141 — Racines d'un polynôme, fonctions symétriques élémentaires, exemples et applications

Cadre : $\mathbb{K}$ est un corps, $x \in \mathbb{K}$, $P \in \mathbb{K}[X]$, A est un anneau commutatif unitaire.

$j = e^{\frac{2i\pi}{3}}$, racine troisième de l'unité

I - Racines d'un polynôme

1 - Racines et multiplicité

Def 1 : $x \in \mathbb{K}$ est racine de P si $X - x \mid P$

Ex 2 : -1 est racine de $X^2 + 3X + 2 = (X+1)(X+2) \in \mathbb{R}[X]$

Prop 3 : $x \in \mathbb{K}$ est racine de P ssi $P(x) = 0$

Def 4 : Soit $x \in \mathbb{K}$ une racine de P. On dit que x est de multiplicité $m \in \mathbb{N}^*$ si $(X - x)^m \mid P$ dans $\mathbb{K}[X]$

Prop 5 : Si $\mathrm{Car}(\mathbb{K}) = 0$, alors $x \in \mathbb{K}$ est racine de P de multiplicité $m \in \mathbb{N}^*$ si, et seulement si
$P(x) = \dots = P^{(m-1)}(x) = 0$ et $P^{(m)}(x) \neq 0$.

Rq 6 : Ce n'est plus vrai si $\mathrm{Car}(\mathbb{K}) \neq 0$.

C-Ex 7 : Si $P = X(X^2+1) \in \mathbb{F}_2[X]$, 1 est racine de multiplicité 2, bien que $P'' = 0$ (et $P''(1) = 0$ donc)

Prop 8 : Si $P \neq 0$ alors P admet au plus $\deg P$ racines dans $\mathbb{K}$, comptées avec leur multiplicité.

Réciproquement, si P admet au moins $\deg(P) + 1$ racines dans $\mathbb{K}$, comptées avec leur multiplicité, alors $P = 0$.

Appli 9 : (Polynôme interpolateur de Lagrange)
Soient $(x_0, \dots, x_m) \in \mathbb{K}^{m+1}$ (en général $\mathbb{K} = \mathbb{R}$ ou $\mathbb{C}$), distincts. Alors on a l'isomorphisme d'espaces vectoriels suivant

$$\Phi : \mathbb{K}_m[X] \longrightarrow \mathbb{K}^{m+1}, \quad P \longmapsto (P(x_0), \dots, P(x_m))$$

$\mathbb{K}_m[X] = \{P \in \mathbb{K}[X] : \deg(P) \leq m\}$

Def 10 : P est dit scindé sur $\mathbb{K}$ si P est produit de polynômes de degré 1 dans $\mathbb{K}[X]$.

Ex 11 : $P = X^3 + X$ est scindé dans $\mathbb{F}_2[X]$, en effet, $P = X(X+1)^2$

2 - Irréductibilité

Def 12 : P est dit irréductible sur $\mathbb{K}$ si, et seulement si
(i) P est non constant
(ii) $P = RQ$, $R, Q \in \mathbb{K}[X] \Rightarrow R$ ou Q est constant.

Ex 13 : Les polynômes de degré 1 sont irréductibles sur tout corps.

Prop 14 : Soit $P \in \mathbb{K}[X]$ tel que $\deg(P) \geq 2$. Si P est irréductible sur $\mathbb{K}[X]$ alors P n'admet pas de racines sur $\mathbb{K}$.
La réciproque est vraie si $\deg(P) \in \{2, 3\}$

Rq 15 : Peut être faux si $\deg(P) \geq 4$ (réciproque)

C-Ex 16 : $P = (X^2+1)^2 \in \mathbb{Q}[X]$ n'est pas irréductible, bien qu'il n'admette aucune racine dans $\mathbb{Q}$.

