

SUR LES ÉQUATIONS POLYNOMIALES DANS LES QUATERNIONS

Autor(en): **Beck, Bernard**

Objektyp: **Article**

Zeitschrift: **L'Enseignement Mathématique**

Band (Jahr): **25 (1979)**

Heft 1-2: **L'ENSEIGNEMENT MATHÉMATIQUE**

PDF erstellt am: **26.09.2024**

Persistenter Link: <https://doi.org/10.5169/seals-50378>

Nutzungsbedingungen

Die ETH-Bibliothek ist Anbieterin der digitalisierten Zeitschriften. Sie besitzt keine Urheberrechte an den Inhalten der Zeitschriften. Die Rechte liegen in der Regel bei den Herausgebern.

Die auf der Plattform e-periodica veröffentlichten Dokumente stehen für nicht-kommerzielle Zwecke in Lehre und Forschung sowie für die private Nutzung frei zur Verfügung. Einzelne Dateien oder Ausdrucke aus diesem Angebot können zusammen mit diesen Nutzungsbedingungen und den korrekten Herkunftsbezeichnungen weitergegeben werden.

Das Veröffentlichen von Bildern in Print- und Online-Publikationen ist nur mit vorheriger Genehmigung der Rechteinhaber erlaubt. Die systematische Speicherung von Teilen des elektronischen Angebots auf anderen Servern bedarf ebenfalls des schriftlichen Einverständnisses der Rechteinhaber.

Haftungsausschluss

Alle Angaben erfolgen ohne Gewähr für Vollständigkeit oder Richtigkeit. Es wird keine Haftung übernommen für Schäden durch die Verwendung von Informationen aus diesem Online-Angebot oder durch das Fehlen von Informationen. Dies gilt auch für Inhalte Dritter, die über dieses Angebot zugänglich sind.

SUR LES ÉQUATIONS POLYNOMIALES DANS LES QUATERNIONS

par Bernard BECK

Soit H un corps de quaternions généralisés, de centre K (voir [1]).
Le but de cet article est d'étudier les solutions dans H de l'équation

$$(1) \quad P(x) = q_n x^n + q_{n-1} x^{n-1} + \dots + q_0 = 0$$

où $q_r \in H$, $r = 0, 1, \dots, n$ et $q_n \neq 0$.

Dans le cas où le corps K est le corps des nombres réels et H le corps des quaternions classiques, I. Niven [2] a démontré les résultats suivants:

- (i) L'équation (1) admet toujours une solution dans H .
- (ii) L'équation (1) admet une infinité de solutions dans H si et seulement si $P(x) = Q(x)(x^2 - 2tx + r)$ où $t, r \in K$, $t^2 < r$.
- (iii) Si le nombre de solutions de (1) est fini, celui-ci est au plus $(2n - 1)^2$.

On étudie ici l'équation (1) dans le cas le plus général, en reliant les solutions de (1) aux racines d'un polynôme $n(P)$ à une indéterminée à coefficients dans K : c'est le théorème de la partie II.

Dans la partie III, on étudie les conséquences de ce théorème et on montre notamment les résultats suivants:

— Si le nombre de solutions de (1) est fini, celui-ci est inférieur ou égal à n .

— Il existe un unique polynôme P unitaire de degré n à coefficients dans H admettant n racines 2 à 2 non conjuguées.

I. RAPPELS ET NOTATIONS

Soit H un corps de quaternions généralisés. On sait que H est un espace vectoriel de dimension 4 sur son centre K et qu'il existe sur H un antiautomorphisme involutif, $q \mapsto \bar{q}$, tel que, quels que soient les éléments λ de K et q, q' de H , on ait

$$\overline{q + q'} = \bar{q} + \bar{q}', \quad \overline{q q'} = \bar{q}' \cdot \bar{q}, \quad \overline{\bar{q}} = q, \quad \overline{\bar{\lambda}} = \lambda$$

(si la caractéristique de K est différente de 2, alors $K = \{\mu \in H \mid \bar{\mu} = \mu\}$, mais cela est faux en caractéristique 2). A tout quaternion q de H , on associe deux éléments de K

$$n(q) = q\bar{q} = \bar{q}q, \quad \text{appelé la norme de } q,$$

$$t(q) = q + \bar{q}, \quad \text{appelé la trace de } q,$$

ainsi que le polynôme de $K[X]$

$$\Delta_q(X) = X^2 - t(q)X + n(q),$$

appelé polynôme caractéristique de q . On a alors $\Delta_q(q) = 0$. Citons sans démonstration les résultats suivants:

Résultat 1. Deux éléments q et q' de H sont conjugués (i.e. il existe $\sigma \in H^*$ tel que $q' = \sigma q \sigma^{-1}$), si et seulement s'ils ont même polynôme caractéristique.

