathbb{R}$.

Proposition I.2.

Si $\mathbb{K} \subset \mathbb{L}$ sont deux corps et $(A, B) \in (\mathbb{K}[X] - \{0\})^2$, alors $A \wedge B$ et $A \vee B$ sont les mêmes dans $\mathbb{L}[X]$ et dans $\mathbb{K}[X]$.

Preuve

→ Pour $A \wedge B$: le calcul de cette quantité se fait par l'algorithme d'Euclide qui manipule des éléments de $\mathbb{K}[X]$. Tous ces éléments restent dans $\mathbb{K}[X]$ au fil des étapes de l'algorithme, donc le résultat de l'algorithme, i.e. $A \wedge B$, reste dans $\mathbb{K}[X]$.

→ Pour $A \vee B$: $A \vee B = \dfrac{AB}{A \wedge B}$, il s'agit donc du rapport de deux éléments de $\mathbb{K}[X]$ et est de plus le même vu l'invariance de $A \wedge B$.

II Polynômes complexes

Théorème (Théorème de D'Alembert-Gauss) II.1.

les polynômes irréductibles de $\mathbb{C}[X]$ sont de degré 1. D'une manière équivalente, pour tout $P \in \mathbb{C}[X]$ non constant, il existe $\lambda_1, \ldots, \lambda_n, a \in \mathbb{C}$ tels que

$$P(X) = a \prod_{i=1}^{n} (X - \lambda_i)$$

Preuve : La preuve de ce théorème dépasse le cadre de ce cours et ne sera donc pas faite.

Proposition II.2.

Soit $P, Q \in \mathbb{K}[X]$, $\lambda, \mu \in \mathbb{K}^*$ et $z_1, \ldots, z_r \in \mathbb{K}$ distincts tels que

$$P(X) = \lambda \prod_{i=1}^{r} (X - z_i)^{\alpha_i} \text{ et } Q(X) = \mu \prod_{i=1}^{r} (X - z_i)^{\beta_i}$$

On a

$$P \wedge Q = \prod_{i=1}^{r} (X - z_i)^{\min(\alpha_i, \beta_i)} \text{ et } P \vee Q = \prod_{i=1}^{r} (X - z_i)^{\max(\alpha_i, \beta_i)}$$

Exemple : Pour tout $m, n \in \mathbb{N}^*$, on a, dans $\mathbb{C}[X]$, $X^m - 1 \wedge X^n - 1 = X^{m \wedge n} - 1$. En effet, on a

$$\begin{aligned} X^m - 1 \wedge X^n - 1 &= \prod_{\omega \in \mathbb{U}_m} (X - \omega) \wedge \prod_{\omega \in \mathbb{U}_n} (X - \omega) \\ &= \prod_{\omega \in \mathbb{U}_m \cap \mathbb{U}_n} (X - \omega) \\ &= \prod_{\omega \in \mathbb{U}_{m \wedge n}} (X - \omega) = X^{m \wedge n} - 1 \end{aligned}$$

Justifions le fait que $\mathbb{U}_n \cap \mathbb{U}_m = \mathbb{U}_{n \wedge m}$.

→ ($\subset$) Pour tout $z \in \mathbb{U}_{n \wedge m}$, on a $z^n = 1$ et $z^m = 1$ car $n \wedge m$ divise n et m.

→ ($\supset$) D'après Bezout, il existe $a, b \in \mathbb{Z}$ tels que $am + bn = a \wedge b$, donc pour tout $z \in \mathbb{U}_n \cap \mathbb{U}_m$, on a $z^{n \wedge m} = (z^n)^a \cdot (z^m)^b = 1$, i.e. $z \in \mathbb{U}_{n \wedge m}$.

Proposition (Localisation des racines) II.3.

Soit $P \in \mathbb{C}_n[X]$ unitaire : $P = X^n + a_{n-1}X^{n-1} + \cdots + a_0$. Pour tout $z \in \mathbb{C}$, si $P(z) = 0$, alors

$$|z| \leq 1 + \max_{k \in [\![0;n]\!]} |a_k|$$

Preuve : La preuve de ce résultat a déjà été faite au chapitre 1.

Proposition II.4.

Pour toute suite $(P_k)_k$ à valeurs dans $\mathbb{C}_n[X]$, la suite de fonctions (P_k) converge simplement vers $P \in \mathbb{C}_n[X]$ si et seulement si les coefficients de (P_k) convergent vers ceux de P.

Preuve

→ (⇐) Supposons que les coefficients de (P_k) convergent vers ceux de P. Soit $a \in \mathbb{C}$. Il est facile de voir que $P_k(a) \xrightarrow[k\to+\infty]{} P(a)$ en passant à la limite.

→ (⇒) Supposons que (P_k) converge simplement vers P. Soit $b_0, \dots, b_n \in \mathbb{C}$ deux à deux différents. Considérons les deux normes suivantes dans $\mathbb{C}_n[X]$

$$\|.\|_{\infty,coeff} : \begin{cases} \mathbb{C}_n[X] & \longrightarrow \mathbb{R}^+ \\ P & \longmapsto \max\limits_{i\in[\![0;n]\!]} |\alpha_i| \end{cases} \qquad \|.\| : \begin{cases} \mathbb{C}_n[X] & \longrightarrow \mathbb{R}^+ \\ P & \longmapsto \sum\limits_{i=0}^{n} |P(b_i)| \end{cases}$$

avec $P(X) = \alpha_n X^n + \dots + \alpha_1 X + \alpha_0$.
$\mathbb{C}_n[X]$ est de dimension finie, donc les normes $\|.\|_{\infty,coeff}$ et $\|.\|$ sont équivalentes. Le fait que (P_k) converge simplement vers P implique que (P_k) converge vers P pour $\|.\|$ et donc par équivalence des normes, P_k converge vers P pour $\|.\|_{\infty,coeff}$, i.e. les coefficients des termes de (P_k) convergent vers ceux de P.

