ACTA ARITHMETICA
119.1 (2005)

Stabilité des polynômes

par

NIDAL ALI (Calais)

1. Introduction

DÉFINITION 1. Soient K un corps, $f(x) \in K[x]$ un polynôme irréductible ; on pose $f_1(x) = f(x)$ et pour tout entier $m \geq 2$, $f_m(x) = (f_{m-1} \circ f)(x)$. On dit que f est un *polynôme stable* sur K si pour tout $m \geq 1$, $f_m(x)$ est irréductible sur K.

Dans [4], les auteurs donnent une méthode efficace pour tester la stabilité de presque tous les polynômes unitaires quadratiques. Dans [10], Odoni montre que le polynôme générique

$$G(s_1, \ldots, s_n, x) = x^n - s_1 x^{n-1} + \cdots + (-1)^n s_n$$

est un polynôme stable dans $A[s_1, \ldots, s_n, x]$ où A est un anneau intégralement clos et $s_1, \ldots, s_n$ sont des variables algébriquement indépendantes sur le corps des fractions de A. Dans [5], les auteurs montrent la stabilité de tout polynôme irréductible de la forme $x^n - c \in R[x]$ où R est soit $\mathbb{Z}$, soit un anneau des polynômes à une variable sur $\mathbb{Z}$ ou sur un corps algébriquement clos.

Soient maintenant K un corps de nombres de degré n, et $\{w_1, \ldots, w_n\}$ une base d'entiers de K. Soient $u_1, \ldots, u_n$ des variables algébriquement indépendantes sur K, $\xi = u_1 w_1 + \cdots + u_n w_n$ et $F(u_1, \ldots, u_n, x) = \operatorname{Irr}(\xi, L, x)$ où $L = \mathbb{Q}(u_1, \ldots, u_n)$. Le polynôme F est à coefficients entiers, homogène et de degré n. (Voir Remarque 2.)

DÉFINITION 2. On dira que $F(u_1, \ldots, u_n, x)$ est un *polynôme générique* des entiers de K.

Le polynôme $F(u_1, \ldots, u_n, x)$ est générique dans le sens où, en spécialisant $u_1, \ldots, u_n$ dans $\mathbb{Z}$, on obtient $F(u_1^*, \ldots, u_n^*, x) = [\operatorname{Irr}(\xi^*, \mathbb{Q}, x)]^d$ où $d = n/t$ avec $t = [\mathbb{Q}(\xi^*) : \mathbb{Q}]$ et ξ^* est un entier de K.

2000 *Mathematics Subject Classification*: 11R09, 11T06, 12E10.

Key words and phrases: polynomial, irreducibility, iteration, stability, inert prime, totally ramified.

Une question importante, motivée par le résultat d'Odoni cité ci-dessus, est de savoir si le polynôme $F(u_1, \ldots, u_n, x)$ est stable sur L. Si tel est le cas, est-ce qu'il y a une infinité de spécialisations de $(u_1, \ldots, u_n)$ en $(u_1^*, \ldots, u_n^*)$ dans $\mathbb{Z}^n$ tels que $F(u_1^*, \ldots, u_n^*, x)$ est stable sur $\mathbb{Q}$? Les trois théorèmes qui suivent montrent que la réponse est positive si certaines conditions arithmétiques sur K sont verifiées.

THÉORÈME 1. *Soit $K = \mathbb{Q}(\theta)$ où θ est une racine dans $\overline{\mathbb{Q}}$ d'un polynôme irréductible dans $\mathbb{Z}[x]$ de la forme $f(x) = x^n - c$. Alors :*

(i) *Il existe une infinité d'entiers α de K tels que le polynôme minimal de α est stable sur $\mathbb{Q}$.*
(ii) *Le polynôme générique des entiers de K est stable sur L.*

THÉORÈME 2. *Soit K un corps de nombres de degré n dans lequel il existe un nombre premier p de $\mathbb{Z}$ totalement ramifié. Alors :*

(i) *Il existe une infinité d'entiers α de K tels que le polynôme minimal de α est stable sur $\mathbb{Q}$.*
(ii) *Le polynôme générique des entiers de K est stable sur L.*

EXEMPLE 1. Ce théorème s'applique en particulier pour toute extension galoisienne $K/\mathbb{Q}$ de degré premier n car tout nombre premier p de $\mathbb{Z}$ ramifié dans K est totalement ramifié.

Maintenant, est-ce que la stabilité du polynôme générique est vraie lorsque K possède un nombre premier p inerte ? On va montrer que cela est vraie si on suppose qu'une certaine propriété de stabilité sur $\mathbb{F}_p$ est verifiée.

DÉFINITION 3. Soient n, e deux entiers naturels non nuls, et p un nombre premier de $\mathbb{Z}$. On définit la *propriété* $S(n, p, e)$ par : il existe un polynôme unitaire, irréductible de degré n et stable sur $\mathbb{F}_{p^e}$.

Il faut remarquer que cette propriété peut aussi bien être vraie que fausse. (Voir section 3.)

