ADS-M-3

Une conjecture sur les zéros d'un polynôme et de ses dérivées

Travail demandé :

Il vous est demandé d'étudier puis de présenter le(s) texte(s) joint(s) à travers un exposé de synthèse d'une durée comprise entre 15 et 20 minutes.

Si l'étude de la totalité du dossier et la préparation d'un exposé cohérent dans la durée impartie ne vous paraît pas possible, vous pouvez décider de vous limiter à une partie du dossier.

Remarques générales :

1. Les textes proposés, quelle que soit leur origine, peuvent présenter des défauts (coquilles typographiques, négligences ou sous-entendus de l'auteur, voire erreurs...) qui, sauf exception, n'ont pas été corrigés.

2. Les textes proposés peuvent contenir des exercices qu'il n'est pas demandé de résoudre. Néanmoins, vous pouvez vous aider des énoncés de ces exercices pour enrichir votre exposé.

3. Vous pouvez annoter les documents qui vous sont fournis. Vos annotations ne seront pas regardées par l'examinateur.

Remarque particulière :

Une partie A, éventuellement vide, de $\mathbb{C}$ est dite convexe si pour tout couple d'éléments a, b de A, le segment $\{ta+(1-t)b \,/\, t \in [0,1]\}$ est inclus dans A. Une intersection de parties convexes est convexe. Pour une partie B de $\mathbb{C}$, l'intersection de toutes les parties convexes qui contiennent B s'appelle l'enveloppe convexe de B.

UNE CONJECTURE SUR LES ZÉROS D'UN POLYNÔME ET DE SES DÉRIVÉES

1. La conjecture

En 2001, le mathématicien Eduardo Casas-Alvero a formulé la conjecture suivante, d'autant plus remarquable qu'elle n'implique que des connaissances du niveau des études secondaires, et n'est toujours pas démontrée, douze ans après avoir été énoncée.

Conjecture 1. *Soit $f \in \mathbb{C}[x]$ un polynôme unitaire de degré $n > 0$. On suppose que pour tout entier $k \in [1, n-1]$, le polynôme f et sa dérivée k-ième $f^{(k)}$ ont un zéro commun dans $\mathbb{C}$. Alors, il existe un nombre complexe a tel que $f(x) = (x-a)^n$.*

Dans la suite, on appellera polynôme de Casas-Alvero, ou polynôme C-A, un polynôme satisfaisant la condition énoncée. On remarquera également que cette condition est équivalente au fait que pour tout k, le PGCD des polynômes f et $f^{(k)}$ est non constant. On notera $f' = f^{(1)}$ et$f'' = f^{(2)}$.

La conjecture ne peut pas s'étendre à n'importe quel corps commutatif. En effet, pour $\mathbb{K} = \mathbb{Z}/7\mathbb{Z}$, le polynôme $f(x) = x^4 + x^2 + 2x$ est un contre-exemple à la conjecture.

La conjecture n'est pas résolue ; même le cas où l'on suppose que f est scindé sur $\mathbb{R}$ n'est pas résolu : le fait que les zéros de $f^{(i)}$ et ceux de $f^{(i+1)}$ soient entrelacés ne permet pas à lui seul de démontrer la conjecture pour un degré supérieur ou égal à 5 (cf. Fig. 1).

Dans cette note, on passe en revue quelques travaux menés sur la conjecture C-A. En particulier, dans le paragraphe 6, on présentera l'abord algébrique de Graf von Bothmer, Labs, Schicho et van de Woestijne qui démontrent la conjecture pour une infinité de valeurs de n, en nous limitant aux cas où n est le double d'un nombre premier. Leur méthode s'applique plus généralement aux entiers de la forme $n'p^e$, où n' est un entier petit (au plus 4) et p un nombre premier. Par essence, il est peu probable que leur méthode permette de résoudre complètement la conjecture C-A ; pour cette raison, nous présentons également d'autres abords plus analytiques. Dans le deuxième paragraphe, nous indiquons quelques symétries de la conjecture et une voie d'attaque via l'inversion.