Exercice II.5.

Soit $n \geq 1$ et $(P_k)_{k\in\mathbb{N}}$ une suite de polynômes unitaires de $\mathbb{C}_n[X]$. On suppose que (P_k) converge simplement vers $P \in \mathbb{C}_n[X]$ unitaire de degré n. Soit U un ouvert non vide de $\mathbb{C}$ tel que U contient $l \in \mathbb{N}$ racines de P comptées avec multiplicité et qu'aucune racine de P n'est dans la frontière de U qu'on note $\partial U = \overline{U} \backslash U$. Montrer qu'il existe $K \in \mathbb{N}$ tel que pour tout $k \geq K$, U contient exactement l racines de P_k comptées avec multiplicité.

III Polynômes réels

Proposition III.1.

Les polynômes irréductibles (unitaires) de $\mathbb{R}[X]$ sont ceux de la forme

→ $X - a$ avec $a \in \mathbb{R}$.

→ $X^2 - aX + b$ avec $a, b, c \in \mathbb{R}$ et $\Delta = a^2 - 4b < 0$.

Preuve : Soit $P \in \mathbb{R}[X]$ unitaire non constant. Si $\deg P \geq 3$, alors deux cas se présentent.

→ P admet une racine $z \in \mathbb{R}$, et alors P est réductible car il est divisible par $X - z$.

→ P admet une racine $z \in \mathbb{C} \setminus \mathbb{R}$ et P est à coefficients réels, donc $\overline{z}$ est aussi une racine de P. P est alors divisible par $(X - z)(X - \overline{z}) = X^2 - 2\mathrm{Re}(z) + |z|^2 \in \mathbb{R}[X]$ et est donc réductible.

Si $\deg P = 1$, alors d'une manière évidente P s'écrit $X - a$ avec $a \in \mathbb{R}$ et est irréductible et si $\deg P = 2$, alors P est irréductible s'il n'admet pas de racine réelle, i.e. son discriminant est négatif.

Remarque : Les polynômes irréductibles de $\mathbb{R}[X]$ de degré 2 s'écrivent aussi de la forme $(X - a)^2 + b^2$ avec $a \in \mathbb{R}$ et $b > 0$.

Exercice III.2.

Montrer que tout polynôme $P \in \mathbb{R}[X]$ positif sur $\mathbb{R}$ s'écrit de la forme $P = A^2 + B^2$ avec $A, B \in \mathbb{R}[X]$.

Proposition III.3.

Soit $P \in \mathbb{R}[X]$ non constant unitaire : $P(X) = X^n + a_{n-1}X^{n-1} + \cdots + a_0$

1. Si P est scindé alors P' et $P + \alpha P', \alpha \in \mathbb{R}$ aussi. Si P est dissocié (i.e. scindé à racines simples), P' aussi.
2. Si P est dissocié alors $\forall k \in [\![0, n-1]\!], a_k^2 + a_{k+1}^2 > 0$.
3. Si P est scindé, alors $\forall k \in [\![1, n-1]\!], a_k a_{k+2} \leq a_{k+1}^2$.
4. Si une suite $(P_k) \in \mathbb{R}_n[X]^{\mathbb{N}}$ de polynômes non constants unitaires scindés (pas forcément tous de même degré) converge simplement vers un polynôme $Q \in \mathbb{R}[X]$, alors Q est non constant et est scindé.

Preuve :

1. Montrons la propriété successivement pour P' et $P + \alpha P'$.

   → Si $a_1 < \cdots < a_r$ sont les racines de P de multiplicités respectives $\alpha_1, \ldots \alpha_r$, alors pour tout i, a_i est racine de P' de multiplicité $\alpha_i - 1$. On trouve ainsi $\alpha_1 + \cdots + \alpha_r - r = n - r$ racines de P' avec multiplicité. De plus, en appliquant le théorème de Rolle sur les segments $[a_i, a_{i+1}]$ on peut affirmer que P' s'annule en $b_1, \ldots, b_{r-1}$ tels que $a_1 < b_1 < a_2 < \cdots < a_{r-1} < b_{r-1} < a_r$, soit $r-1$ racines (simples) supplémentaires. On a donc un total de $n - r + r - 1 = n - 1$ racines de P' comptées avec multiplicité et P' est de degré n-1, donc P' est scindé. Cette preuve montre aussi que P' est dissocié si P l'est.

   → Soit $\alpha \in \mathbb{R}$. Si $\alpha = 0$ alors il s'agit du cas précédent. Sinon considérons $f : t \longmapsto e^{\beta t}P(t)$ où $\beta = \dfrac{1}{\alpha}$. On a alors pour tout $t \in \mathbb{R}$,

   $$f'(t) = 0 \iff e^{\beta t}(\beta P(t) + P'(t)) = 0 \iff P(t) + \alpha P'(t) = 0$$

   Le reste est similaire à la discussion précédente : Si λ est racine de P de multiplicité $\delta \geq 1$ alors elle l'est dans $P + \alpha P'$ de multiplicité exactement $\delta - 1$. Pour retrouve les autres racines manquantes, il suffit d'appliquer Rolle à f entre chaque deux racines consécutives.

