ACTA ARITHMETICA
XCIII.1 (2000)

Irreducibility of the iterates of a quadratic polynomial over a field

by

Mohamed Ayad (Calais) and Donald L. McQuillan (Dublin)

1. Introduction. Let K be a field of characteristic $p \geq 0$ and let $f(X)$ be a polynomial of degree at least two with coefficients in K. We set $f_1(X) = f(X)$ and define $f_{r+1}(X) = f(f_r(X))$ for all $r \geq 1$. Following R. W. K. Odoni [7], we say that f is *stable* over K if $f_r(X)$ is irreducible over K for every $r \geq 1$. In [6] the same author proved that the polynomial $f(X) = X^2 - X + 1$ is stable over $\mathbb{Q}$. He wrote in [7] that the proof given there is quite difficult and it would be of interest to have an elementary proof. In the sequel we shall use elementary methods for proving the stability of quadratic polynomials over number fields; especially the rational field, and over finite fields of characteristic $p \geq 3$.

2. Preliminary results. We recall here the classical result:

Lemma 1 (Capelli's lemma). *Let K be a field and let $u(X), v(X) \in K[X]$ be polynomials. Let α be any root of $u(X)$ in an algebraic closure of K. Then $u(v(X))$ is irreducible over K if and only if $u(X)$ is irreducible over K and $v(X) - \alpha$ is irreducible over $K(\alpha)$.*

Proof. See [9] and [2, énoncé 2.9] for two different proofs.

Let now K be a field of characteristic $p \neq 2$ and let $f(X) = X^2 - lX + m \in K[X]$. We assume that $f(X)$ is irreducible over K. In this section we give conditions under which for a given positive integer n, $f_n(X)$ is irreducible but $f_{n+1}(X)$ is reducible over K. In the algebraic closure of K choose any sequence $\beta_0, \beta_1, \ldots, \beta_n$ with $\beta_0 = 0$ and $\beta_j = f(\beta_{j+1})$ for $j = 0, \ldots, n-1$. It is evident that β_r is a root of $f_r(X)$ for $r = 1, \ldots, n$ and that, if the square root is well chosen, $\beta_{r+1} = l/2 + \sqrt{d/4 + \beta_r}$ for $r = 0, \ldots, n$, where $d = l^2 - 4m$ is the discriminant of $f(X)$.

2000 *Mathematics Subject Classification*: 11C08, 11T06, 12E05.

We define the finite increasing sequence of fields K_r, for $r = 0, \dots, n+1$, by $K_r = K(\beta_r)$. We set $d_0 = d/4$, $d_r = d_0 + \beta_r$ for all $r \geq 0$, $\delta = -d - 2l$ and $\delta_0 = \delta/4$.

Claim. *For every $r \geq 0$, we have $d_{r+1} = -\delta_0 + \sqrt{d_r}$.*

Proof. We have

$$d_{r+1} = d_0 + \beta_{r+1} = d_0 + \frac{l}{2} + \sqrt{d_r} = \frac{2d_0 + l}{2} + \sqrt{d_r}$$
$$= \frac{d/2 + l}{2} + \sqrt{d_r} = \frac{d + 2l}{4} + \sqrt{d_r} = -\delta_0 + \sqrt{d_r}.$$

The following lemma will be used to prove the first theorem of this paper.

Lemma 2. *Let K be a field of characteristic $p \neq 2$ and let d be an element of K, not a square. Let $g, h \in K$, $h \neq 0$, then the following propositions are equivalent*:

(i) *$g + h\sqrt{d}$ is a square in the field $K(\sqrt{d})$.*

(ii) *There exist elements a and ϱ in K such that $g^2 - dh^2 = \varrho^2$ and $a^2 = (g + \varrho)/2$.*

(iii) *There exists $a \in K$ such that $-dh^2 = 4a^2(a^2 - g)$.*

Proof. (i)⇒(ii). Suppose that $g+h\sqrt{d}$ is a square in $K(\sqrt{d}\,)$, $g+h\sqrt{d} = (a + b\sqrt{d}\,)^2$. Then $a^2 + db^2 = g$ and $2ab = h$. Since $h \neq 0$, we deduce that $a \neq 0$. Replacing b by $h/(2a)$, we obtain a quadratic equation in a^2: $a^4 - ga^2 + h^2 d/4 = 0$. We conclude that its discriminant is a square in K say: $g^2 - dh^2 = \varrho^2$ and $a^2 = (g + \varrho)/2$ for some $\varrho \in K$.

(ii)⇒(iii). Starting from the relations contained in (ii), we obtain $\varrho = 2a^2 - g$ and

$$-dh^2 = \varrho^2 - g^2 = (2a^2 - g)^2 - g^2 = 4a^2(a^2 - g).$$

(iii)⇒(i). Since $h \neq 0$ we deduce that $a \neq 0$ and that

$$\left(a + \frac{h}{2a}\sqrt{d}\right)^2 = \frac{4a^4 + dh^2}{4a^2} + h\sqrt{d} = g + h\sqrt{d}.$$

Note. For future reference we note the expression

$$g + h\sqrt{d} = \left(a + \frac{h}{2a}\sqrt{d}\right)^2.$$

We now define polynomials $g_r(X)$ in $K[X]$ as follows: $g_0(X) = -X$, $g_1(X) = X^2 + \delta_0$ and $g_{r+1}(X) = g_1(g_r(X))$ thus $g_{r+1}(X) = g_r^2(X) + \delta_0$, $r \geq 1$. Next we define elements g_r in K by $g_r = g_r(\delta_0)$ thus $g_0 = -\delta_0$, $g_1 = \delta_0^2 + \delta_0$ and $g_{r+1} = g_r^2 + \delta_0$, $r \geq 1$.