3 - Corps de rupture, corps de décomposition et clôture algébrique

Def 17 : Soit P irréductible sur $\mathbb{K}$. On appelle corps de rupture de P sur $\mathbb{K}$ toute extension de corps $\mathbb{L}$ sur $\mathbb{K}$ telle que
(i) $\mathbb{L} = \mathbb{K}(x)$ avec $x \in \mathbb{L}$
(ii) $P(x) = 0$

Prop 18 : Soit P irréductible. $\frac{\mathbb{K}[X]}{\langle P \rangle}$ est un corps de rupture de P sur $\mathbb{K}$, égal à $\mathbb{K}(\overline{X})$ où, on a :

$$\mathbb{K}[X] \longrightarrow \frac{\mathbb{K}[X]}{\langle P \rangle}, \quad X \longmapsto \overline{X}$$

Th 19 : Tout corps de rupture est unique à isomorphisme près.

Ex 20 : $\mathbb{C}$ est corps de rupture de X^2+1 sur $\mathbb{R}$

Prop 21 : Si $\deg(P) = n$, P est irréductible sur $\mathbb{K}$ ssi P n'a pas de racines dans les extensions $\mathbb{L}$ de $\mathbb{K}$ vérifiant $[\mathbb{L} : \mathbb{K}] \leq \frac{n}{2}$

Appli 22 : $X^4 + X + 1$ est irréductible dans $\mathbb{F}_2[X]$

Def 23 : $\mathbb{L}$ est corps de décomposition de P sur $\mathbb{K}$ si
(i) P est scindé dans $\mathbb{L}$
(ii) $\mathbb{L}$ est engendré par $\mathbb{K}$ et par les racines de P

Th 24 : Il existe un unique corps de décomposition à isomorphisme près.

Ex 25 : $\mathbb{Q}(\sqrt{2})$ est corps de décomposition de $X^2 - 2$ sur $\mathbb{Q}$

Def 26 : $\mathbb{K}$ est algébriquement clos si tout polynôme $P \in \mathbb{K}[X]$ de $\deg(P) \geq 1$, est scindé sur $\mathbb{K}$

C-Ex 27 : $\mathbb{Q}$ et $\mathbb{R}$ ne sont pas algébriquement clos

Prop 28 : Les corps finis ne sont pas algébriquement clos

Th 29 : (Théorème de d'Alembert - Gauss)
$\mathbb{C}$ est algébriquement clos

II - Polynômes symétriques

1 - Structure algébrique

Déf 30 : (Action de groupe) On a une action S_n sur $A[X_1, \dots, X_n]$ de la manière suivante : $\forall \sigma \in S_n$, $\forall P \in A[X_1, \dots, X_n]$, $(\sigma \cdot P)(X_1, \dots, X_n) = P(X_{\sigma(1)}, \dots, X_{\sigma(n)})$

Prop 31 : Pour tout $\sigma \in S_n$, $u_\sigma : A[X_1, \dots, X_n] \to A[X_1, \dots, X_n]$, $P \mapsto \sigma \cdot P$ est un automorphisme de A-algèbre, de réciproque $u_{\sigma^{-1}}$

Déf 32 : Soit $P \in A[X_1, \dots, X_n]$. On dit que P est un polynôme symétrique si et seulement si, $\forall \sigma \in S_n$, $\sigma \cdot P = P$

Ex 33 : (i) $X_1^2 + X_2^2$ est symétrique $(n = 2)$

(ii) Pour n quelconque, $V(X_1, \dots, X_n)^2 = \begin{vmatrix} 1 & X_1 & \cdots & X_1^{n-1} \\ \vdots & \vdots & & \vdots \\ 1 & X_n & \cdots & X_n^{n-1} \end{vmatrix} = \prod_{1 \leq i < j \leq n} (X_i - X_j)^2$

(carré du déterminant de Vandermonde) est un polynôme symétrique en n variables

Déf 34 : (Polynômes symétriques élémentaires)

Soit $n \in \mathbb{N}^*$. On définit les polynômes symétriques élémentaires par

$$\forall j \in [\![1,n]\!], \quad \Sigma_j^{(n)} = \sum_{\substack{I \subset [\![1,n]\!] \\ |I| = j}} \prod_{i \in I} X_i \in A[X_1, \dots, X_n]$$

Ex 35 : On a donc $\Sigma_1^{(n)} = X_1 + \dots + X_n$, $\Sigma_n^{(n)} = X_1 \cdots X_n$