   Remarquons au passage que cette propriété n'est pas vraie pour tout corps $\mathbb{K}$. En effet, lorsque $\mathbb{K} = \mathbb{Q}[\sqrt{6}]$ et $P(X) = X^3 - 6X$, on voit que P est scindé dans $\mathbb{K}$ mais pas P'.

2. Supposons que P et dissocié. Procédons par l'absurde. Supposons qu'il existe $k \in [\![0; n-1]\!]$ tel que $a_k = a_{k+1} = 0$. On a alors

   $$P^{(k)}(X) = k!a_k + (k+1)!a_{k+1}X + \frac{(k+2)!}{2}a_{k+2}X^2 + \cdots + \frac{n!}{(n-k)!}a_n X^{n-k}$$

   0 est alors racine de multiplicité 2. De plus, P est dissocié et donc d'après la propriété précédente, $P^{(k)}$ aussi, ce qui est absurde. On en déduit donc que pour tout $k \in [\![0; n-1]\!]$, $a_k^2 + a_{k+1}^2 > 0$.

3. On sait que

   $$\frac{P'}{P} = \sum_{i=1}^{n} \frac{1}{X - \lambda_i}$$

   avec les $\lambda_1, \ldots, \lambda_n$ les racines de P. Donc

   $$\left(\frac{P'}{P}\right)' = -\sum_{i=1}^{m} \frac{1}{(X - \lambda_i)^2} \text{ et alors } \frac{P''P - P'^2}{P^2} \leq 0$$

   sur $\mathbb{R} \setminus Z(P)$. On a alors en particulier, en le démontrant par la limite si $0 \in Z(P)$

   $$P''(0)P(0) - P'(0)^2 \leq 0$$

On remplace P par $P^{(k)}$, également scindé et on trouve

$$P^{(k+2)}(0)P^{(k)}(0) \leq P^{(k+1)}(0)^2$$

soit

$$(k+2)!a_{k+2}k!a_k \leq (k+1)!^2 a_{k+1}^2 \quad \text{puis} \quad a_{k+2}a_k \leq \frac{k+1}{k+2}a_{k+1}^2 \leq a_{k+1}^2$$

d'où le résultat.

4. Soit $(P_k) \in \mathbb{R}_n[X]^{\mathbb{N}}$ une suite de polynômes non constants unitaires scindés convergeant simplement vers $Q \in \mathbb{R}[X]$. Posons pour tout $k \in \mathbb{N}$ et $z \in \mathbb{C}$,

$$P_k(z) = \prod_{j=1}^{\deg P_k} (z - a_{k,j})$$

On a alors pour tout $z \in \mathbb{C} \setminus \mathbb{R}$,

$$|P_k(z)| = \prod_{j=1}^{\deg P_k} |z - a_{k,j}| \geq |\text{Im } z|^{\deg P_k} \geq \min(|\text{Im } z|, |\text{Im} z|^n)$$

En faisant tendre k vers l'infini, on obtient

$$|Q(z)| \geq \min(|\text{Im } z|^n, |\text{Im } z|) > 0$$

Q est donc soit constant soit scindé dans $\mathbb{R}$ (il n'a pas de racine complexe non réelle) car pour tout $z \in \mathbb{C} \setminus \mathbb{R}$, $Q(z) \neq 0$. Le premier cas est impossible car si $Q(X) = C$ est constant alors en prenant $z = i(1 + |C|)$, on obtient une contradiction avec l'inégalité.

Exercice III.4.

Trouver les $P \in \mathbb{R}[X]$ unitaires à coefficients dans $\{-1, 0, 1\}$ qui sont scindés sur $\mathbb{R}$.

Proposition (Formules de Vieta) III.5.

Soit $n \in \mathbb{N}^*$, $P(X) = a_0 + a_1X + \cdots + a_nX^n$ et $\lambda_1, \ldots, \lambda_n$ les racines (non nécessairement différentes) de P. Supposons que $a_n \neq 0$. On a pour tout $l \in [\![0; n]\!]$

$$\sum_{1 \leq i_1 < i_2 < \cdots < i_l \leq n} \left(\prod_{j=1}^{l} \lambda_{i_j} \right) = (-1)^l \frac{a_{n-l}}{a_n}$$

Preuve : Nous ne ferons par la preuve détaillée de ce résultat mais nous en donnerons uniquement l'idée principale. Pour voir d'où vient cette formule, il suffit de développer $a_n(X - \lambda_1) \ldots (X - \lambda_n)$ et d'identifier les coefficients de ce polynôme avec ceux de P. En particulier, il est facile de voir cette propriété pour $l = n$ et $l = 1$ qui s'écrivent

$$(-1)^n \frac{a_0}{a_n} = \lambda_1 \ldots \lambda_n \quad \text{et} \quad -\frac{a_{n-1}}{a_n} = \lambda_1 + \cdots + \lambda_n$$

IV Polynômes à coefficients rationnels

Exercice IV.1.

Soit $n \geq 1$, $a_0, \ldots, a_n \in \mathbb{Z}$ tels que $a_0 \neq 0$ et $a_n \neq 0$. On pose $P(X) = a_n X^n + \cdots + a_1 X + a_0$. Soit $a \in \mathbb{Q}$. Trouver une condition nécessaire sur a pour qu'il soit racine de P.

Exercice IV.2.

Soit $P \in \mathbb{Q}[X]$ irréductible et a une racine complexe de P. Montrer que a est une racine simple de P.

Exercice IV.3.

Soit $P \in \mathbb{Q}[X]$ de degré égal à 5. Montrer que si P admet une racine double dans $\mathbb{C}$, alors il possède une racine dans $\mathbb{Q}$.

V Irréductibilité de $\mathbb{Z}[X]$

Exercice V.1.