THÉORÈME 3. *Soit K un corps de nombres de degré n dans lequel il existe un nombre premier p inerte. On suppose que $S(n, p, 1)$ est vraie. Alors :*

(i) *Il existe une infinité d'entiers α de K tels que le polynôme minimal de α est stable sur $\mathbb{Q}$.*
(ii) *Le polynôme générique des entiers de K est stable sur L.*

REMARQUE 1. Soit K un corps de nombres de degré n dans lequel il existe un nombre premier p inerte. Alors d'après le Théorème de Tschebotaröw ([3, Lemme 3]), il existe une infinité de nombres premiers l inertes dans K. Il est possible que pour l'un des ces nombres l, $S(n, l, 1)$ soit verifiée. Cela signifie que l'hypothèse du Théorème 3 relative à $S(n,p,1)$ est probablement superflue.

Les trois théorèmes précédents donnent la stabilité de F sur L sous certaines conditions arithmétiques, mais dans le cas général, i.e. pour un corps de nombres K de degré n quelconque, on ne sait pas si F est stable ou non.

Cependant on montre dans la section 4 le résultat suivant:

Proposition 1. *Le polynôme $F_2(u_1,\dots,u_n,x)$ est irréductible sur L.*

2. Lemmes préliminaires

Définition 4. Soient K un corps de nombres de degré n, θ un élément primitif de K sur $\mathbb{Q}$, et A son anneau des entiers. On définit l'*indice* de θ (noté $I(\theta)$) comme le cardinal de $A/\mathbb{Z}[\theta]$.

Lemme 1 ([7, Art. 96, p. 176]). *Soient K un corps de nombres de degré n, A son anneau des entiers, et p un nombre premier rationnel tel que sa décomposition dans A est donnée par $Ap=\prod_{i=1}^{t}\mathcal{P}_i^{e_i}$. On suppose qu'il existe $r_1,\dots,r_{s+1}$ dans $\mathbb{N}^*$ tels que $r_1+\dots+r_{s+1}=t$ et*

$$\begin{cases}\deg(\mathcal{P}_1)=\deg(\mathcal{P}_2)=\dots=\deg(\mathcal{P}_{r_1}):=c_1,\\ \deg(\mathcal{P}_{r_1+1})=\deg(\mathcal{P}_{r_1+2})=\dots=\deg(\mathcal{P}_{r_2}):=c_2,\\ \vdots\\ \deg(\mathcal{P}_{r_s+1})=\deg(\mathcal{P}_{r_s+2})=\dots=\deg(\mathcal{P}_{r_{s+1}}):=c_{s+1}.\end{cases}$$

Alors pour que p divise tous les indices $I(\theta)$ pour tout entier primitif θ de K il faut et il suffit qu'il existe $j\in\{1,\dots,s+1\}$ tel que le nombre des polynômes unitaires, irréductibles sur $\mathbb{F}_p$ de degré c_j est strictement plus petit que r_j.

Lemme 2 ([7, Th. 1, p. 137]). *Soient K un corps de nombres de degré n, A son anneau des entiers, $F(u_1,\dots,u_n,x)$ le polynôme générique des entiers de K, et p un nombre premier de $\mathbb{Z}$ tel que la décomposition de p dans A est donnée par $Ap=\prod_{i=1}^{t}\mathcal{P}_i^{e_i}$. Alors*

$$F(u_1,\dots,u_n,x)=\prod_{i=1}^{t}F_i(u_1,\dots,u_n,x)^{e_i}+pG(u_1,\dots,u_n,x)$$

où les polynômes $F_i(u_1,\dots,u_n,x)$ sont irréductibles sur $\mathbb{F}_p$, unitaires, et $G(u_1,\dots,u_n,x)$ n'est pas divisible par aucun facteur $F_i(u_1,\dots,u_n,x)$ dans $\mathbb{F}_p[u_1,\dots,u_n,x]$.

Lemme 3 ([7, Art. 95, p. 172]). *Soient K un corps de nombres de degré n, θ un élément primitif de K sur $\mathbb{Q}$, et $f(x)=\mathrm{Irr}(\theta,\mathbb{Q},x)$. On suppose que*

$$f(x) = \prod_{i=1}^{t} f_i(x)^{e_i} + ph(x)$$

avec tous les $f_i(x)$ *irréductibles sur* $\mathbb{F}_p$ *et* $\deg(h) < \deg(f)$. *Alors les deux conditions suivantes sont équivalentes* :

(i) $p \mid I(\theta)$.
(ii) *Il existe* $i \in \{1, \dots, t\}$ *tel que* $e_i \geq 2$ *et* $f_i(x) \mid h(x)$ *dans* $\mathbb{F}_p[x]$.

Définition 5. Soient $f(x) = a_n x^n + a_{n-1}x^{n-1} + \cdots + a_1 x + a_0$ un polynôme à coefficients entiers et $r \geq 1$ un entier premier à n. On dit que f est un *polynôme* p^r*-Eisenstein* pour un certain nombre premier p de $\mathbb{Z}$ si :

(i) $\vartheta_p(a_0) = r$.
(ii) $\vartheta_p(a_j) \geq r$ pour tout $j = 1, \dots, n-1$.
(iii) $\vartheta_p(a_n) = 0$.