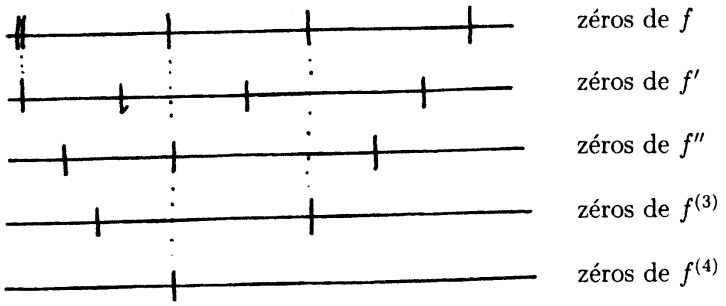

Figure 1 Zéros potentiels de f de degré 5

Dans le troisième paragraphe, nous présentons le théorème de Gauss-Lucas sur la localisation des zéros d'un polynôme et de ses dérivées et nous en déduisons la conjecture C-A en petit degré. Dans le paragraphe suivant, nous montrons qu'on ne peut trop relâcher la condition de la conjecture en présentant des "contre-exemples" si on omet une des dérivées. Dans le paragraphe 5, nous établissons que l'ensemble des zéros commun à un polynôme C-A f et à ses dérivées ne peut être exactement 2.

2. Les symétries

L'observation élémentaire suivante décrit les symétries de l'ensemble des polynômes C-A : leurs zéros peuvent être simultanément transformés par une similitude.

Lemme 1. *Si f est un polynôme C-A de degré n, alors, pour tout $a \in \mathbb{C}^*$ et tout $b \in \mathbb{C}$, le polynôme $a^{-n} f(ax+b)$ est C-A.*

La conjecture C-A implique que l'ensemble des polynômes C-A f de degré n donné pour lesquels $f(0) \neq 0$ est stable pour l'*inversion* $f(x) \mapsto x^n f(1/x)/f(0)$, et donc par toute transformation, dite transformation de Möbius, qui est produit d'un nombre fini de similitudes et d'inversions. La proposition suivante montre que cette condition nécessaire est également suffisante.

Proposition 1. *Si l'ensemble des polynômes C-A de degré n qui ne s'annulent pas à l'origine est stable par inversion, alors la conjecture C-A est vraie en degré n.*

Esquisse de démonstration. Supposons par l'absurde que f est un polynôme C-A de degré n avec au moins deux zéros distincts. Quitte à appliquer une transformation affine, on peut supposer que 1 est un zéro de f ; soit d sa multiplicité : on a $1 \leq d < n$. On peut

alors trouver une famille de transformations de Möbius, $\lambda(t)$, dépendant d'un paramètre $t \in \mathbb{C}^*$ telles que

$$\forall t : \lambda(t)(1) = 1, \text{ et } \forall z \in \mathbb{C}\backslash\{1\} : \lim_{t\to 0} \lambda(t)(z) = -1.$$

Alors, quand t tend vers 0, $\lambda(t)(f(x))$ tend vers $(x-1)^d(x+1)^{n-d}$. Mais alors ce polynôme devrait également être C-A, ce qu'il n'est pas. □

D'autres transformations peuvent être imaginées. Par exemple, si on sait montrer que l'ensemble des polynômes C-A est stable par la transformation $\prod(x-\alpha_i) \mapsto \prod(x-\alpha_i^2)$, alors on peut en déduire la conjecture C-A. On ne sait malheureusement pas comment exploiter ces observations.

3. Le théorème de Gauss-Lucas

On rappelle le théorème classique de Gauss-Lucas

Théorème 1. *Pour tout polynôme non constant $f \in \mathbb{C}[x]$, les zéros de sa dérivée f' sont situés dans l'enveloppe convexe des zéros de f. Plus précisément, si α est un zéro de f', alors, ou bien c'est un zéro de f, ou bien il est situé dans l'intérieur relatif de l'enveloppe convexe des zéros de f.*

Ici, l'*intérieur relatif* d'un point est ce point, celui d'un intervalle d'extrémité a et b est l'intervalle ouvert d'extrémités a et b, et celui d'un polygone est ce polygone privé de ses bords. Le théorème de Gauss-Lucas permet de montrer qu'un polynôme C-A a au moins un de ses zéros dans l'intérieur relatif de l'enveloppe convexe, notée C, de l'ensemble de ses zéros. Soit en effet $z_1, \ldots, z_k$ les zéros de f, distincts deux à deux, qui ne sont pas dans l'intérieur relatif de C, et soit $m_1, \ldots, m_k$ leurs multiplicités respectives ; on pose $m = \max_i m_i$. Si $m = \deg(f)$, alors f est la puissance m-ième d'un polynôme linéaire et l'assertion est manifestement vraie. Sinon, on a $m < n$ et considère le polynôme $f^{(m)}$: tous ses zéros sont dans l'intérieur relatif de C et donc l'un des zéros de f y est.