Soient $n \geq 1$ et $a_1, \ldots a_n \in \mathbb{Z}$ deux à deux distincts. Soit $P = 1 + \prod_{i=1}^{n}(X - a_i)^2$. Montrer que P est irréductible dans $\mathbb{Z}[X]$.

Exercice (Critère d'Eisenstein) V.2.

Soit $P(X) = X^n + a_{n-1}X^{n-1} + \cdots + a_0 \in \mathbb{Z}[X]$. On suppose qu'il existe un nombre premier p tel que $p^2 \nmid a_0$ et pour tout $i \in [\![0; n-1]\!]$, $p | a_i$. Montrer que P est irréductible dans $\mathbb{Z}[X]$.

Exercice V.3.

Montrer que X^4+1 est irréductible dans $\mathbb{Q}[X]$ et que pour tout p premier, X^4+1 est réductible dans $\mathbb{Z}/p\mathbb{Z}$.

VI Complément : lemme de Gauß

Dans cette partie, on dit que $P \in \mathbb{Z}[X] - \{0\}$ est irréductible dans $\mathbb{Z}[X]$ si on ne peut pas l'écrire sous forme de QR avec $Q, R \in \mathbb{Z}[X]$ et $\deg Q \geq 1$ et $\deg R \geq 1$. On mentionne ceci car pour certains auteurs $2X$ par exemple est réductible car 2 n'est pas inversible dans $\mathbb{Z}$. En d'autres termes, dans notre définition, les termes constants ne comptent pas comme un facteur même s'ils sont non inversibles dans $\mathbb{Z}$.

Exercice VI.1.

Le but de cet exercice est de montrer qu'un polynome $P \in \mathbb{Z}[X]$ non constant est irréductible dans $\mathbb{Z}[X]$ si et seulement s'il l'est sur $\mathbb{Q}[X]$. Le sens réciproque étant clair, on se propose alors de montrer le sens direct.

1. Posons pour tout polynôme $P = \sum_{k=0}^{n} a_k X^k$ non nul $c(P) = \bigwedge_{i=0}^{n} a_i$ son contenu. Montrer que
$$\forall P, Q \in \mathbb{Z}[X] - \{0\},\ c(PQ) = c(P)c(Q)$$
2. En déduire le résultat

Correction de l'exercice II.5 :

Notons pour tout polynôme Q, $F(Q)$ le nombre de racines de Q dans U. Supposons par l'absurde que la propriété qu'on veut démontrer est fausse, i.e.

$$\forall K \geq 0,\ \exists k \geq K,\ F(P_k) \neq l$$

D'une manière équivalente, que l'ensemble $A = \{k \in \mathbb{N},\ F(P_k) \neq l\}$ est infini. A étant infini, il existe une extractrice ψ telle que pour tout $k \in \mathbb{N}$, $\psi(k) \in A$. Pour alléger les notations, on va noter (P_k) au lieu de $(P_{\psi(k)})$ car $(P_{\psi(k)})$ converge aussi vers P.

On sait d'après la proposition II.4 que les coefficients des termes de (P_k) convergent vers ceux de P. En particulier, P étant unitaire, le coefficient devant X^n des termes de (P_k) converge vers 1 et est donc non nul à partir d'un certain rang et alors il existe $A > 0$ tel que pour tout $k \geq A$, $\deg P_k = n$. Posons alors pour tout $k \geq A$, $\lambda_{k,1}, \ldots, \lambda_{k,n}$ les racines de P_k. Les coefficients de P_k convergent et sont donc tous bornés. En utilisant la proposition II.3, on peut en déduire que les suites $(\lambda_{k,1})_{k\geq A}, \ldots, (\lambda_{k,n})_{k\geq A}$ sont toutes bornées. Par conséquent, d'après Bolzano-Weierstraß, il existe une extractrice φ (la même pour les n suites, quitte à faire des extractions successives) et $\lambda_1, \ldots, \lambda_n$ tels que

$$\forall i \in [\![1; n]\!],\ \lambda_{\varphi(k),i} \xrightarrow[k\to+\infty]{} \lambda_i$$

En utilisant ce qu'on vient de voir, il est facile de voir (soit en utilisant les relations coefficient racines, ou alors en passant par la convergence simple) que

$$P_{\varphi(k)}(X) = \prod_{i=1}^{n}(X - \lambda_{\varphi(k),i}) \xrightarrow[k\to+\infty]{} \prod_{i=1}^{n}(X - \lambda_i)$$

coefficient par coefficient et donc que $P(X) = \displaystyle\prod_{i=1}^{n}(X - \lambda_i)$. On a alors pour tout $i \in [\![1; n]\!]$,

- → Soit $\lambda_i \in U$, et alors U étant ouvert, il existe $K > 0$ tel que pour tout $k > K$, $\lambda_{i,\varphi(k)} \in U$
- → Soit $\lambda_i \notin U$ et alors par hypothèse (pas de racines dans la frontière) $\lambda_i \in \mathbb{C} \setminus \overline{U}$. Cet ensemble est ouvert, il existe donc $K > 0$ tel que pour tout $k \geq K$, $\lambda_{i,\varphi(k)} \in \mathbb{C} \setminus \overline{U}$ et alors $\lambda_{i,\varphi(k)} \notin U$.

Ceci permet de dire que pour k assez grand, $\lambda_{i,\varphi(k)}$ et λ_i sont soit tous les deux dans U soit tout les deux à l'extérieur de U et donc en particulier que $F(P_{\varphi(k)}) = F(P) = l$, ce qui est absurde par hypothèse.