Lemme 4. *Soient* K *un corps de nombres de degré* n, A *son anneau des entiers*, *et* p *un nombre premier de* $\mathbb{Z}$. *Alors les trois conditions suivantes sont équivalentes* :

(i) p *est totalement ramifié dans* K.
(ii) *Il existe un polynôme* $\phi(x) \in \mathbb{Z}[x]$ *et une racine* $\alpha \in \overline{\mathbb{Q}}$ *de* ϕ *tels que* $K = \mathbb{Q}(\alpha)$ *et* $\phi(x)$ *est un polynôme* p*-Eisenstein.*
(iii) *Il existe un polynôme* $\psi(x) \in \mathbb{Z}[x]$ *et une racine* $\beta \in \overline{\mathbb{Q}}$ *de* ψ *tels que* $K = \mathbb{Q}(\beta)$ *et* $\psi(x)$ *est un polynôme* p^r*-Eisenstein pour un certain entier* r *premier à* $\deg\psi$.

Preuve. (i)$\Rightarrow$(ii). Soit $\mathcal{P}$ un idéal premier de A au-dessus de p. Alors $Ap = \mathcal{P}^n$ avec $\mathcal{P} \cap \mathbb{Z} = p$.

Supposons que $p \mid I(\gamma)$ pour tout entier primitif γ de K. Alors d'après le Lemme 1 ($Ap = \mathcal{P}^n$, $j = 1$, $c_j = 1$) le nombre des polynômes unitaires irréductibles dans $\mathbb{F}_p[x]$ et de premier degré, qui est égale à p, est strictement plus petit que le nombre des idéaux $\mathcal{P}_i$ de degré c_j, qui est 1, donc $p < 1$, ce qui est absurde. Donc il existe au moins un entier primitif λ de K tel que $p \nmid I(\lambda)$.

Maintenant soit $\{w_1, \dots, w_n\}$ une base d'entiers de K, $\xi = u_1 w_1 + \cdots + u_n w_n$, $F(u_1, \dots, u_n, x)$ le polynôme générique des entiers de K. Puisque p est totalement ramifié dans K, d'après le Lemme 2 on a

$$F(u_1, \dots, u_n, x) = L(u_1, \dots, u_n, x)^n + pG(u_1, \dots, u_n, x)$$

avec $L(u_1, \dots, u_n, x)$ linéaire en $u_1, \dots, u_n, x$ et ne divisant pas le polynôme $G(u_1, \dots, u_n, x)$ dans $\mathbb{F}_p[u_1, \dots, u_n, x]$.

Soit $(l_1, \dots, l_n) \in \mathbb{Z}^n$ tel que $L(u_1, \dots, u_n, x) = x + l_1 u_1 + \cdots + l_n u_n$ et soit $(u_1^*, \dots, u_n^*) \in \mathbb{Z}^n$ tel que $\lambda = u_1^* w_1 + \cdots + u_n^* w_n$.

Soit $f(x) = \mathrm{Irr}(\lambda, \mathbb{Q}, x)$. Alors

$$f(x) = F(u_1^*, \dots, u_n^*, x) = (x+a)^n + pG(u_1^*, \dots, u_n^*, x)\,;$$

ceci implique que $f(x) = (x+a)^n + ph(x)$ avec $h(x) = G(u_1^*, \dots, u_n^*, x)$.

Puisque $p \nmid I(\lambda)$, le Lemme 3 montre que $(x+a) \nmid h(x)$ dans $\mathbb{F}_p[x]$. On pose $\phi(X) = f(X-a) = X^n + ph(X-a)$; il est facile de voir que $\phi(X)$ est un polynôme p-Eisenstein.

(ii)$\Rightarrow$(iii). Évident.

(iii)$\Rightarrow$(i). On pose $\psi(x) = x^m + b_{m-1}x^{m-1} + \cdots + b_1x + b_0 \in \mathbb{Z}[x]$. Soient $\mathcal{P}$ un idéal premier de A au-dessus de p et e son indice de ramification. Les deux inégalités: $[\mathbb{Q}(\beta) : \mathbb{Q}] = n \leq m$ et $e \leq [\mathbb{Q}(\beta) : \mathbb{Q}]$ ([9, Théorème 21, p. 65]) montrent que $e \leq m$. On va montrer que $e = m$. En effet, on a

$$\psi(\beta) = 0 = \beta^m + b_{m-1}\beta^{m-1} + \cdots + b_1\beta + b_0 \equiv \beta^m \pmod{\mathcal{P}},$$

donc $\vartheta_{\mathcal{P}}(\beta) > 0$. On en déduit que pour tout $j \in \{1, \dots, m-1\}$,

$$\vartheta_{\mathcal{P}}(b_j\beta^j) = \vartheta_{\mathcal{P}}(b_j) + j\vartheta_{\mathcal{P}}(\beta) = e\vartheta_p(b_j) + j\vartheta_{\mathcal{P}}(\beta) > er = \vartheta_{\mathcal{P}}(b_0).$$

Il s'ensuit que

$$\begin{aligned}\vartheta_{\mathcal{P}}(-b_{m-1}\beta^{m-1} - \cdots - b_1\beta - b_0)& \\ &= \inf\{\vartheta_{\mathcal{P}}(-b_{m-1}\beta^{m-1} - \cdots - b_1\beta), \vartheta_{\mathcal{P}}(b_0)\} \\ &= \vartheta_{\mathcal{P}}(b_0) = er.\end{aligned}$$

Ceci implique que $m\vartheta_{\mathcal{P}}(\beta) = er$.