Cette remarque permet de démontrer la conjecture C-A pour les degrés $n \leq 4$. Supposons par exemple que f est un polynôme C-A de degré 4 et soient z_1, z_2, z_3, z_4 ses zéros (non nécessairement distincts). Puisque f et f' ont un zéro en commun, f a un zéro double et on peut, sans perte de généralité, supposer que $z_1 = z_2$. D'après ce qui précède, ou bien les quatre zéros sont confondus (la conjecture est vérifiée) ou bien les trois zéros z_1, z_3, et z_4 sont deux à deux distincts et alignés. On peut alors effectuer une similitude qui envoie ces trois points alignés sur la droite réelle. Il y a deux possibilités :

ou bien z_1 est entre z_3 et z_4 ; alors f'' a un zéro dans l'intervalle ouvert d'extrémités z_1 et z_3 et un zéro dans l'intervalle ouvert d'extrémités z_1 et z_4, et alors f'' n'a aucun zéro

en commun avec f, ce qui est contradictoire,

ou bien z_3 est entre z_1 et z_4 ; alors, f'' doit avoir un zéro en z_3 et un zéro dans l'intervalle ouvert d'extrémités z_1 et z_3 ; dans ce cas, $f^{(3)}$ n'a pas de zéro en commun avec f, ce qui est contradictoire.

De tels arguments sont insuffisants pour traiter le cas de degrés supérieurs à 4 : en effet, des arguments de nature purement topologique ne permettent pas d'exclure une configuration comme celle de la figure 1.

4. "Contre-exemples approchés" avec uniquement des zéros réels

Nous montrons ici que la conclusion de la conjecture n'est pas valide si on suppose seulement que f a un zéro commun avec chacune de ses dérivées, sauf une ; plus précisément on a le résultat suivant

Théorème 2. *Pour tout $n > 1$ et $\ell \in \{1, \ldots, n-1\}$, il existe un polynôme $f \in \mathbb{R}[x]$ avec $f(0) = f(1) = 0$ dont tous les zéros sont réels et inclus dans l'intervalle $[0,1]$ et qui possède un zéro commun avec chacune de ses dérivées $f^{(k)}$, pour $k \in \{1, \ldots, n-1\} \backslash \{\ell\}$.*

Esquisse de démonstration. Si f est un polynôme réel qui n'a que des zéros réels, il en va de même pour toutes ses dérivées. Pour $1 \leq k \leq n$, on note $\alpha_{k,1} \leq \alpha_{k,2} \leq \cdots \leq \alpha_{k,n-k}$ les zéros de $f^{(k)}$. Nous allons démontrer un résultat un peu plus précis. Pour $k \in E(\ell) = \{1, \ldots, n-1\} \backslash \{\ell\}$, choisissons m_k dans $[1, n-k]$. Pour un $(n-2)$-uplet $\beta = (\beta_k)_{k \in E(\ell)}$, on note $g(\beta)$ le polynôme $x(x-1) \prod_{k \in E(\ell)} (x - \beta_k)$. L'application $\Phi : [0,1]^{n-2} \to [0,1]^{n-2}$ qui à β associe $(\alpha_{k,m_k})_{k \in E(\ell)} (g(\beta))$ est continue ; d'après le théorème de Brouwer (résultat admis), elle admet un point fixe. On vérifie facilement que le polynôme $g(\beta)$ associé à un tel point fixe a les propriétés requises. □

Un exemple. Pour $n = 5$ et les paires $(1,2), (2,3)$ et $(4,4)$, on trouve $\beta_1, \beta_4 \approx 0,629099$ et $\beta_2 \approx 0,887298$. Le graphe des dérivées de f est donné dans la Figure 2.

5. Deux zéros ne conviennent pas

On démontre dans ce paragraphe le résultat suivant.

