Développement : Théorème de Liouville

Sources :Francinou et Gianella - Algèbre tome 1

December 13, 2017

Bruno Nitrosso, EPP et candidat libre

1. Énoncé. — Théorème : Il n'existe pas de polynômes $P, Q, R \in \mathbb{C}[X]$ vérifiant l'équation $P^n + Q^n + R^n = 0$ pour $n \geq 3$ sans que les trois ne soient égaux entre eux à une constante multiplicative près. On choisit de noter les polynômes de façon à ce que $deg(P) \geq deg(Q) \geq deg(R)$.

2. Historique. — *On peut rapprocher ce résultat du Grand Théorème de Fermat. Liouville le démontra en 1879.*

3. Première étape : on peut se restreindre à des polynômes premiers deux à deux. —

- Si p, q, r forment une solution et si $d = p \wedge q \wedge r$, le triplet $P = \dfrac{p}{d}$, $Q = \dfrac{q}{d}$ et $R = \dfrac{r}{d}$ forme aussi une solution (mais celle-ci avec des polynômes premiers entre eux). multiplicité
- On observe que P, Q, R sont multiples deux à deux d'une constante ssi p, q, r le sont aussi.
- On se limitera par la suite aux solutions potentielles P, Q, R telles que $P \wedge Q \wedge R = 1$
- On observe que si un facteur irréductible d divise deux polynômes (par exemple P et Q), il divise P^n et Q^n et donc, d divise leur somme. Et donc aussi R^n.
- Comme d est irréductible dans un anneau factoriel, d divise R^n nécessite que d divise R.
- Or, du fait que $P \wedge Q \wedge R = 1$, $d \wedge R = 1$.
- Donc, d est un inversible, c'est à dire une constante non nulle.
- on a au final : $P \wedge Q = Q \wedge R = R \wedge P = 1$.

4. Deuxième étape : le cas où $deg(R) \geq 1$. —

- En prenant la dérivée de l'équation (et en simplifiant par n car $\mathbb{R}$ est de caractéristique 0): $P^{n-1}P' + Q^{n-1}Q' + R^{n-1}R' = 0$.
- En multipliant par R' l'équation initiale puis par R la deuxième et en soustrayant :
$$P^{n-1}(PR' - P'R) + Q^{n-1}(QR' - Q'R) + R^{n-1}(RR' - R'R) = 0$$
- Comme R et R' commutent on a donc : $P^{n-1}(PR' - P'R) = Q^{n-1}(-QR' + Q'R)$
- Comme par hypothèse P et R ne sont pas multiples l'un de l'autre par une constante, $(PR' - P'R) \neq 0$
- Idem pour $(-QR' + Q'R)$
- Comme P est premier avec Q, on en déduit que P^{n-1} divise $(Q'R - QR')$
- Par un raisonnement de degrés $(n-1)degP \leq degQ + degR - 1 \leq 2degP - 1$. Ce qui est impossible car $n \geq 3$.

5. Troisième étape : le cas où $deg(R) = 0$. —

- Si n est impair, $P^n + Q^n = (P+Q)(\Sigma(-1)^k Q^k P^{n-k}) = c$