Puisque $\beta^m = -b_{m-1}\beta^{m-1} - \cdots - b_1\beta - b_0$, on a , $\vartheta_{\mathcal{P}}(\beta^m) = m\vartheta_{\mathcal{P}}(\beta) = er$, donc $m \mid er$. Comme $(m, r) = 1$, on obtient que $m \mid e$ et par suite $m \leq e$, d'où l'égalité. ∎

Corollaire 1. *Soient p un nombre premier de $\mathbb{Z}$ et $f(x) = a_nx^n + a_{n-1}x^{n-1} + \cdots + a_1x + a_0 \in \mathbb{Z}[x]$ un polynôme p^r-Eisenstein pour un certain entier naturel r premier à n. Alors $f(x)$ est stable sur $\mathbb{Q}$.*

Preuve. Dans (iii)$\Rightarrow$(i), on a montré que $\deg(\psi(x)) = [K : \mathbb{Q}]$, donc on obtient en même temps l'irréductibilité sur $\mathbb{Q}$ du polynôme $\psi(x)$ qui est p^r-Eisenstein. Ce résultat a été montré par Dumas ([6, 12-2, p. 252]) en utilisant le polygone de Newton.

Pour montrer qu'un polynôme p^r-Eisenstein est stable il suffit de montrer que le composé de deux polynômes p^r-Eisenstein est p^r-Eisenstein. En effet, soient $f(x) = a_nx^n + a_{n-1}x^{n-1} + \cdots + a_1x + a_0$ et $g(x) = b_mx^m + b_{m-1}x^{m-1} + \cdots + b_1x + b_0$ deux polynômes à coefficients entiers, p^r-Eisenstein. On pose

$$f \circ g(x) = c_lx^l + c_{l-1}x^{l-1} + \cdots + c_1x + c_0$$

avec $l = mn$, $c_l = a_nb_m^n$ et

$$c_0 = f \circ g(0) = f(b_0) = a_nb_0^n + a_{n-1}b_0^{n-1} + \cdots + a_1b_0 + a_0.$$

On a $f(x) \equiv a_n x^n \pmod{p^r}$ et $g(x) \equiv b_m x^m \pmod{p^r}$, donc $f \circ g(x) \equiv c_l x^l \pmod{p^r}$, d'où p^r divise $c_0, \ldots, c_{l-1}$. Il est évident que $\vartheta_p(c_0) = \vartheta_p(a_0) = r$, $p \nmid c_l$ et que $(r, l) = 1$, d'où le résultat. ∎

LEMME 5 ([4, Théorème 5]). *Soient p un nombre premier impaire de $\mathbb{Z}$, q une puissance de p, et $f(x) = x^2 - ax + b \in \mathbb{F}_q[x]$ un polynôme irréductible de discriminant d. Alors les deux conditions suivantes sont équivalentes :*

(i) *$f(x)$ est stable sur $\mathbb{F}_q$.*
(ii) *Pour tout entier $m \geq 1$, $f_m(-d/4)$ n'est pas un carré dans $\mathbb{F}_q$.*

LEMME 6 ([5, Corollaire 5]). *Soit $f(x) = x^n - c \in R[x]$ un polynôme irréductible où R est soit $\mathbb{Z}$, soit un anneau des polynômes à une variable sur $\mathbb{Z}$ ou sur un corps algébriquement clos. Alors f est un polynôme stable dans $R[x]$.*

LEMME 7 ([8, Théorème 16, p. 221]). *Soit K un corps et $f(x) = x^n - \alpha \in K[x]$. Alors $f(x)$ est réductible sur K si et seulement si il existe p premier tel que $p \mid n$ et $\alpha \in K^p$, ou $4 \mid n$ et $\alpha \in -4K^4$.*

LEMME 8. *Soit K un corps, $f(x)$, $g(x)$ deux polynômes dans $K[x]$, et soit α une racine quelconque de $f(x)$ dans une clôture algébrique de K. Alors les deux conditions suivantes sont équivalentes.*

(i) *$f \circ g(x)$ est irréductible sur K.*
(ii) *$f(x)$ est irréductible sur K et $g(x) - \alpha$ est irréductible sur $K(\alpha)$.*

Preuve. Voir [11, Satz 4, p. 288] ou [1, énoncé 2.9] pour deux preuves différentes.