Proposition 2. *Soit f un polynôme C-A de degré n et soit a_i un zéro commun à f et $f^{(i)}$. On a $\operatorname{card}\{a_i \,/\, 1 \leq i \leq n-1\} \neq 2$.*

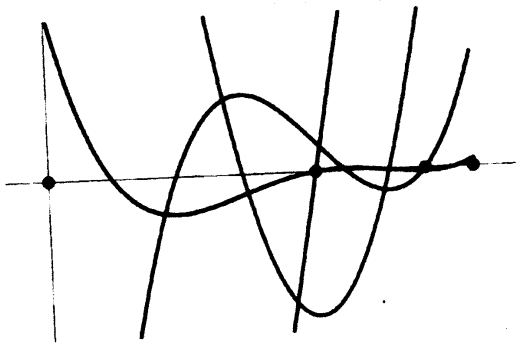

Figure 2 Contre-exemple approché en degré 5

On remarquera que cet énoncé est plus fort que le fait que f ne peut pas être de la forme $(x-a)^k(x-b)^{n-k}$ avec $0 < k < n$, établi dans la démonstration de la proposition 1.

Démonstration. On raisonne par l'absurde, en supposant que le cardinal des a_i est 2. Quitte à effectuer une transformation affine, on peut supposer que $\{a_i \,/\, 1 \leq i \leq n-1\} = \{0,1\}$. On va montrer par induction descendante sur k que $f^{(k)}$ est un polynôme totalement positif ou totalement négatif sur l'intervalle ouvert $]0,1[$. C'est vrai pour $k = n$: on a $f^{(n)} = n!$. Supposons notre hypothèse satisfaite au rang k. Alors, il existe un nombre complexe c_{k-1} tel que pour tout réel x on a $f^{(k-1)}(x) = \int_0^x f^{(k)}(t)dt + c_{k-1}$; puisque $f^{(k)}(t)$ est réel pour tout réel t et que $f^{(k-1)}$ s'annule en 0 ou en 1, le nombre c_{k-1} est réel et donc le polynôme $f^{(k-1)}$ est à coefficients réels. Il est strictement monotone sur l'intervalle $[0,1]$ et il s'annule en une des extrémités de cet intervalle. Il est donc strictement positif ou strictement négatif sur $]0,1[$. Cette propriété est donc également vraie pour le polynôme $f = f^{(0)}$; mais alors le polynôme f ne peut pas s'annuler en 0 et en 1 ; cette contradiction achève la démonstration de la proposition. □

6. La réduction modulo p

Le théorème suivant est actuellement le résultat positif principal sur la conjecture de Casas-Alvero. Moyennant deux résultats admis concernant les valuations p-adiques sur $\mathbb{C}$, nous en donnerons la démonstration, en nous restreignant au cas où n est le double d'un nombre premier, cas techniquement plus simple mais qui illustre les ressorts de la démonstration générale.

Théorème 3. *On considère un entier $n' \in \{1,2,3,4\}$, un nombre premier p supérieur à n' et différent de 7 si $n' = 4$, un entier $e \geq 0$ et on pose $n = n'p^e$. Alors la conjecture de Casas-Alvero est vraie pour le degré n.*

Valuation. Une valuation sur un corps commutatif $\mathbb{K}$ est une application $v : \mathbb{K} \to \mathbb{R} \cup \{\infty\}$ telle que l'on a

(1) $v^{-1}(\{\infty\}) = \{0\}$,
(2) $v(ab) = v(a) + v(b)$,
(3) $v(a+b) \geq \min(v(a), v(b))$,

pour tout couple (a, b) d'éléments de $\mathbb{K}$.

Valuation p-adique sur $\mathbb{C}$. Pour un nombre premier p, il existe une unique valuation v sur $\mathbb{Q}$ qui est telle que pour tout entier positif m on a $v(m) = \max\{e \,/\, p^e \text{ divise } m\}$; on l'appelle la valuation p-adique sur $\mathbb{Q}$ et on la note v_p. Nous admettons d'une part qu'il existe une valuation v sur $\mathbb{C}$ qui coïncide avec v_p sur $\mathbb{Q}$ (on continuera de la noter v_p). On note $V^+ = \{z \in \mathbb{C} \,/\, v_p(z) \geq 0\}$. Nous admettons d'autre part qu'il existe un corps commutatif $\mathbb{K}$ et une application *surjective* $\sigma : V^+ \to \mathbb{K}$ telle que

(1) $\sigma(1_{\mathbb{C}}) = 1_{\mathbb{K}}$,
(2) $\forall a, b \in V^+ : \sigma(a+b) = \sigma(a) + \sigma(b)$,
(3) $\forall a, b \in V^+ : \sigma(ab) = \sigma(a)\sigma(b)$,
(4) $\forall a \in V^+ : v_p(a) > 0 \Rightarrow \sigma(a) = 0$.