Résultat 2. Le polynôme Δ_q est irréductible dans $K[X]$ si et seulement si q n'est pas dans K .

Résultat 3. Tout élément q de H qui n'est pas dans K admet une infinité de conjugués distincts.

Ces trois résultats montrent que si q n'est pas dans K , le polynôme $\Delta_q(X)$ a une infinité de racines dans H . Pour les autres propriétés des corps de quaternions, voir [1].

On considère l'anneau $H[X]$ des polynômes à une indéterminée à coefficients dans H où l'indéterminée commute avec les coefficients. Alors $H[X]$ est un $K[X]$ -module à droite libre de rang 4; en effet, soit $\{q_1, \dots, q_4\}$ une base du K -espace vectoriel H ; tout polynôme P de $H[X]$ s'écrit de manière évidente

$$P(X) = \sum_{i=1}^4 q_i F_i(X) \quad \text{avec} \quad F_i(X) \in K[X].$$

Résultat 4. Tout polynôme P de $H[X]$ se factorise de manière unique en $P = P_1 F$ avec F unitaire dans $K[X]$, P_1 n'étant divisible par aucun polynôme non constant de $K[X]$.

Démonstration. On écrit $P(X) = \sum_{i=1}^4 q_i F_i(X)$ comme précédemment et on prend pour F le P.G.C.D. des F_i . \square

Résultat 5. $H[X]$ est un $K[X]$ -module à droite euclidien, i.e. pour tout polynôme P de $H[X]$ et pour tout polynôme F de $K[X]$, il existe deux polynômes Q et R de $H[X]$ tels que $\text{degré } R < \text{degré } F$ et $P = QF + R$.

Démonstration. On écrit $P(X) = \sum_{i=1}^4 q_i F_i(X)$ et on effectue la division euclidienne des F_i par F . \square

Etant donné un polynôme $P(X) = \sum_{r=0}^n q_r X^r$ dans $H[X]$, on pose $\bar{P}(X) = \sum_{r=0}^n \bar{q}_r X^r$ et

$$n(p) = P \cdot \bar{P} = \sum_{0 \leq r, s \leq n} q_r \bar{q}_s X^{r+s}.$$

Résultat 6. Le polynôme $n(P)$ est un élément de $K[X]$.

Démonstration. On a $n(P) = \sum_{l=0}^{2n} \alpha_l X^l$

et

$$\alpha_l = \sum_{\substack{1 \leq r, s \leq n \\ r+s=l}} q_r \bar{q}_s = a_l + \sum_{\substack{0 \leq r < s \leq n \\ r+s=l}} t(q_r \bar{q}_s),$$

où

$$a = \begin{cases} 0 & \text{si } l \text{ est impair} \\ n(q_{l/2}) & \text{si } l \text{ est pair} \end{cases}$$

Donc $\alpha_l \in K$. \square

Définissons à présent les racines d'un polynôme de $H[X]$. Tout élément $P(X) = \sum_{r=0}^n q_r X^r$ de $H[X]$ peut être considéré comme une fonction sur H en posant $P(x) = \sum_{r=0}^n q_r x^r$ pour tout x dans H , la variable étant toujours à droite des coefficients. La multiplication sur $H[X]$ ne définit pas une multiplication de fonctions au sens habituel; toutefois, si $P \in H[X]$ et si $F \in K[X]$, alors, pour tout élément x de H , on a

$$P \cdot F(x) = P(x) F(x).$$

(On peut traduire cela en disant que $H[X]$ est canoniquement isomorphe en tant que $K[X]$ -module à droite à l'ensemble des fonctions polynômes sur H à variable à droite.)

On dit qu'un quaternion x est *racine* du polynôme P si $P(x) = 0$.

II. DÉTERMINATION DES RACINES D'UN POLYNÔME P DE $H[X]$.

LEMME 1. Soient $P(X) \in H[X]$ et $\lambda \in K$; alors on a $P(\lambda) = 0$ si et seulement si $X - \lambda$ divise $P(X)$ dans $H[X]$.

Démonstration. Evidente.

LEMME 2. Soient $P(X) \in H[X]$ et Δ un polynôme irréductible de degré 2 dans $K[X]$; alors, si Δ est le polynôme caractéristique d'un quaternion q , on a l'alternative suivante :

- a) Δ divise P et alors tous les conjugués $\sigma q \sigma^{-1}$ de q sont racines de P ,
- b) Δ ne divise pas P et alors au plus un conjugué q' de q est racine de P .