3. Stabilité sur les corps finis. Maintenant on va étudier la propriété $S(n, p, e)$ définie dans l'introduction, qui va intervenir dans le Théorème 3. Tout d'abord il faut remarquer que $S(2, 2, 1)$ n'est pas vraie. En effet, le seul polynôme unitaire et irréductible du second degré sur $\mathbb{F}_2$ est $f(x) = x^2 + x + 1$ et il est instable puisque

$$f_3(x) = (x^4 + x^3 + 1)(x^4 + x^3 + x^2 + x + 1).$$

PROPOSITION 2. *Soient p un nombre premier de $\mathbb{Z}$, et n, e deux entiers naturels non nuls. Alors :*

(i) *$S(n, p, e) \Rightarrow S(n, p, e \times s)$, pour tout entier s premier à n.*
(ii) *$S(n, p, e) \Rightarrow S(n^m, p, e)$, pour tout entier $m \geq 1$.*

Preuve. (i) Soient s un entier premier à n et $f(x)$ un polynôme unitaire, de degré n et stable sur $\mathbb{F}_{p^e}$. Pour tout entier $m \geq 1$, on désigne par α_m l'une des racines de $f_m(x)$, donc $[\mathbb{F}_{p^e}(\alpha_m) : \mathbb{F}_{p^e}] = n^m$. On considère le diagramme suivant :

$$\begin{tikzcd}[arrows=dash] & \mathbb{F}_{p^{es}}(\alpha_m) \arrow[dl] \arrow[dr] & \\ \mathbb{F}_{p^{es}} \arrow[dr, "s"'] & & \mathbb{F}_{p^e}(\alpha_m) \arrow[dl, "n^m"] \\ & \mathbb{F}_{p^e} & \end{tikzcd}$$

Comme $(s, n) = 1$, on a $(s, n^m) = 1$. Ceci implique que $\mathbb{F}_{p^{es}}$ et $\mathbb{F}_{p^e}(\alpha_m)$ sont linéairement disjoints sur $\mathbb{F}_{p^e}$, donc $[\mathbb{F}_{p^{es}}(\alpha_m) : \mathbb{F}_{p^{es}}] = [\mathbb{F}_{p^e}(\alpha_m) : \mathbb{F}_{p^e}] = n^m$; ainsi $f_m(x)$ est irréductible sur $\mathbb{F}_{p^{es}}$ et par suite $f(x)$ est stable sur $\mathbb{F}_{p^{es}}$.

(ii) Supposons que $S(n, p, e)$ est vraie. Il existe donc un polynôme $g(x)$ unitaire, irréductible de degré n, stable sur $\mathbb{F}_{p^e}$. Mais la stabilité de $g(x)$ implique celle de $g_m(x)$ qui a comme degré n^m ; donc pour tout $m \geq 1$, $S(n^m, p, e)$ est vraie. ∎

Proposition 3. *Soit p un nombre premier impair. Alors pour tout entier $e \geq 1$, $S(2, p, e)$ est vraie.*

Preuve. On pose $q = p^e$ et on va montrer en utilisant le Lemme 5 qu'il existe un polynôme unitaire quadratique stable sur $\mathbb{F}_q$. Pour $a \in \mathbb{F}_q^*$ soit $\left(\frac{a}{q}\right)$ le symbole de Legendre ; on note que $\left(\frac{a}{q}\right) = 1$ si a est un carré de $\mathbb{F}_q^*$ et $\left(\frac{a}{q}\right) = -1$ sinon.

On distingue deux cas selon les valeurs de q :

1) $q \equiv 1 \pmod 4$. Soit $a \in \mathbb{F}_q^*$ tel que $\left(\frac{a}{q}\right) = -1$; alors le polynôme $f(x) = (x - a)^2 + a$ est stable sur $\mathbb{F}_q$. En effet, soit d le discriminant de f ; alors $d = -4a$. Comme $\left(\frac{a}{q}\right) = -1$ et $\left(\frac{-1}{q}\right) = 1$, on a $\left(\frac{d}{q}\right) = -1$, donc $f(x)$ est irréductible sur $\mathbb{F}_q$.

Puisque $-d/4 = a$ et $f(a) = a$, on a $f_m(a) = a$ pour tout $m \geq 1$, par suite le Lemme 5 s'applique et f est stable sur $\mathbb{F}_q$.

2) Si $q \equiv -1 \pmod 4$ alors $\left(\frac{-1}{q}\right) = -1$ et il existe $u, v \in \mathbb{F}_q^*$ tels que $-1 = u^2 + v^2$ ([2, énoncé 12-2]).

Posons $f(x) = (x - 4u^2 - 2)^2 + 4u^2$. Le polynôme f est irréductible sur $\mathbb{F}_q$ car son discriminant $d = -16u^2$ n'est pas un carré dans $\mathbb{F}_q$. Maintenant $-d/4 = 4u^2$, $f(-d/4) = f(4u^2) = -4v^2$ et $f_2(-d/4) = f(-4v^2) = -4v^2$. Or $-4v^2$ n'est pas un carré dans $\mathbb{F}_q$, ce qui implique que pour tout $m \geq 1$, $f_m(-d/4)$ n'est pas un carré dans $\mathbb{F}_q$ et par suite le polynôme $f(x)$ est stable sur $\mathbb{F}_q$. ∎

4. Preuves des résultats

Preuve du Théorème 1. (i) D'après le Lemme 6, le polynôme $f(x) = \mathrm{Irr}(\theta, \mathbb{Q}, x)$ est stable sur $\mathbb{Q}$.