Notation. Pour $a \in V^+$, on notera $\widetilde{a} = \sigma(a)$. Bien que $\widetilde{p} = \widetilde{0}$, nous suivrons l'usage et noterons simplement a l'élément $\widetilde{a}$ dans le cas où $a \in \mathbb{Z}$. En particulier, 0 et 1 dénotent respectivement le neutre de $\mathbb{K}$ pour l'addition et le neutre de $\mathbb{K}$ pour la multiplication.

Coefficients du binôme. L'image par σ du coefficient binômial $\binom{2p}{k}$ est nulle si et seulement si $k \notin \{0, p, 2p\}$. En particulier, on a dans $\mathbb{K}[x]$ la relation $(f+g)^p = f^p + g^p$, dite *le rêve du bizuth.*

Dérivées de Hasse. Pour un polynôme $f = \alpha_n x^n + \alpha_{n-1}x^{n-1} + \cdots + \alpha_1 x + \alpha_0$ de $\mathbb{C}[x]$ ou de $\mathbb{K}[x]$, et un entier $i \leq n$, on définit sa i-ème dérivée de Hasse par

$$H_i(f) = \binom{n}{i}\alpha_n x^{n-i} + \binom{n-1}{i}\alpha_{n-1}x^{n-i-1} + \cdots + \binom{i}{i}\alpha_i.$$

On notera que pour un polynôme $f \in \mathbb{C}[x]$, on a $H_i(f) = f^{(i)}/i!$, mais que pour $f \in \mathbb{K}[x]$, on peut avoir $H_i(f) \neq 0$, alors que $f^{(i)} = 0$, comme le montre l'exemple du polynôme $f = x^{2p}$ pour $i = p$.

Condition C-A dans $\mathbb{K}[x]$. Dans le cas de $\mathbb{C}[x]$, un polynôme est C-A s'il est unitaire de degré positif et s'il a au moins un zéro commun avec chacune de ses dérivées de Hasse. Dans la suite, on dira qu'un polynôme de $\mathbb{K}[x]$ est C-A s'il est unitaire de degré positif et s'il a au moins un zéro commun avec chacune de ses dérivées de Hasse.

Démonstration du théorème 3. Comme indiqué dans l'introduction de ce paragraphe, nous nous limitons au cas où $n' = 2$ et $e = 1$, c'est-à-dire au cas où $n = 2p$, avec p premier impair. On raisonne par l'absurde en supposant que $f \in \mathbb{C}[x]$ est un polynôme C-A avec au moins deux zéros distincts. En effectuant une translation, on peut supposer que l'un de ses zéros est 0, c'est-à-dire que $f(x) = x^h(x - x_0)\cdots(x - x_{2p-h-1})$, où $1 \leq h < n$ et les x_i, non nécessairement distincts deux à deux, sont tous non nuls ; on peut supposer que parmi les x_i, le zéro x_0 est de valuation minimale. Une homothétie de rapport $1/x_0$ permet de remplacer x_0 par 1 et tous les autres x_i par des complexes de valuation positive. En bref, on s'est ramené au cas où

$$\begin{aligned} f(x) &= x^h(x-1)(x-x_1)\cdots(x-x_{2p-h-1}) \\ &= x^{2p} + c_{2p-1}x^{2p-1} + \cdots + c_h x^h, \\ &\qquad \textit{avec } \forall i \in [1, 2p-h-1] \,:\, v_p(x_i) \geq 0. \end{aligned}$$

Puisque tous les x_i ont une valuation positive, il en va de même des c_i et on peut considérer le polynôme de $\mathbb{K}[x]$

$$\begin{aligned} \widetilde{f}(x) &= x^h(x-1)(x-\widetilde{x_1})\cdots(x-\widetilde{x_{2p-h-1}}) \\ &= x^{2p} + \widetilde{c_{2p-1}}x^{2p-1} + \cdots + \widetilde{c_h}x^h. \end{aligned}$$

Si le zéro 0, 1 ou x_i est commun à f et $H_i(f)$, alors le zéro 0, 1 ou $\widetilde{x_i}$ est commun à $\widetilde{f}$ et $H_i(\widetilde{f})$. Il s'ensuit que le polynôme $\widetilde{f}$ est C-A.