Rq 36 : Chaque Σ_j est somme de $\binom{n}{j}$ monômes de degré j

Th 37 : (Théorème de structure des polynômes symétriques)

On a l'isomorphisme de A-algèbre suivant :

$$A[X_1, \dots, X_n] \longrightarrow A[\Sigma_1^{(n)}, \dots, \Sigma_n^{(n)}]$$
$$P \longmapsto P(\Sigma_1^{(n)}, \dots, \Sigma_n^{(n)})$$

Ex 38 : Si $P = X_1^2 + \dots + X_n^2$ alors $P = Q(\Sigma_1^{(n)}, \Sigma_2^{(n)})$ où $Q(X_1, X_2) = X_1^2 - 2X_2$.

2 - Relations coefficients - racines

Dans cette sous-partie, $P = \sum_{k=0}^{n} a_k X^k$, $a_n \neq 0$, $a_k \in A$, $\forall k \in [\![0,n]\!]$

Prop 39 : Soient $\alpha_1, \dots, \alpha_n \in A$ les racines de P, comptées avec leur multiplicité. Alors, si $P = a_n(X - \alpha_1) \cdots (X - \alpha_n)$, on a :

$$\forall k \in [\![1,n]\!], \quad a_{n-k} a_n^{-1} = (-1)^k \Sigma_k^{(n)}(\alpha_1, \dots, \alpha_n)$$

Ex 40 : Si $P = aX^2 + bX + c$, $a, b, c \in \mathbb{K}$, $a \neq 0$, alors si $P = a(X - x_1)(X - x_2)$ on a $\frac{b}{a} = -(x_1 + x_2)$, $\frac{c}{a} = x_1 x_2$

Appli 41 : (Systèmes somme-produit)

Le système somme-produit $\begin{cases} z_1 + z_2 = u \\ z_1 z_2 = v \end{cases}$, $u, v \in \mathbb{C}$, $z_1, z_2 \in \mathbb{C}$, revient à $z^2 - uz + v = 0$

Prop 42 : (Identités de Newton)

Si on pose $S_k^{(n)}(X_1, \dots, X_n) = \sum_{j=1}^{n} X_j^k$ alors, en adoptant la convention $\forall k > n$, $\Sigma_k^{(n)}(X_1, \dots, X_n) = 0$, on a

$$\forall k \in \mathbb{N}^*, \quad k \Sigma_k^{(n)} = \sum_{i=1}^{k} (-1)^{i+1} \Sigma_{k-i}^{(n)} S_i^{(n)}$$

Appli 43 : Si $\mathrm{Car}(\mathbb{K}) = 0$, $M \in \mathcal{M}_n(\mathbb{K})$. M est nilpotente ssi $\forall k \in [\![1,n]\!]$, $\mathrm{Tr}(M^k) = 0$

III - Applications

1 - Réduction d'endomorphismes

Cadre : Dans cette sous-partie, E est un $\mathbb{K}$-ev de dimension finie n et $u \in \mathcal{L}_{\mathbb{K}}(E)$

Déf 44 : (Polynôme caractéristique)

Le polynôme caractéristique de u est donné par $\chi_u = \det(X\mathrm{Id}_E - u)$

Rq 45 : C'est un polynôme de degré n sur $\mathbb{K}$

Déf 46 : (Spectre) On dit que $\lambda \in \sigma(u)$ (spectre, λ est une valeur propre) ssi $\exists x \neq 0$, $u(x) = \lambda x$

Prop 46-bis : $\sigma(u) = \{\text{Racines de } \chi_u\}$

Prop 47 : u est trigonalisable ssi χ_u est scindé sur $\mathbb{K}$

Appli 48 : $\forall M \in \mathcal{M}_n(\mathbb{C})$, M est trigonalisable.

Prop 49 : Soit $u \in \mathcal{L}_{\mathbb{R}}(\mathbb{R}^{2m+1})$. Alors u admet une valeur propre réelle.