Maintenant pour tout $(i, l) \in \mathbb{Z}^2$ tel que l est premier à n, on pose $\alpha_i = i\theta^l$, $g_i(x) = x^n - i^n c^l$; alors $g_i(\alpha_i) = 0$. Le polynôme $g_i(x)$ est encore irréductible sur $\mathbb{Q}$. En effet, supposons que g_i soit réductible sur $\mathbb{Q}$; ceci implique d'après le Lemme 7 qu'il existe un nombre premier p divisant n tel que $i^n c^l \in \mathbb{Q}^p$, ou $4 \mid n$ et $i^n c^l \in -4\mathbb{Q}^4$.

Si $i^n c^l \in \mathbb{Q}^p$ alors $c^l \in \mathbb{Q}^p$. Or $(l, n) = 1$, donc $c \in \mathbb{Q}^p$, d'où f est réductible sur $\mathbb{Q}$, ce qui est absurde.

Si $4 \mid n$ et $i^n c^l \in -4\mathbb{Q}^4$ alors il existe $a \in \mathbb{Q}$ tel que $c^l = -4a^4$. On pose $c = -2^h d$ avec d impair ; alors $c^l = -2^{hl} d^l = -4a^4$. Pour tout nombre premier q tel que $q \mid d$, on a $\vartheta_q(d) \equiv 0 \pmod 4$, donc il existe $e \in \mathbb{Q}$ tel que $d = e^4$. Ceci implique que $c^l = -2^{hl} e^{4l} = -4a^4$, ce qui donne $hl \equiv 2 \pmod 4$, d'où $h \equiv 2 \pmod 4$ puisque l est impair. Par suite $c \in -4\mathbb{Q}^4$, i.e. f est réductible sur $\mathbb{Q}$, ce qui n'est pas possible. Donc g_i est irréductible sur $\mathbb{Q}$.

Ainsi on obtient une infinité d'entiers de K ayant des polynômes minimaux stables sur $\mathbb{Q}$.

(ii) Soit α un entier de K tel que $f(x) = \operatorname{Irr}(\alpha, \mathbb{Q}, x)$ est stable sur $\mathbb{Q}$. Alors il existe $(u_1^*, \dots, u_n^*) \in \mathbb{Z}^n$ tel que $f(x) = F(u_1^*, \dots, u_n^*, x)$, donc $F(u_1, \dots, u_n, x)$ est stable sur L. ∎

Preuve du Théorème 2. (i) Soit p un premier de $\mathbb{Z}$ totalement ramifié dans K. D'après le Lemme 4, on sait qu'il existe un entier primitif α de K tel que $\phi(X) = \operatorname{Irr}(\alpha, K, x)$ est un polynôme p-Eisenstein. Soit A l'anneau des entiers de K et pour tout $i \in \mathbb{Z}$, soit $\alpha_i = \alpha + ip \in A$.

On peut vérifier que le polynôme minimal de α_i est encore p-Eisenstein, donc stable sur $\mathbb{Q}$. Ainsi on a construit une infinité d'entiers de K ayant des polynômes minimaux stables sur $\mathbb{Q}$.

(ii) On fait le même raisonnement qu'en cas du Théorème 1. ∎

Preuve du Théorème 3. (i) Soient A l'anneau des entiers de K et $g(x)$ le polynôme unitaire, de degré n et stable sur $\mathbb{F}_p$. Comme p est inerte, ceci implique que A/pA est une extension de $\mathbb{F}_p$ de degré n. Soit $\beta \in A$ tel que $\overline{\beta}$ est un élément primitif de A/pA et $\operatorname{Irr}(\overline{\beta}, \mathbb{F}_p, x) = g(x)$. Le polynôme $g(x)$ est stable sur $\mathbb{F}_p$, donc $\operatorname{Irr}(\overline{\beta}, \mathbb{F}_p, x)$ est stable sur $\mathbb{F}_p$ et par suite $\operatorname{Irr}(\beta, \mathbb{Q}, x)$ est stable sur $\mathbb{Q}$.

Pour tout élément $a \in A$ et pour tout entier $l \geq 0$, soit $\alpha = \beta^{p^l} + pa$; alors $\overline{\alpha} = \overline{\beta}^{p^l}$, donc $\operatorname{Irr}(\alpha, \mathbb{Q}, x)$ est stable sur $\mathbb{Q}$. Par conséquent, on a construit une infinité d'éléments de A ayant des polynômes minimaux stables sur $\mathbb{Q}$.