Nous montrons maintenant que $\widetilde{c_i}$ est nul si p ne divise pas i. Supposons d'abord qu'il existe $k \in [p+1, 2p-1]$ tel que $\widetilde{c_k} \neq 0$, et choisissons un tel k maximal. On a

$$H_k(\widetilde{f}) = \binom{2p}{k} x^{2p-k} + \widetilde{c_k} = \widetilde{c_k}.$$

Donc $H_k(\widetilde{f})$ est un polynôme constant. Puisqu'il a un zéro commun avec $\widetilde{f}$, il est nul et donc $\widetilde{c_k} = 0$.

Si $h \geq p$, on peut écrire

$$\widetilde{f}(x) = x^{2p} + \widetilde{c_p}x^p. \tag{1}$$

Si $h < p$, on peut écrire $\widetilde{f}(x) = x^{2p} + \widetilde{c_p}x^p + \widetilde{c_{p-1}}x^{p-1} + \cdots + \widetilde{c_h}x^h$. Supposons maintenant qu'il existe $k \in [h, p-1]$ tel que $\widetilde{c_k} \neq 0$, et choisissons un tel k maximal. On a

$$H_k(\widetilde{f}) = \binom{2p}{k} x^{2p-k} + \binom{p}{k}\widetilde{c_{p-k}}x^k + \widetilde{c_k} = \widetilde{c_k},$$

et on montre comme précédemment que $\widetilde{c_k} = 0$.
La relation (1) est donc établie dans tous les cas.

On peut trouver un nombre complexe z_p tel que $(z_p)^p = c_p$; on a alors $(\widetilde{z_p})^p = \widetilde{c_p}$. En utilisant le rêve du bizuth, la relation (1) devient

$$\widetilde{f}(x) = x^{2p} + \widetilde{z_p}^p x^p = \left(x^2 + \widetilde{z_p} x\right)^p . \tag{2}$$

On a

$$\begin{aligned} H_p(\widetilde{f}) &= \binom{2p}{p} x^p + \binom{p}{p} \widetilde{c_p} = \\ &= 2x^p + \widetilde{c_p} = (1+1)x^p + \widetilde{c_p} = \\ &= (1+1)^p x^p + \widetilde{c_p} = (2x + \widetilde{z_p})^p . \end{aligned}$$

Considérons le polynôme $g(x) = x^2 + \widetilde{z_p} x$. Sa dérivée est le polynôme $g'(x) = 2x + \widetilde{z_p}$. Puisque $\widetilde{f}$ et $H_p(\widetilde{f})$ ont un zéro commun, il en va de même de g et g', donc g a un zéro double et donc $\widetilde{z_p} = 0$, d'où $\widetilde{f}(x) = x^{2p}$, ce qui contredit notre hypothèse que f a deux zéros distincts. Cela établit le Théorème 3 dans le cas où $n = 2p$, avec p premier impair. □

7. Exercices

Exercice 1 Montrer que $V^+ = \{z \in \mathbb{C} \,/\, v_p(z) \geq 0\}$ est un anneau et que $V^{++} = \{z \in \mathbb{C} \,/\, v_p(z) > 0\}$ est un idéal de cet anneau. Montrer qu'en outre tout idéal de V^+ qui contient strictement V^{++} est V^+. Montrer que V^{++} est un idéal intègre.

Exercice 2 Soit p un nombre premier supérieur à 3. Montrer que la conjecture C-A est vraie pour les polynômes de degré 3 de $\mathbb{K}[x]$. En déduire que la conjecture C-A est vraie pour les polynômes de degré $3p$ sur $\mathbb{C}$.

Exercice 3 Montrer que le polynôme $x^4 + x \in \mathbb{Z}/7\mathbb{Z}$ ne satisfait pas la conjecture C-A, où les dérivées sont prises au sens de Hasse.

Exercice 4 Démontrer la conjecture C-A pour les polynômes de degré premier de $\mathbb{C}[x]$.

Exercice 5 Compléter la démonstration de la Proposition 1.

Exercice 6 Démontrer l'existence de la valuation p-adique sur $\mathbb{Q}$.

Exercice 7 Démontrer que le corps $\mathbb{K}$ du texte est algébriquement clos, c'est-à-dire que tout polynôme non constant de $\mathbb{K}[x]$ a au moins un zéro dans $\mathbb{K}$.