Déf 50 : (Multiplicité des valeurs propres) Soit $\lambda \in \sigma(u)$

(i) Multiplicité algébrique $m_\lambda(u) :=$ Multiplicité de λ dans χ_u

(ii) Multiplicité géométrique $g_\lambda(u) = \dim_{\mathbb{K}}(SEP(u, \lambda))$ (Sous-espace propre $= \mathrm{Ker}(u - \lambda \mathrm{Id})$)

Rq 51 : $\forall \lambda \in \sigma(u)$, $m_\lambda(u) \geq g_\lambda(u)$

Prop 52 : u est diagonalisable si et seulement si χ_u est scindé et, pour tout $\lambda \in \sigma(u)$, $m_\lambda(u) = g_\lambda(u)$

Rq 52-bis : Si χ_u est scindé à racines simples, alors u est diagonalisable

C-Ex 53 : $A = \begin{bmatrix} 1 & 1 \\ 0 & 1 \end{bmatrix}$, $\chi_A = (X-1)^2$, $\dim(SEP(A, 1)) = 1$, A n'est pas diagonalisable

2 - Cas particulier du degré 2 ou 3

Th 54 : (Polynômes de degré 2)

Si $P = aX^2 + bX + c$, $a, b, c \in \mathbb{R}$, $a \neq 0$, soit $\Delta = b^2 - 4ac$ (discriminant de P)

(i) Si $\Delta < 0$, alors P admet deux racines conjuguées $\dfrac{-b \pm i\sqrt{|\Delta|}}{2a}$

(ii) Si $\Delta = 0$, alors P admet une racine double réelle $\dfrac{-b}{2a}$

(iii) Si $\Delta > 0$, alors P admet deux racines réelles simples $\dfrac{-b \pm \sqrt{\Delta}}{2a}$ (cf. Fig 1)

Appli 54-bis : Équations différentielles linéaires à coefficients constants d'ordre 2.

Appli 54-ter : (le laplacien discret 1D)

Soit $n \in \mathbb{N} \setminus \{0, 1, 2\}$. Soit $A_n = (n+1)^2 A^{(n)}$, où $A^{(n)} = \begin{pmatrix} 2 & -1 & & (0) \\ -1 & \ddots & \ddots & \\ & \ddots & \ddots & -1 \\ (0) & & -1 & 2 \end{pmatrix} \in \mathcal{M}_n(\mathbb{R})$ DVPT 1

On a alors : (i) $A^{(n)} \in S_n^{++}(\mathbb{R})$

(ii) $\sigma(A^{(n)}) = \left\{ 2 - 2\cos\left(\frac{p\pi}{n+1}\right), p \in [\![1, n]\!] \right\}$

Coro 55 : Si $\mathrm{Cond}_2(A) = |||A|||\,|||A^{-1}|||$, alors $\mathrm{Cond}_2(A_n) \underset{n \to +\infty}{\sim} \frac{4n^2}{\pi^2}$

Th 56. (Formules de Cardan)

Soient $p, q \in \mathbb{R}$. Les racines complexes du polynôme $P = X^3 + pX + q$ sont z_k, $k \in [\![0, 2]\!]$, et sont données par $z_k = u_k + v_k$, où, $\forall k \in [\![0, 2]\!]$,

$$u_k = j^k \sqrt[3]{\frac{1}{2}\left(-q + \sqrt{\frac{-\Delta}{27}}\right)} \; ; \; v_k = j^{-k} \sqrt[3]{\frac{1}{2}\left(-q - \sqrt{\frac{-\Delta}{27}}\right)}$$ DVPT 2

où $\Delta = -(4p^3 + 27q^2)$ est le discriminant de l'équation.