Correction de l'exercice III.2. :

Posons

$$\mathcal{S} = \{P \in \mathbb{R}[X],\ \exists A, B \in \mathbb{R}[X],\ P = A^2 + B^2\}$$

Le but de l'exercice est de montrer que l'ensemble des polynômes positifs sur $\mathbb{R}$ est inclus dans $\mathcal{S}$ (au passage, ces deux ensembles sont égaux car l'inclusion réciproque est évidente).
Montrons d'abord que $\mathcal{S}$ est stable par multiplication. On a pour tout $A, B, C, D \in \mathbb{R}[X]$,

$$(A^2 + B^2)(C^2 + D^2) = (AC + BD)^2 + (AD - BC)^2$$

ce qui nous donne bien la stabilité par multiplication.

Soit P un polynôme positif sur $\mathbb{R}$. Si P est constant alors le résultat est évident. Supposons désormais $\deg P \geq 1$. On peut alors écrire

$$P(X) = \lambda \prod_{i=1}^{r}(X - a_i)^{\alpha_i} \prod_{i=1}^{s} \underbrace{(X^2 + b_i X + c_i)}_{\text{irréductible}}$$

avec pour tout i, $a_i, b_i, c_i \in \mathbb{R}$, $b_i^2 - 4c_i < 0$ et les a_i distincts. On a alors

→ $\lambda > 0$ car $P(x) \xrightarrow[x\to+\infty]{} +\infty$, donc $\lambda \in \mathcal{S}$.

→ Pour tout $i \in [\![1;s]\!]$, $X^2 + b_iX + c_i = \left(X + \frac{b_i}{2}\right)^2 + \sqrt{\frac{-b_i^2+4c_i}{4}}^2 \in \mathcal{S}$.

→ Pour tout $i \in [\![1;r]\!]$, on peut écrire $P(X) = Q(X)(X-a_i)^{\alpha_i}$ avec $Q \in \mathbb{R}[X]$. a_i n'est pas racine de Q, donc $Q(a_i) \neq 0$ et alors $Q(a_i) > 0$. Il existe donc $\varepsilon > 0$ tel que pour tout $x \in]a_i - \varepsilon, a_i]$, $Q(x) > 0$ et alors pour tout $x \in]a_i-\varepsilon, a_i]$, $(x-a_i)^{\alpha_i} \geq 0$, ce qui nous donne nécessairement que α_i est pair. On en déduit que $(X-a_i)^{\alpha_i} = \left((X-a_i)^{\frac{\alpha_i}{2}}\right)^2 \in \mathcal{S}$.

P est donc produit d'éléments de $\mathcal{S}$ et donc par stabilité par multiplication, il est bien dans $\mathcal{S}$.

Correction de l'exercice III.4. :

On suppose $P(X) = a_nX^n + \cdots + a_1X + a_0$ scindé avec $a_n = 1$. On se ramène à $P(0) \neq 0$ en factorisant éventuellement par X^k pour k la valuation de P (0 sera alors racine réelle et le caractère scindé du polynôme en sera inchangé).

Soient $x_1, \ldots, x_n$ les racines de P. On a,

$$\prod_{k=1}^{n} x_n = (-1)^n P(0) \quad \text{donc} \quad \prod_{k=1}^{n} x_k^2 = P(0)^2 = 1$$

Pour obtenir la première égalité, il suffit de remplacer X par 0 dans la décomposition de P.

L'inégalité arithmético-géométrique donne alors

$$\sum_{k=1}^{n} x_k^2 \geq n\sqrt[n]{x_1^2 \ldots x_n^2} = n \tag{1}$$

et en utilisant les formules de Vieta,

$$n \leq \sum_{k=1}^{n} x_k^2 = \left(\sum_{k=1}^{n} x_k\right)^2 - 2\sum_{k<l} x_kx_l = (-a_{n-1})^2 - 2a_{n-2} \leq a_{n-1}^2 + 2\,|a_{n-1}| \leq 3 \tag{2}$$

et donc $n \leq 3$. Le cas $n = 3$ impose le cas d'égalité dans les inégalités ci-dessus

→ Égalité dans (1), i.e. le cas d'égalité de l'inégalité arithmético-géométrique qui donne nécessairement : $x_1^2 = \cdots = x_n^2$. En utilisant l'égalité $\prod_1^n x_k^2 = 1$ on obtient que $x_1^2 = \cdots = x_n^2 = 1$ i.e. $Z(P) \subset \{-1, 1\}$.

→ Égalité dans l'inégalité de droite de (2), i.e. $a_{n-1}^2 - 2a_{n-2} = 3 \Longleftrightarrow a_{n-1} = \pm 1$ et $a_{n-2} = -1$.

En particulier, la condition $n = 3$ impose que

$$P \in \{\underbrace{(X-1)^3}_{P_1}, \underbrace{(X-1)^2(X+1)}_{P_2}, \underbrace{(X-1)(X+1)^2}_{P_3}, \underbrace{(X+1)^3}_{P_4}\}$$

Il est clair que les coefficients de P_1 et P_4 ne sont pas tous dans $\{-1, 0, 1\}$ et donc ne vérifient pas les conditions voulues. Cependant P_2 et P_3 conviennent.
Pour le cas $n = 2$, on peut écrire $P = X^2 + aX + b$ où $b = \pm 1$ et $a \in \{-1, 0, 1\}$. La condition est alors $\Delta = a^2 - 4b \geq 0$ et donc les seuls polynômes convenables sont $X^2 - X - 1, X^2 - 1$ et $X^2 + X - 1$.
Pour $n = 1$ la propriété voulue est toujours vérifiée. En posant donc

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

On déduit que l'ensemble des polynômes scindés à coefficients dans $\{-1, 0, 1\}$ est égal à

$$\{X^kQ,\ k \in \mathbb{N},\ Q \in A\}$$

Correction de l'exercice IV.1. :

Soit a une racine de P. On a $a_0 \neq 0$ donc $a \neq 0$. Posons $a = \frac{p}{q}$ avec $p \wedge q = 1$. On a alors $P\left(\frac{p}{q}\right) = 0$, i.e.

$$a_n p^n + a_{n-1}p^{n-1}q + \cdots + a_1 pq^{n-1} + a_0 q^n = 0$$

On a alors $p|a_0q^n$ et $q|a_np^n$ et donc par Gauß, $p|a_0$ et $q|a_n$.

