III. Quelques conséquences du théorème

Objekttyp: **Chapter**

Zeitschrift: **L'Enseignement Mathématique**

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

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

PDF erstellt am: **20.09.2024**

(i) $\Rightarrow$ (ii): Si $P(q') = 0$, alors $a \neq 0$ et $q' = -a^{-1}b$. Or $n(P) = P\bar{P}$ $\equiv (aX+b)(\bar{a}X+\bar{b}) \equiv n(a)\,\Delta_{-a^{-1}b} \bmod \Delta_q$.
Or $-a^{-1}b = q'$ et $\Delta_{q'} = \Delta_q$, donc $n(P) \equiv 0 \bmod \Delta_q$. Donc Δ_q divise $n(P)$ dans $K[X]$.

(ii) $\Rightarrow$ (iii): évident.

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

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 $P \geqslant 2$. 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 $P(q') = 0$. □

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. □

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:

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

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

$$\sum_{i=1}^{r} M_p(q_i) \leqslant n \,.$$

Si, de plus, $K = \mathbf{R}$ *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, $q_1, \ldots, q_r$ *des quaternions deux à deux non conjugués,* $n_1, \ldots, n_r$ *des entiers* $\geqslant 1$ *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, $1 \leqslant i \leqslant r$, *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* $1 \leqslant i \leqslant r$.

b) *S'il existe un* i, $1 \leqslant i \leqslant r$, *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, $1 \leqslant i \leqslant r$, *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, $q_1, ..., q_n$. Si $P_1 - P_2 \neq 0$, $\Delta_{q1} \otimes ... \otimes \Delta_{q_n}$ divise $n(P_1 - P_2)$. Donc degré $n(P_1 - P_2) \geqslant 2n$. Or degré $n(P_1 - P_2) \leqslant 2(n-1)$, 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 $q_1, ..., q_{n-1}$ comme seules racines, les q_i $1 \leqslant i \leqslant n - 1$ étant deux à deux non conjugués. Alors si q_n n'est conjugué à aucun des q_i, $1 \leqslant i \leqslant n - 1$, 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:

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

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 $q_1, ..., q_n$ 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, $1 \leqslant i \leqslant n$; 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, $1 \leqslant i \leqslant n$ 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 exite $j \neq i$ 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, $1 \leqslant i \leqslant n$.

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

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

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 $u = P(q) q P(q)^{-1}$;*

(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. □

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 $P(q') q' P(q')^{-1} \doteq \tilde{q}$ 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 $u_i = P(q_i) q_i P(q_i)^{-1}$, $i = 1, 2$, 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 $P_{u_1}(q') = P_{u_2}(q') \doteq 0$ pour tout conjugué q' de q, mais alors $u_1 P(q') = u_2 P(q')$. 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. □

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.