(i) Si $\Delta > 0$, P admet trois racines réelles distinctes

(ii) Si $\Delta = 0$, P admet des racines réelles, dont une multiple

(iii) Si $\Delta < 0$, P admet une racine réelle et deux racines complexes conjuguées (cf. Fig 2)

3 - Utilisation du polynôme dérivé

Th 57 (Théorème de Gauss-Lucas)

Soit $P \in \mathbb{C}[X]$. Les racines de P' sont dans l'enveloppe convexe des racines de P (cf. Fig 3)

Th 58 : (Théorème de Rolle) Soit $a < b \in \mathbb{R}$

Soit $f \in \mathcal{C}^0([a, b]) \cap \mathcal{C}^1(]a, b[)$ avec $f(a) = f(b)$

Alors $\exists c \in]a, b[: f'(c) = 0$

Appli 59 : Soit $P \in \mathbb{R}[X]$, ayant pour racines $\alpha_1 < \dots < \alpha_n \in \mathbb{R}$

P' admet $n-1$ racines $\beta_1 < \dots < \beta_{n-1}$ avec $\forall i \in [\![1, n-1]\!]$,

$\beta_i \in]\alpha_i, \alpha_{i+1}[$ (cf. Fig 4)

3 - Localisation de racines dans le plan complexe

Th 60 : Soit $P \in \mathbb{C}_n[X]$. Si $\|P\| = \sum_{i=0}^{n} |a_i|$, où $P = \sum_{i=0}^{n} a_i X^i$, alors si $Q \in \mathbb{C}_n[X]$ est dans un voisinage de P pour $\|\cdot\|$, alors les racines de Q sont dans un voisinage des racines de P

Coro 61 : Si $M \in \mathcal{M}_n(\mathbb{C})$, et si $N \in \mathcal{M}_n(\mathbb{C})$ se trouve dans un voisinage de M (pour une certaine norme, on est en dimension finie), alors les valeurs propres de N se trouvent dans un voisinage de celles de M

Th 62 (Théorème de Gershgorin)

Soit $A \in \mathcal{M}_n(\mathbb{C})$. Alors on a :

$$\sigma(A) \subset \bigcup_{i=1}^{n} \left\{ z \in \mathbb{C} : |z - a_{i,i}| \leq \sum_{j \neq i} |a_{i,j}| \right\}$$

Appli 63 : Soit $P = X^n + \sum_{i=0}^{n-1} a_i X^i \in \mathbb{C}[X]$

Alors, si z est une racine de P, z vérifie :

$$|z| \leq \max\left\{ |a_0|, 1 + |a_1|, \dots, 1 + |a_{n-1}| \right\}$$

Th 64 : (Théorème de Rouché)

Soit $U \subset \mathbb{C}$ un ouvert simplement connexe (sans « trou »)

Soient $P, Q \in \mathbb{C}[X]$, et $Z(P)$, $Z(Q)$ les ensembles des zéros de P, Q

Soit Γ un lacet tel que $\Gamma \subset U \setminus (Z(P) \cup Z(Q))$ formant le bord d'un compact K

Supposons que $\forall z \in \Gamma$, $|P(z) - Q(z)| < |P(z)|$

Alors $\#(Z(P) \cap K) = \#(Z(Q) \cap K)$

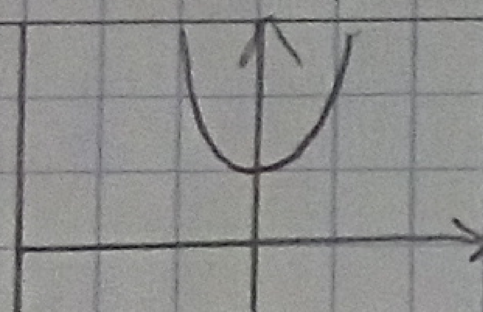
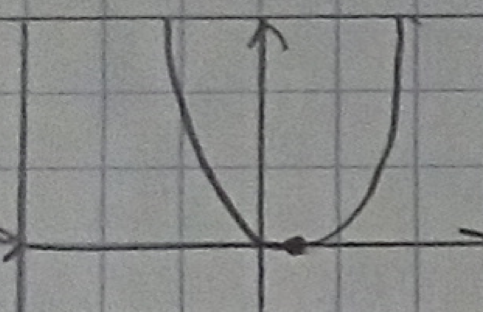
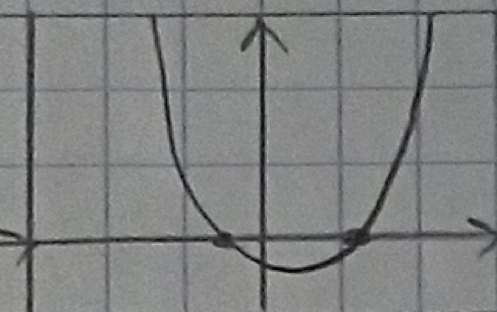
Ex 65 : Si $P(z) = z^8 - 5z^3 + z - 2$, $Q(z) = -5z^3$