(ii) On fait le même raisonnement qu'en cas du Théorème 1. ∎

REMARQUE 2. Soient K un corps de nombres de degré n, et $\{w_1, \dots, w_n\}$ une base d'entiers de K. Soit $F(u_1, \dots, u_n, x) = \operatorname{Irr}(\xi, L, x)$ le polynôme générique des entiers de K. Alors on a

$$F(u_1, \dots, u_n, x) = \prod_{i=1}^{n} (x - \xi_{\sigma_i})$$

où $\sigma_1, \ldots, \sigma_n$ désignent les n plongements distincts de K dans $\overline{\mathbb{Q}}(u_1, \ldots, u_n)$ et $\xi_{\sigma_i} = u_1\sigma_i(w_1) + \cdots + u_n\sigma_i(w_n)$. En effet, $\xi \in \mathbb{Q}(u_1, \ldots, u_n, w_1, \ldots, w_n)$ et $[\mathbb{Q}(u_1, \ldots, u_n, w_1, \ldots, w_n) : \mathbb{Q}(u_1, \ldots, u_n)] = n$. Comme $\xi_{\sigma_i} \neq \xi_{\sigma_j}$ pour tout $i \neq j$, il s'ensuit que ξ est un élément primitif de $\mathbb{Q}(u_1, \ldots, u_n, w_1, \ldots, w_n)$ sur $\mathbb{Q}(u_1, \ldots, u_n)$, donc $\deg_x(F(x)) = n$. On a aussi montré que si θ est un élément primitif de K alors $\mathbb{Q}(u_1, \ldots, u_n, \xi) = \mathbb{Q}(u_1, \ldots, u_n, \theta)$.

La formule de décomposition de F montre en particulier que F est homogène en $(u_1, \ldots, u_n, x)$.

Preuve de la Proposition 1. Supposons que $F_2(u_1, \ldots, u_n, x)$ est réductible sur L. Alors d'après le Lemme 8, $F(u_1, \ldots, u_n, x) - \xi$ est réductible sur $L(\xi)$. Mais d'après la Remarque 2, $L(\xi) = L(\theta) = \mathbb{Q}(\theta, u_1, \ldots, u_n)$, donc soit

$$\begin{aligned} F(u_1, \ldots, u_n, x) - \xi &= T(u_1, \ldots, u_n, x) \cdot H(u_1, \ldots, u_n, x) \\ &= [T_m(*) + T_{m-1}(*) + \cdots + T_1(*) + T_0(*)] \\ &\quad \cdot [H_k(*) + H_{k-1}(*) + \cdots + H_1(*) + H_0(*)] \end{aligned}$$

avec $m + k = n$, T_i et H_j désignant les composantes homogènes de T et H de degrés respectifs i et j dans $\mathbb{Q}(\theta, u_1, \ldots, u_n)[x]$. Pour faciliter l'écriture on a noté $(u_1, \ldots, u_n, x) = (*)$. Or le polynôme $F(*)$ est homogène, donc on en déduit après identification que

$$\begin{aligned}
&(1) && T_m(*)H_k(*) = F(*),\\
&(2) && T_m(*)H_{k-1}(*) + T_{m-1}(*)H_k(*) = 0,\\
&(3) && T_m(*)H_{k-2}(*) + T_{m-1}(*)H_{k-1}(*) + T_{m-2}(*)H_k(*) = 0,\\
& && \vdots\\
&(n) && T_1(*)H_0(*) + T_0(*)H_1(*) = -\xi,\\
&(n+1) && T_0(*)H_0(*) = 0.
\end{aligned}$$

Comme $F(*)$ est irréductible sur $L = \mathbb{Q}(u_1, \ldots, u_n)$, il est séparable. Ceci implique que d'après (1), $T_m(*)$ est premier à $H_k(*)$ dans $L(\theta)[x]$. Or d'après (2), $T_m(*) \mid T_{m-1}(*) \cdot H_k(*)$, donc $T_m(*) \mid T_{m-1}(*)$. La seule possibilité est que $T_{m-1}(*) = 0$. De même on montre que $H_{k-1}(*) = 0$. Maintenant l'équation (3) s'écrit $T_m(*)H_{k-2}(*) + T_{m-2}(*)H_k(*) = 0$. Ceci implique que $T_m(*) \mid T_{m-2}(*)$ et $H_k(*) \mid H_{k-2}(*)$, donc $T_{m-2}(*) = H_{k-2}(*) = 0$ et par suite on obtient avec le même raisonnement que $T_i(*) = 0$, $H_j(*) = 0$ pour tout $(i, j) \in \{2, \ldots, m-1\} \times \{2, \ldots, k-1\}$. Puisque $T_0(*)H_0(*) = 0$, on peut supposer que $T_0(*) = 0$.

La formule (n) montre que $T_1(*)H_0(*) = -\xi$. On pose $H_0(*) = b$ avec $b \in Q(\theta)$; donc il existe $a \in Q(\theta)$ tel que $T_1(*) = a\xi$ et $ab = -1$. Par suite on obtient

$$F(*) - \xi = [T_m(*) + a\xi][H_k(*) + H_1(*) + b].$$

On a $H_1(*) = 0$, sinon dans $F(*) - \xi$, il y aurait une composante homogène de degré 2 qui est $a\xi H_1(*)$, ce qui n'est pas possible. Donc $F(*) - \xi = [T_m(*) + a\xi][H_k(*) + b] = T_m(*)H_k(*) + bT_m(*) + a\xi H_k(*) + ab\xi$. Après identification des parties homogènes de deux membres de l'égalité on obtient $bT_m(*) + a\xi H_k(*) = 0$, ce qui est absurde puisque a et b sont non nuls et $T_m(*)$ est premier à $H_k(*)$ dans $L(\theta)[x]$. ∎

5. Conclusion. Dans les trois théorèmes, on a montré qu'il existe une infinité d'entiers du corps K tels que leurs polynômes minimaux sont stables sur $\mathbb{Q}$, et aussi la stabilité sur L du polynôme générique des entiers $F(u_1, \ldots, u_n, x)$. Mais il faut remarquer que la stabilité de F sur L n'implique pas en général l'existence d'un ou plusieurs entiers de K ayant des polynômes minimaux stables sur $\mathbb{Q}$.