Démonstration.

- a) Si Δ divise P , il existe $P_1 \in H[X]$ tel que pour tout élément x de H , on ait $P(x) = P_1(x) \Delta(x)$ et le résultat 1 montre que tout quaternion conjugué de q est racine de P . Il y en a une infinité.
- b) Si Δ ne divise pas P , alors on a $P = P_1 \Delta + aX + b$ avec a et b dans H non simultanément nuls.
 - b₁) Si $a = 0$, pour tout quaternion q de polynôme caractéristique Δ , on a: $P(q) = b \neq 0$.
 - b₂) Si $a \neq 0$, il existe au plus une solution au problème, à savoir $-a^{-1}b$, et pour cela il faut et il suffit que Δ soit le polynôme caractéristique de $-a^{-1}b$. \square

Nous sommes en mesure maintenant de démontrer le résultat principal.

THÉORÈME. Soient P un polynôme de $H[X]$ et q un quaternion quelconque de H . Les conditions suivantes sont équivalentes :

- (i) Il existe un conjugué q' de q tel que $P(q') = 0$.
- (ii) Le polynôme caractéristique de q divise $n(P)$ dans $K[X]$.
- (iii) Le quaternion q est racine de $n(P)$.

Démonstration. Le polynôme Δ_q est dans le centre $K[X]$ de l'anneau $H[X]$. On peut donc calculer modulo Δ_q dans $H[X]$ (i.e. modulo l'idéal bilatère $\Delta_q \cdot H[X]$ de $H[X]$).

Si Δ_q divise P , le théorème est évident. Supposons donc que Δ_q ne divise pas P . On a $P(X) \equiv aX + b \pmod{\Delta_q}$ avec a, b dans H non simultanément nuls.

(i) \Rightarrow (ii): Si $P(q') = 0$, alors $a \neq 0$ et $q' = -a^{-1}b$. Or $n(P) = P\bar{P} \equiv (aX+b)(\bar{a}X+\bar{b}) \equiv n(a) \Delta_{-a^{-1}b} \pmod{\Delta_q}$.

Or $-a^{-1}b = q'$ et $\Delta_{q'} = \Delta_q$, donc $n(P) \equiv 0 \pmod{\Delta_q}$. Donc Δ_q divise $n(P)$ dans $K[X]$.

(ii) \Rightarrow (iii): évident.

(iii) \Rightarrow (i): On a $n(P) \equiv (aX+b)(\bar{a}X+\bar{b}) \pmod{\Delta_q}$. Si $a = 0$, alors $n(P) \equiv n(b) \pmod{\Delta_q}$, donc $n(P)(q) = n(b) \neq 0$. Ceci est contraire à l'hypothèse. Donc $a \neq 0$. Par suite on a $n(P) \equiv n(a) \Delta_{-a^{-1}b} \pmod{\Delta_q}$. Comme $n(P)(q) = 0$, on a $\Delta_{-a^{-1}b}(q) = 0$; donc $\Delta_{-a^{-1}b} = \Delta_q$ et ainsi $P(-a^{-1}b) = 0$. \square

III. QUELQUES CONSÉQUENCES DU THÉORÈME

COROLLAIRE 1. *Supposons que H soit le corps des quaternions classiques sur le corps \mathbf{R} des nombres réels. Alors, pour tout polynôme P de $H[X]$ non constant, il existe un quaternion q de H tel que $P(q) = 0$.*

Démonstration. On peut supposer que P n'a pas de racines dans \mathbf{R} . Alors, d'après le lemme 1, $n(P)$ n'a pas de facteur du premier degré dans $\mathbf{R}[X]$.

Soit Δ un polynôme irréductible de degré 2 dans $\mathbf{R}[X]$, divisant $n(P)$. Un tel Δ existe puisque degré $n(P) = 2$ degré $P \geq 2$. Or on sait qu'il existe un quaternion q tel que $\Delta_q = \Delta$ et le théorème nous dit qu'il existe un conjugué q' de q tel que $P(q') = 0$. \square

C'est le résultat (i) de Niven.

COROLLAIRE 2. *Soit H un corps de quaternions généralisés de centre K . Un polynôme P de $H[X]$ admet une infinité de racines si et seulement s'il existe un polynôme irréductible Δ de degré 2 de $K[X]$ et un quaternion q tel que $\Delta = \Delta_q$ et Δ divise P .*

La démonstration est une conséquence triviale du lemme 2 et du théorème. Si $K = \mathbf{R}$, tout polynôme irréductible de degré 2 est le polynôme caractéristique d'un quaternion q , d'où le résultat (ii) de Niven.