si $z \in \partial D(0, 1)$, alors

$|P(z) - Q(z)| = |z^8 + z - 2| \leq |z|^8 + |z| + 2 = 4 < 5 = |Q(z)|$

P et Q ont le même nombre de zéros dans $\overline{D(0,1)}$, c'est-à-dire trois

Annexe

Courbe de P ($a > 0$)			
Signe de Δ	$\Delta < 0$	$\Delta = 0$	$\Delta > 0$

Polynômes de degré 2 réels — Fig 1

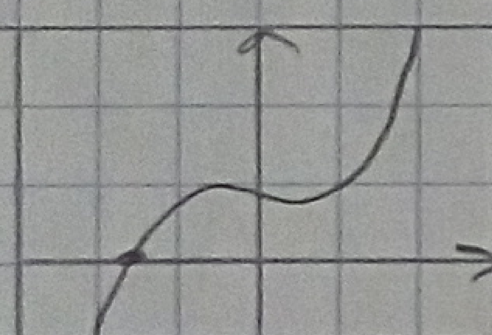
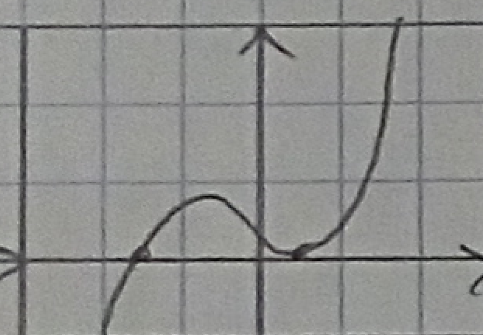
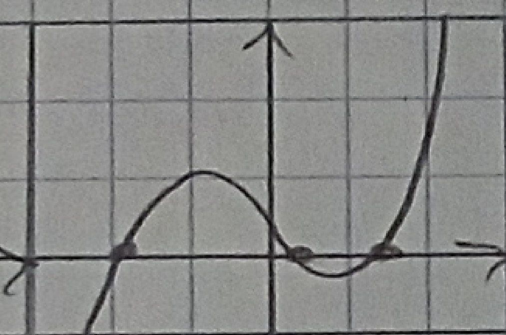
Courbe de P (Exemple)			
Signe de Δ	$\Delta < 0$	$\Delta = 0$	$\Delta > 0$

