II. Détermination des racines d'un polynome 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.

  b_1) Si $a = 0$, pour tout quaternion q de polynôme caractéristique Δ, on a: $P(q) = b \neq 0$.

  b_2) 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 $-a^{-1}b$. □

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 $\Delta_q \,.\, H[X]$ de $H[X]$).

Si Δ_q divise P, le théorème est évident. Supposons donc que Δ_q ne divise pas P. On a $P(X) \equiv aX + b \bmod \Delta_q$ 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 $n(P) = P\bar{P}$ $\equiv (aX+b)(\bar{a}X+\bar{b}) \equiv n(a) \Delta_{-a^{-1}b} \bmod \Delta_q$.
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 $P(-a^{-1}b) = 0$. $\square$

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 $P \geqslant 2$. 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 $P(q') = 0$. $\square$

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.*