Correction de l'exercice IV.2. :

Les seuls diviseurs unitaires de P sont P et 1 car P est irréductible, donc $P \wedge P' \in \{1, P\}$. Mais $\deg P' < \deg P$ donc P ne peut pas diviser P' et alors $P \wedge P' = 1$. On a alors d'après Bezout,

$$\exists U, V \in Q[X],\ UP + VP' = 1$$

En évaluant en a, on a $\underbrace{U(a)P(a)}_{=0} + V(a)P'(a) = 1$ et alors nécessairement $P'(a) \neq 0$, i.e. a est une racine simple de P.
Remarquer aussi que dire $P \wedge P' = 1$ est équivalent à dire que P et P' n'ont aucune racine complexe commune et que donc, en particulier, a n'est pas racine de P', ce qui fournit le résultat.

Correction de l'exercice IV.3. :

Supposons sans perte de généralité que P est unitaire. P admet une racine double dans $\mathbb{C}$, donc d'après l'exercice précédent, P est réductible. On écrit $P = QR$ avec Q, R non constants, unitaires et irréductibles (s'il y a plus de deux facteurs irréductibles non constants, au moins un sera de degré 1 et donc P admet une racine rationnelle). Le cas $Q = R$ étant impossible vu que $\deg(P) = 5$ est impair, on a alors que Q et R sont premiers entre eux. En effet, Q et R étant irréductibles unitaires, on a $Q \wedge R \in \{1, Q\} \cap \{1, R\} = \{1\}$.

- → Si $\deg Q = 1$, alors $Q = X - r$, avec $r \in \mathbb{Q}$ et donc r est racine rationnelle de P.
- → Si $\deg Q = 2$, alors a est racine double de P mais d'après l'exercice précédent n'est racine double ni de Q ni de R et donc $Q(a) = R(a) = 0$ ce qui est absurde car $Q \wedge R = 1$.

On a donc bien le résultat voulu.

Correction de l'exercice V.1. :

Supposons par l'absurde que P est réductible. Il existe donc $Q, R \in \mathbb{Z}[X]$ tels que $\deg Q \geq 1$, $\deg R \geq 1$ et $P = QR$. On a alors

$$\forall i \in [\![1; n]\!],\ \underbrace{Q(a_i)}_{\in \mathbb{Z}} \underbrace{R(a_i)}_{\in \mathbb{Z}} = P(a_i) = 1$$

et alors

$$\forall i \in [\![1; n]\!],\ Q(a_i) = R(a_i) = \pm 1$$

De plus P est positif et ne s'annule pas sur R, donc Q et R aussi, sont de signe constant et ont le même signe. On suppose que $Q > 0$ et $R > 0$ (le cas $Q < 0$ et $R < 0$ se traite de la même manière), chose qui implique en particulier que Q et R sont unitaires (P est unitaire). On a alors

$$\forall i \in [\![1; n]\!],\ Q(a_i) - 1 = 0 \text{ et } R(a_i) - 1 = 0$$

$Q - 1$ et $R - 1$ admettent n racines distinctes, sont donc de degré au moins n et la somme de leurs degrés est $2n$. On en déduit que $\deg Q = \deg R = n$ et

$$Q(X) - 1 = R(X) - 1 = \prod_{i=1}^{n} (X - a_i)$$

et que finalement

$$\prod_{i=1}^{n}(X-a_i)^2+1=P(X)=\left(\prod_{i=1}^{n}(X-a_i)+1\right)^2$$

ce qui est absurde. P est donc bien irréductible.

Correction de l'exercice V.2. :

Supposons par l'absurde que P est réductible dans $\mathbb{Z}[X]$, i.e. il existe $Q,R\in\mathbb{Z}[X]$ de degré supérieur ou égal à 1 tels que $P=QR$, qu'on peut supposer unitaires (P est unitaire). Il existe donc $r,s\in\mathbb{N}^*$, $(b_i)_{i\in[\![0;r-1]\!]}\in\mathbb{Z}^r$ et $(c_i)_{i\in[\![0;s-1]\!]}\in\mathbb{Z}^r$ tels que

$$Q(x)=X^r+b_{r-1}X^{r-1}+\cdots+b_1X+b_0 \quad \text{et} \quad R(X)=X^s+c_{s-1}X^{s-1}\cdots+c_1X+c_0$$

On passe dans $\mathbb{Z}/p\mathbb{Z}[X]$: comme $\forall i\in[\![0;n-1]\!], a_i\equiv 0[p]$, on peut écrire dans $\mathbb{Z}/p\mathbb{Z}[X]$

$$P(X)=X^n+\underbrace{\overline{a_{n-1}}X^{n-1}+\cdots+\overline{a_1}X+\overline{a_0}}_{=\overline{0}}=X^n$$