Illustration des formules de Cardan — Fig 2

$P = X^5 - X$, racines •

$P' = 5X^4 - 1$, racines +

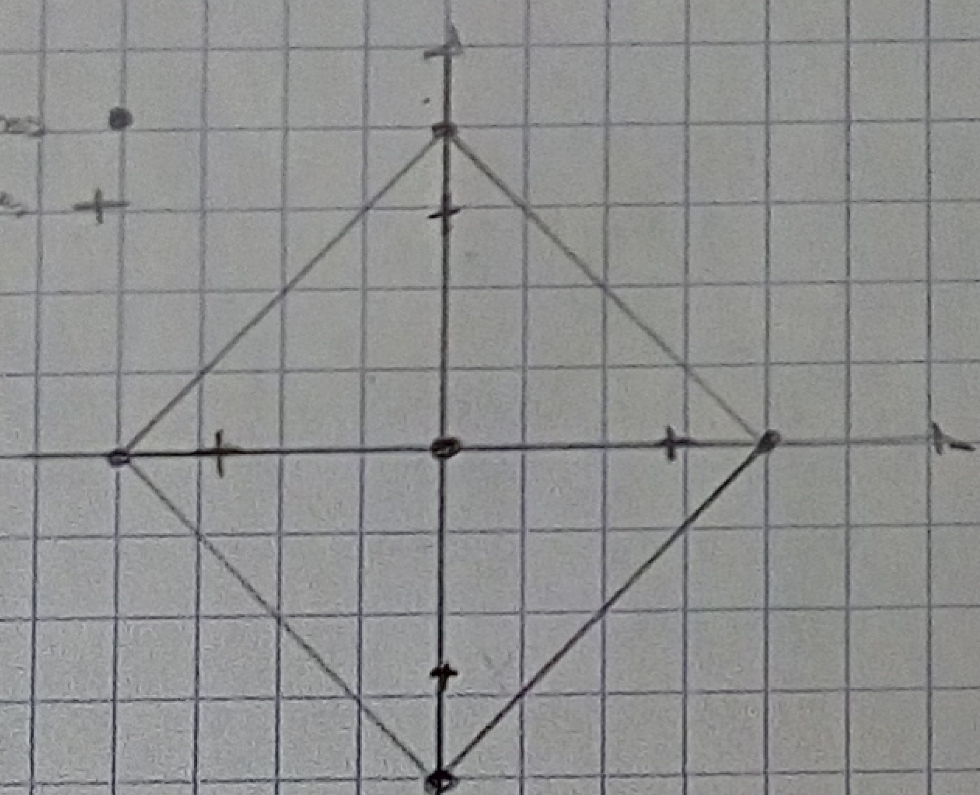


Illustration du théorème de Gauss-Lucas — Fig 3

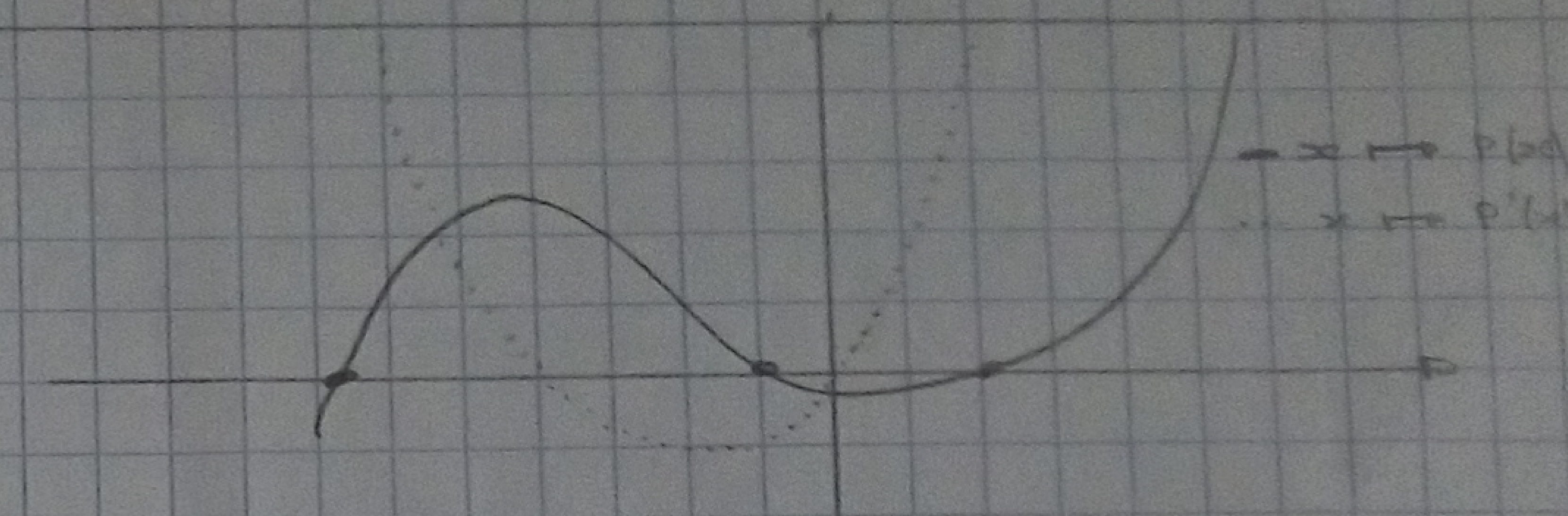


Illustration du théorème de Rolle — Fig 4

Références

J. Calais, *Éléments de théorie des anneaux*