COROLLAIRE 3. *Soit H un corps de quaternions généralisés de centre K . Si le polynôme P de $H[X]$ n'a qu'un nombre fini de racines, celui-ci est inférieur ou égal au degré de P .*

Démonstration. D'après le théorème, à tout quaternion q tel que Δ_q divise $n(P)$, correspond un conjugué q' de q tel que $P(q') = 0$. Comme P n'a qu'un nombre fini de racines, q' est unique d'après le lemme 2. Comme degré $n(P) = 2$ degré P et degré $\Delta_q = 2$, on constate que P a au plus degré P racines distinctes et celles-ci sont deux à deux non conjuguées. \square

Définition. Soit P un polynôme non nul de $H[X]$ n'ayant qu'un nombre fini de racines, et soit q un élément de H . On définit la multiplicité de q par rapport à P (notée $M_P(q)$) de la manière suivante:

$$M_P(q) = \begin{cases} 0 & \text{si } P(q) \neq 0, \\ \text{Max } \{k \in \mathbb{N} \mid \Delta_q^k \text{ divise } n(P)\} & \text{si } P(q) = 0. \end{cases}$$

COROLLAIRE 3'. Si $P \in H[X]$ n'a qu'un nombre fini de racines, q_1, \dots, q_r , et $n = \text{degré } P$, alors

$$\sum_{i=1}^r M_P(q_i) \leq n.$$

Si, de plus, $K = \mathbb{R}$ et H est le corps des quaternions classiques, alors

$\sum_{i=1}^r M_P(q_i) = n$ et on peut dire que P a exactement n racines (avec multiplicités).

Démonstration : évidente.

On a déterminé l'ensemble des racines d'un polynôme ainsi que leurs multiplicités. Il reste à déterminer les polynômes ayant un ensemble de racines données avec leurs multiplicités.

PROPOSITION. Soient H un corps de quaternions généralisés de centre K , q_1, \dots, q_r des quaternions deux à deux non conjugués, n_1, \dots, n_r des entiers ≥ 1 tels que $\sum_{i=1}^r n_i = n$. On suppose, de plus, que les q_i ne sont pas dans K , ce qui ne restreint pas la généralité, grâce au lemme 1.

a) Si pour tout i , $1 \leq i \leq r$, on a $n_i = 1$, alors il existe un unique polynôme unitaire de degré n de $H[X]$, qui ait pour seules racines les q_i avec $1 \leq i \leq r$.

b) S'il existe un i , $1 \leq i \leq r$, tel que $n_i > 1$, alors il existe une infinité de polynômes unitaires P de $H[X]$ de degré n , tels que P ait pour seules racines les q_i , $1 \leq i \leq r$, avec pour multiplicité n_i .

Démonstration.

a) *Unicité.* Si P_1 et P_2 sont deux tels polynômes unitaires, $P_1 - P_2$ est un polynôme de degré inférieur ou égal à $n - 1$, qui admet n racines deux à deux non conjugués, q_1, \dots, q_n . Si $P_1 - P_2 \neq 0$, $\Delta_{q_1} \otimes \dots \otimes \Delta_{q_n}$ divise $n(P_1 - P_2)$. Donc degré $n(P_1 - P_2) \geq 2n$. Or degré $n(P_1 - P_2) \leq 2(n - 1)$, donc $P_1 = P_2$.

Existence. Remarquons que dans ce cas on a $n = r$. On procède par récurrence sur l'entier n . Le cas $n = 1$ étant trivial, soit Q un polynôme unitaire de degré $n - 1$ admettant q_1, \dots, q_{n-1} comme seules racines, les q_i $1 \leq i \leq n - 1$ étant deux à deux non conjugués. Alors si q_n n'est conjugué à aucun des q_i , $1 \leq i \leq n - 1$, on a $Q(q_n) \neq 0$. Posons

$$u = Q(q_n) \cdot q_n \cdot Q(q_n)^{-1}$$

et

$$P(X) = (X - u) Q(X).$$

Par définition de la multiplication dans $H[X]$ on a $P(q) = Q(q) \cdot q - u Q(q)$ pour tout quaternion q et l'on en déduit:

$$P(q_i) = 0 \text{ pour } 1 \leq i \leq n - 1$$

et $P(q_n) = Q(q_n) q_n - (Q(q_n) q_n Q(q_n)^{-1}) Q(q_n) = 0$.