De plus, on a également dans $\mathbb{Z}/p\mathbb{Z}[X]$

$$X^n=P(X)=Q(X)R(X)=(X^r+\overline{b_{r-1}}X^{r-1}+\cdots+\overline{b_1}X+\overline{b_0})(X^s+\overline{c_{s-1}}X^{s-1}\cdots+\overline{c_1}X+\overline{c_0})$$

Or par unicité de la décomposition de X^n en facteurs irréductibles dans $\mathbb{Z}/p\mathbb{Z}[X]$, $Q(X)$ et $R(X)$ doivent être de la forme X^{s_1} et X^{s_2}. Pour qu'on ait la bonne puissance, il est nécessaire que $s_1=r$ et $s_2=s$, i.e., dans $\mathbb{Z}/p\mathbb{Z}[X]$, $Q(X)=X^r$ et $R(X)=X^s$, et alors

$$\overline{b_{r-1}}=\cdots=\overline{b_1}=\overline{b_0}=\overline{c_{s-1}}=\cdots=\overline{c_1}=\overline{c_0}=\overline{0}$$

Or $a_0=c_0b_0$ et d'après l'égalité ci-dessus, $p|b_0$ et $p|c_0$ et donc $p^2|a_0$, ce qui est absurde.

Correction de l'exercice V.3. :

→ Irréductibilité dans $\mathbb{R}[X]$.
On décompose X^4+1

$$X^4+1=(X^2+1)^2-2X^2=\underbrace{(X^2+\sqrt{2}X+1)}_{A(X)}\underbrace{(X^2-\sqrt{2}X+1)}_{B(X)}$$

Si X^4+1 était réductible dans $\mathbb{Q}[X]$, on pourrait écrire $X^4+1=QR$ tel que $Q,R\in\mathbb{Q}[X]$, $\deg R\geq\deg Q\geq 1$ et Q et R sont unitaires. Le cas $\deg Q=1$ est impossible car X^4+1 n'admet pas de racine rationnelle. Le cas $\deg Q=2$ est impossible car par unicité de la décomposition en facteurs irréductibles dans $\mathbb{R}[X]$, on aurait $Q,R\in\{A,B\}$ ce qui est absurde car $A,B\notin\mathbb{Q}[X]$. On en déduit donc que X^4+1 est irréductible dans $\mathbb{Q}[X]$.

→ Irréductibilité dans $\mathbb{Z}/p\mathbb{Z}$.
Si $p=2$, alors on peut écrire dans $\mathbb{Z}/p\mathbb{Z}$

$$X^4+\overline{1}=X^4+\overline{2}X^2+\overline{1}=(X^2+\overline{1})^2$$

donc X^4+1 est réductible. Supposons maintenant $p\geq 3$.

- Si $\overline{2}$ est un carré modulo p, i.e. il existe $a\in\mathbb{Z}/p\mathbb{Z}$ tel que $a^2=\overline{2}$, on peut écrire

$$X^4+1=(X^2+\overline{1})^2-\overline{2}X^2=(X^2+\overline{1})^2-a^2X^2=(X^2+\overline{1}+a)(X^2+\overline{1}-a)$$

- Si $\overline{-2}$ est un carré modulo p, i.e. il existe $b \in \mathbb{Z}/p\mathbb{Z}$ tel que $b^2 = \overline{-2}$, on peut écrire
$$X^4 + 1 = (X^2 - \overline{1})^2 - \overline{-2}X^2 = (X^2 - \overline{1})^2 - b^2X^2 = (X^2 + \overline{1} + b)(X^2 + \overline{1} - b)$$
- Supposons maintenant que ni $\overline{2}$ ni $\overline{-2}$ ne sont des carrés modulo p. On a alors d'après le chapitre 21, $\overline{2}^{\frac{p-1}{2}} = \overline{-1}$ et $\overline{-2}^{\frac{p-1}{2}} = \overline{-1}$ et donc en faisant le produit des deux, $\overline{-4}^{\frac{p-1}{2}} = \overline{1}$. On peut donc écrire $\overline{1} = \overline{-4}^{\frac{p-1}{2}} = \overline{-1}^{\frac{p-1}{2}} \times \overline{4}^{\frac{p-1}{2}} = \overline{-1}^{\frac{p-1}{2}}$ ce qui nous permet de dire que -1 est un carré modulo p. En posant $c^2 = \overline{-1}$ avec $c \in \mathbb{Z}/p\mathbb{Z}$, on peut finalement écrire
$$X^4 + \overline{1} = X^4 - \overline{-1} = X^4 - c^2 = (X^2 - c)(X^2 + c)$$

On en déduit donc que $X^4 + 1$ est bien réductible dans $\mathbb{Z}/p\mathbb{Z}[X]$.

Correction de l'exercice VI.1. :

