$X^n - a$

La décomposition en facteurs irréductibles du polynôme $X^n - a$, explicitée dans cette note, figure dans Bourbaki, Algèbre V *p.87; elle y apparaît comme un cas très particulier de la théorie de Kummer. Peu évoquée, semble-t-il, ailleurs, cette décomposition mérite d'être plus largement connue, et démontrée directement (i.e sans utiliser la théorie de Kummer).*

Soient n un entier ≥ 2, et K un corps tel que le groupe des racines n-èmes de l'unité $\mu_n(K)$ (désormais noté μ_n) ait n éléments ; autrement dit, le polynôme $X^n - 1$ est décomposé dans $K[X]$ et ses racines sont distintes ; cela entraîne que le polynôme dérivé nX^{n-1} est non nul, donc que n est inversible dans K ; cela entraîne aussi les mêmes propriétés pour les diviseurs d de n ; en particulier, pour tout $u \in K$, on a $X^d - u^d = \prod_{\zeta \in \mu_d}(X - \zeta u)$.

On considère un élément $a \in K^\times$, et l'ordre r de sa classe dans le groupe (multiplicatif) quotient $K^\times/(K^\times)^n$; cet entier est donc le plus petit tel qu'il existe $c \in K$ avec $a^r = c^n$; c'est un diviseur de n. On pose

$$n = rs.$$

Proposition 1. *Sous les hypothèses qui précèdent, l'ensemble $B = \{b \in K | b^s = a\}$ possède s éléments. Dans l'anneau $K[X]$, le polynôme $X^n - a$ se factorise en*

$$X^n - a = \prod_{b \in B}(X^r - b).$$

Chaque facteur $X^r - b$ est irréductible.

Montrons d'abord qu'il existe un élément $b \in K^\times$ tel que

$$a = b^s.$$

Par hypothèse, il existe $c \in K$ tel que $a^r = c^n = (c^s)^r$; par suite, en posant $\zeta = a/c^s$, on a $\zeta \in \mu_r$. Choisissons $\omega \in \mu'_n$ (c'est-à-dire une racine *primitive* n-ème de l'unité) ; en vertu de la relation $\mathrm{ord}(\omega^s) = \mathrm{ord}(\omega)/\mathrm{pgcd}(\mathrm{ord}(\omega), s)$, on voit que ω^s est d'ordre exactement r, et donc qu'il engendre μ_r ; par suite, il existe un entier k tel que $\zeta = \omega^{sk}$; en posant $b = \omega^k c$, on a bien $a = b^s$.

Comme μ_s possède s éléments (dans K), l'ensemble B de l'énoncé a lui aussi s éléments : $B = \{\eta b,\ \eta \in \mu_s\}$.

Soit $b_0 \in B$. On a dans $K[X]$:

$$X^n - a = X^{rs} - b_0^s = \prod_{\eta \in \mu_s}(X^r - \eta b_0) = \prod_{b \in B}(X^r - b).$$

Il reste à montrer que ces facteurs $X^r - b$ sont irréductibles.
Remarquons d'abord que, pour $b \in B$, l'ordre de b dans $K^\times/(K^\times)^r$ est égal à r. En effet, soit t cet ordre ; on a donc $b^t \in (K^\times)^r$, et t divise r ; on a aussi $a^t = b^{st} \in (K^\times)^{rs} = (K^\times)^n$; donc r divise t (et lui est par suite égal), puisque r est l'ordre de la classe de a dans $K^\times/(K^\times)^n$.

On est donc ramené à démontrer le résultat suivant, où l'hypothèse sur le terme constant rend inutile la présence de racines de l'unité dans le corps de base.

Proposition 2. *Soient r un entier ≥ 2, et K un corps dans lequel l'entier r est non nul. Soit $b \in K^\times$ un élément dont la classe dans $K^\times/(K^\times)^r$ est d'ordre égal à r. Alors le polynôme $X^r - b$ est irréductible dans $K[X]$.*

Comme b est non nul et que r est inversible, le polynôme $X^r - b$ est séparable. Il possède donc r racines dans une extension de décomposition $K \subset L$; en notant β l'une de ces racines, les autres sont de la forme $\zeta\beta$, avec $\zeta^r = 1$. Soit $P(X) \in K[X]$ le polynôme minimal (unitaire) de β, et m son degré. Comme le polynôme P divise $X^r - b$, il se décompose dans $L[X]$ de la façon suivante :

$$P(X) \;=\; \prod_{\zeta \in U} (X - \zeta\beta),$$

où $U \subset \mu_r(L)$ est un ensemble de m racines de l'unités. Faisant $X = 0$, on obtient

$$(\prod_{\zeta \in U} \zeta)\beta^m \;=\; (-1)^m P(0) \in K^\times$$

Comme le produit $\prod_{\zeta \in U} \zeta$ est dans $\mu_r(L)$, et que $\beta^r = b$, l'élévation à la puissance r donne

$$b^m \in (K^\times)^r$$

L'hypothèse faite sur b, montre alors que $m = r$, donc que $X^r - b$ est égal à son facteur irréductible $P(X)$.

Remarques 1) La proposition 2, et sa démonstration, sont dues à Abel, du moins lorsque r est premier ; dans ce cas, la condition sur b se réduit à ne pas être une puissance r-ième dans K.

2) La réciproque de la proposition 2 n'est pas vraie en l'absence de racines de l'unité ; autrement dit, la condition sur b n'est pas nécessaire pour l'irréductibilité

3) Dans *Algebra*, ch.VIII, §9, Lang donne des conditions, plus faibles que celles de la proposition 2, assurant que le polynôme est irréductible ; la démonstration en est moins immédiate.

Daniel Ferrand
Novembre 2007