Ainsi P est un polynôme unitaire de degré n qui admet q_1, \dots, q_n comme racines. Montrons que P n'a pas d'autres racines. D'après la partie (ii) du théorème, Δ_{q_i} divise $n(P)$ pour tout i , $1 \leq i \leq n$; comme degré $n(P) = 2n$, on a

$$n(P) = \prod_{i=1}^n \Delta_{q_i}.$$

Si q est une racine de P , Δ_q divise $n(P)$ d'après le théorème et donc il existe i , $1 \leq i \leq n$ tel que q et q_i soient conjugués. Si $q \neq q_i$, on sait d'après le lemme 2 que Δ_{q_i} divise P mais alors $\Delta_{q_i}^2$ divise $n(P)$ donc il existe $j \neq i$ tel que $\Delta_{q_j} = \Delta_{q_i}$ donc q_i et q_j sont conjugués, ce qui est contraire à l'hypothèse. On a donc nécessairement $q = q_i$. Le polynôme P ainsi construit n'a pas d'autres racines que les q_i , $1 \leq i \leq n$.

b) On généralise tout d'abord la définition de la multiplicité d'une racine d'un polynôme: Si $F \in K[X]$ et $q \in H$, posons

$$m_F(q) = \max \{k \in \mathbb{N} \mid (X - q)^k \text{ divise } F \text{ dans } K(q)[X]\}.$$

Si P est un polynôme quelconque de $H[X]$, on écrit $P = P_1 F$ comme en I, Résultat 4. Alors, pour tout quaternion q de H , on définit la multiplicité de q par rapport à P comme étant l'entier

$$M_P(q) = M_{P_1} \cdot (q) + m_F(q).$$

On constate que ceci est une bonne généralisation de la définition précédente.

Il faut alors démontrer deux résultats intermédiaires.

LEMME 3. Soient $P \in H[X]$ et $u \in H$. On pose $P_u(X) = (X-u)P(X)$.
Alors

- (i) $n(P_u) = n(P) \Delta_u$;
- (ii) si q est un quaternion tel que $P(q) \neq 0$ et $P_u(q) = 0$, on a $u = P(q)qP(q)^{-1}$;
- (iii) si q n'est pas conjugué de u , on a $M_P(q) = M_{P_u}(q)$.

Démonstration. (i) et (ii) sont évidents. Pour (iii), on constate que si q n'est pas conjugué de u , alors $(P(q) = 0) \Leftrightarrow (P_u(q) = 0)$, d'où le résultat cherché d'après (i) et la définition de la multiplicité. \square

LEMME 4. Soit un polynôme P de $H[X]$, admettant une racine $q \notin K$ dans H , telle que Δ_q ne divise pas P (i.e. $P(q') \neq 0$ pour tout conjugué q' de q distinct de q). Alors :

- (i) si q' est un conjugué de q distinct de q , la quantité $P(q')q'P(q')^{-1} = \tilde{q}$ est une constante ne dépendant que de P et de q ;
- (ii) si u est un conjugué de q distinct de \tilde{q} , alors $M_{P_u}(q) = M_P(q) + 1$.

Démonstration. (i) Posons $u_i = P(q_i)q_iP(q_i)^{-1}$, $i = 1, 2$, où q_1 et q_2 sont deux conjugués de q distincts de q . Alors P_{u_i} admet q et q_i comme racines. Donc, d'après le lemme 2, on a $P_{u_1}(q') = P_{u_2}(q') = 0$ pour tout conjugué q' de q , mais alors $u_1P(q') = u_2P(q')$. D'où l'on tire $u_1 = u_2$ en prenant $q' \neq q$.

(ii) Si u est un conjugué de q distinct de \tilde{q} , alors $P_u(q') \neq 0$ pour tout conjugué q' de q , distinct de q . Comme, d'autre part, $n(P_u) = n(P) \Delta_u = n(P) \Delta_q$ (Lemme 3 (i)), on a $M_{P_u}(q) = M_P(q) + 1$, d'après la définition de la multiplicité. \square

Le quaternion q n'étant pas dans K , il a une infinité de conjugués $u \neq \tilde{q}$. La partie a) de la proposition et les lemmes 3 et 4 permettent alors d'achever la démonstration de b) par récurrence.

BIBLIOGRAPHIE

- [1] BLANCHARD, A. *Les corps non commutatifs*. Chap. I, PUF Collection SUP (1972).
- [2] NIVEN, I. Equations in quaternions. *Amer. Math. Monthly* 48 (1941), pp. 654-661.

(Reçu le 30 octobre 1978)

Bernard Beck

3, rue du Château
92600 Asnières
(France)

vide-leer-empty