1. Il est facile de voir que pour tout $P(X) = \sum_{i=0}^{n} a_k X^k \in \mathbb{Z}[X] \setminus \{0\}$ et $a \in \mathbb{N}^*$ tel que $a|c(P)$,
$$\frac{1}{a}c(P) = \bigwedge_{i=0}^{n} \frac{a_i}{a} = c\left(\frac{P}{a}\right)$$
Donc montrer le résultat voulu est équivalent à montrer que
$$c\left(\frac{P}{c(P)} \times \frac{Q}{c(Q)}\right) = 1$$
et donc quitte à remplacer $\frac{P}{c(P)}$ par P et $\frac{Q}{c(Q)}$ par Q, il suffit de montrer que
$$\forall P, Q \in \mathbb{Z}[X] \setminus \{0\},\ c(P) = c(Q) = 1 \Longrightarrow c(PQ) = 1$$
Soient $P, Q \in \mathbb{Z}[X] \setminus \{0\}$ et $p \in \mathbb{Z}$ premier. Si $p|c(PQ)$, alors dans $\mathbb{Z}/p\mathbb{Z}[X]$, $PQ = 0$ (car p divise tous les coefficients de PQ) et alors, $\mathbb{Z}/p\mathbb{Z}$ étant intègre, $P = 0$ ou $Q = 0$ dans $\mathbb{Z}/p\mathbb{Z}[X]$ et alors p divise tous les coefficients de P ou tous les coefficients de Q, i.e. $p|c(P)$ ou $p|c(Q)$ ce qui est absurde car $c(P) = c(Q) = 1$. On en déduit donc qu'on a bien $c(PQ) = 1$.
2. Soit $P \in \mathbb{Z}[X] \setminus \{0\}$ réductible dans $\mathbb{Q}[X]$. Étant donné que diviser P par un entier (qui divise tous les coefficients pour rester dans $\mathbb{Z}[X]$) ne change pas fait que P soit irréductible ou non dans $\mathbb{Z}[X]$, quitte à diviser par $c(P)$, on suppose que $c(P) = 1$.

   Soit $\lambda \in \mathbb{Z}$ le coefficient dominant de P. P étant réductible dans $\mathbb{Q}[X]$, il existe $Q, R \in \mathbb{Q}[X]$ unitaires tels que $\deg Q \geq 1$, $\deg R \geq 1$ et $P = \lambda QR$. On va montrer que λ s'écrit $\lambda = cd$ avec $c, d \in \mathbb{Z}$ et $cQ, dR \in \mathbb{Z}[X]$.

   Posons $a = \min \underbrace{\{k \geq 1,\ kQ \in \mathbb{Z}[X]\}}_{\neq \varnothing}$. On veut montrer que $c(aQ) = 1$. Supposons le contraire. On a alors $\dfrac{aQ}{c(aQ)} \in \mathbb{Z}[X]$, et $c(aQ)$ divise le coefficient dominant de aQ qui est égal à a, donc $\dfrac{a}{c(aQ)} \in \mathbb{N}^*$ ce qui contredit la minimalité de a. En posant donc $b = \min\{k \geq 1,\ kR \in \mathbb{Z}[X]\}$, on a de même $c(bR) = 1$. On a alors
$$ab = ab \cdot c(P) = c(abP) = c(\lambda \times aQ \times bR) = |\lambda| c(aQ)c(bR) = |\lambda|$$
   Quitte à changer le signe de a, on peut donc écrire $P = \underbrace{aQ}_{\in \mathbb{Z}[X]} \times \underbrace{bR}_{\in \mathbb{Z}[X]}$ et alors P est bien réductible dans $\mathbb{Z}[X]$.

On peut montrer d'une manière plus générale, par la même démonstration ci-haut, que si $P = \lambda \prod_{i=1}^{r} Q_i \in \mathbb{Z}[X] \setminus \{0\}$ est une factorisation de P dans $\mathbb{Q}[X]$ avec Q_i unitaires et λ le coefficient dominant de P, alors on peut écrire $\lambda = c(P)\lambda_1 \dots \lambda_r$ avec pour tout $i \in [\![1;r]\!]$, $\lambda_i \in \mathbb{Z}$ et $\lambda_i Q_i \in \mathbb{Z}[X]$. En particulier

→ Si $P = \lambda \prod_{i=1}^{r} Q_i$ est la factorisation en irréductibles dans $\mathbb{Q}[X]$, alors $P = c(P) \prod_{i=1}^{r} (\lambda_i Q_i)$ est une factorisation en irréductibles dans $\mathbb{Z}[X]$.

→ Pour tout $Q \in \mathbb{Z}[X] \setminus \{0\}$,

$$Q|P \text{ dans } \mathbb{Z}[X] \Longleftrightarrow Q|P \text{ dans } \mathbb{Q}[X] \text{ et } c(Q)|c(P)$$

Le cas particulier où $\pm Q$ est unitaire est assez connu et est une conséquence du fait qu'on peut effectuer la division euclidienne dans $\mathbb{Z}[X]$ par un polynôme unitaire (ou de coefficient dominant égal à -1) de $\mathbb{Z}[X]$ (en effet, lorsque $\mathbb{K}$ n'est pas un corps, on ne peut pas toujours faire la division euclidienne dans $\mathbb{K}[X]$) et du fait que la division euclidienne dans $\mathbb{Z}[X]$ (lorsqu'elle est faisable dans $\mathbb{Z}[X]$) et $\mathbb{Q}[X]$ donne toujours le même résultat.

→ Si P est unitaire et $P = \prod_{i=1}^{r} Q_i$ est une factorisation dans $\mathbb{Q}[X]$ avec les Q_i unitaires, alors pour tout $i \in [\![1;r]\!]$, $Q_i \in \mathbb{Z}[X]$. En effet, en reprenant les notations vu précédemment, $1 = c(P)\lambda_1 \dots \lambda_r$ implique que pour tout $i \in [\![1;r]\!]$, $\lambda_i \in \{-1, 1\}$. Cette propriété est particulièrement intéressante dans le cas où l'égalité $P = \prod_{i=1}^{r} Q_i$ est une factorisation en irréductibles dans $\mathbb{Q}[X]$, vu qu'elle donne que chaque facteur est en fait (unitaire et) dans $\mathbb{Z}[X]$.

* *
*

Document compilé par Omar Bennouna et Issam Tauil le 25/05/2022 pour cpge-paradise.com.
Si vous repérez une erreur, ou avez des remarques, prière de me contacter via l'adresse contact@cpge-paradise.com.