Maintenant et plus généralement on peut définir un polynôme générique du corps K en prenant $\{w_1, \ldots, w_n\}$ une base quelconque de K et en construisant le polynôme $F(u_1, \ldots, u_n, x) = \mathrm{Irr}(u_1w_1 + \cdots + u_nw_n, L, x)$. Pour étudier sa stabilité, on peut choisir n'importe quelle base de K. En effet, soient $\{\theta_1, \ldots, \theta_n\}$ une autre base de K, $v_1, \ldots, v_n$ des variables algébriquement indépendantes sur K, $H = \mathbb{Q}(v_1, \ldots, v_n)$, et soient $\eta = v_1\theta_1 + \cdots + v_n\theta_n$, $G(v_1, \ldots, v_n, x) = \mathrm{Irr}(\eta, H, x)$. On va vérifier qu'il y a équivalence entre la stabilité de F sur L et celle de G sur H :

Soit M la matrice de passage de $\{\theta_1, \ldots, \theta_n\}$ à $\{w_1, \ldots, w_n\}$. Alors

$$\begin{aligned}\xi &= u_1w_1 + \cdots + u_nw_n \\ &= (u_1, \ldots, u_n) \cdot \begin{pmatrix} w_1 \\ \vdots \\ w_n \end{pmatrix} = (u_1, \ldots, u_n) \cdot M \cdot \begin{pmatrix} \theta_1 \\ \vdots \\ \theta_n \end{pmatrix} \\ &= (v'_1, \ldots, v'_n) \cdot \begin{pmatrix} \theta_1 \\ \vdots \\ \theta_n \end{pmatrix} = v'_1\theta_1 + \cdots + v'_n\theta_n.\end{aligned}$$

Cela montre que $F(u_1, \ldots, u_n, x) = G(v'_1, \ldots, v'_n, x)$. Or les v'_i sont linéaires en $u_1, \ldots, u_n$ et réciproquement ceci implique que $L = \mathbb{Q}(u_1, \ldots, u_n) = \mathbb{Q}(v'_1, \ldots, v'_n)$ et ils sont algébriquement indépendants sur $\mathbb{Q}$; donc on peut prendre $v_1 = v'_1, \ldots, v_n = v'_n$ et par suite $\xi = u_1w_1 + \cdots + u_nw_n = v_1\theta_1 + \cdots + v_n\theta_n = \eta$, $F(u_1, \ldots, u_n, x) = G(v_1, \ldots, v_n, x)$. Ainsi on obtient l'équivalence du stabilité de F et G sur L.

Remerciements. Je tiens à remercier mon directeur de thèse M. Ayad pour les discussions ainsi que pour ses conseils qui m'ont permis de mener à terme ce travail.

Références

[1] M. Ayad, *Théorie de Galois, 122 exercices corrigés*, *niveau I*, Ellipses, Paris, 1997.
[2] —, *Théorie de Galois, 115 exercices corrigés*, *niveau II*, Ellipses, Paris, 1997.
[3] —, *On irreducible polynomials over* $\mathbb{Q}$ *which are reducible over* $\mathbb{F}_p$ *for all* p, preprint, 2004.
[4] M. Ayad and D. L. McQuillan, *Irreducibility of the iterates of a quadratic polynomial over a field*, Acta Arith. 93 (2000), 87–97.
[5] L. Danielson and B. Fein, *On the irreducibility of the iterates of* $x^n - b$, Proc. Amer. Math. Soc. 130 (2001), 1589–1596.
[6] G. Dumas, *Sur quelques cas d'irréductibilité des polynômes à coefficients rationnels*, J. Math. Pures Appl. (6) 2 (1906), 191–258.
[7] H. Hancock, *Foundations of the Theory of Algebraic Numbers*, *Vol. 2*, Mac Millan, New York, 1931.
[8] S. Lang, *Algebra*, Addison-Wesley, 1965.
[9] D. A. Marcus, *Number Fields*, Springer, 1977.
[10] R. W. K. Odoni, *The Galois theory of iterates and composites of polynomials*, Proc. London Math. Soc. 51 (1985), 385–414.
[11] N. G. Tschebotaröw, *Grundzüge der Galois'schen Theorie*, translated from Russian by H. Schwerdtfeger, Noordhoff, Groningen, 1950.

Université du Littoral
Côte d'Opale
50 rue Ferdinand Buisson
F-62228 Calais Cedex, France
E-mail: Ali.Nidal@lmpa.univ-littoral.fr

Reçu le 13.9.2004
et révisé le 10.3.2005 (4846)