We can now state the following:

THEOREM 1. *Let $n \geq 1$ and let $f_n(X)$ be irreducible in $K[X]$. If $f_{n+1}(X)$ is reducible over K, then for every r, $0 \leq r \leq n-1$, there exist elements a_r and $\varrho_r \in K_{n-r-1}$ such that $g_r^2 - \varrho_r^2 = d_{n-r-1}$ and $a_r^2 = (g_r + \varrho_r)/2$. Furthermore, for every r such that $1 \leq r \leq n-1$, we have*

$$\varrho_{r-1} = \pm\left(a_r - \frac{\sqrt{d_{n-r-1}}}{2a_r}\right).$$

Conversely if there exist elements a_r and ϱ_r with these properties then $f_{n+1}(X)$ is reducible in $K[X]$.

P r o o f. Suppose that $f_n(X)$ is irreducible and $f_{n+1}(X)$ is reducible over K; then by Lemma 1 $f(X) - \beta_n$ is reducible over $K_n = K(\beta_n)$. The discriminant of $f(X) - \beta_n$ is

$$4(d_0 + \beta_n) = 4d_n = 4(-\delta_0 + \sqrt{d_{n-1}}) = 4(g_0 + \sqrt{d_{n-1}}).$$

Hence $g_0 + \sqrt{d_{n-1}}$ is a square in $K_n = K_{n-1}(\sqrt{d_{n-1}})$. Recall that $g_0 = -\delta_0 \in K \subset K_{n-1}$. By Lemma 2 there exist elements a_0 and $\varrho_0 \in K_{n-1}$ such that $g_0^2 - \varrho_0^2 = d_{n-1}$ and $a_0^2 = (g_0 + \varrho_0)/2$. Let r be an integer, $0 \leq r \leq n-2$, and suppose that there exist $a_r, \varrho_r \in K_{n-r-1}$ such that $g_r^2 - \varrho_r^2 = d_{n-r-1}$ and $a_r^2 = (g_r + \varrho_r)/2$. Then $g_r^2 - d_{n-r-1} = \varrho_r^2$ is a square in $K_{n-r-1} = K_{n-r-2}(\sqrt{d_{n-r-2}})$. Now

$$g_r^2 - d_{n-r-1} = g_r^2 + \delta_0 - \sqrt{d_{n-r-2}} = g_{r+1} - \sqrt{d_{n-r-2}}.$$

By Lemma 2 again we conclude that there exist elements $a_{r+1}, \varrho_{r+1} \in K_{n-r-2}$ such that $g_{r+1}^2 - d_{n-r-2} = \varrho_{r+1}^2$ and $a_{r+1}^2 = (g_{r+1} + \varrho_{r+1})/2$. Conversely, suppose that there exist $a_0, \varrho_0 \in K$ such that $g_0^2 - \varrho_0^2 = d_{n-1}$ and $a_0^2 = (g_0 + \varrho_0)/2$. By Lemma 2 we deduce that $g_0 + \sqrt{d_{n-1}}$ is a square in $K_n = K(\beta_n)$. Since β_{n+1} is a root of $f(X) - \beta_n$ and the discriminant of this polynomial is $4(g_0 + \sqrt{d_{n-1}})$, we conclude that $f(X) - \beta_n$ is reducible over K_n and by Capelli's lemma $f_{n+1}(X)$ is reducible over K.

REMARK 1. Suppose that $f_n(X)$ is irreducible and $f_{n+1}(X)$ is reducible over K. Then with the notations of the preceding theorem and with the aid of the claim, we have

$$\begin{aligned}\varrho_r^2 &= g_r^2 - d_{n-r-1} = g_r^2 + \delta_0 - \sqrt{d_{n-r-2}} \\ &= g_{r+1} - \sqrt{d_{n-r-2}} = \left(a_{r+1} - \frac{\sqrt{d_{n-r-2}}}{2a_{r+1}}\right)^2.\end{aligned}$$

Thus

$$\varrho_r = \pm\left(a_{r+1} - \frac{\sqrt{d_{n-r-2}}}{2a_{r+1}}\right).$$

We also have:

$$\beta_{n+1} = \frac{l}{2} + \sqrt{d_n} = \frac{l}{2} + \sqrt{-\delta_0 + \sqrt{d_{n-1}}} = \frac{l}{2} + \sqrt{g_0 + \sqrt{d_{n-1}}}$$
$$= \frac{l}{2} + \sqrt{\left(a_0 + \frac{\sqrt{d_{n-1}}}{2a_0}\right)^2} = \frac{l}{2} \pm \left(a_0 + \frac{\sqrt{d_{n-1}}}{2a_0}\right).$$

EXAMPLE 1. Let $K = \mathbb{Q}$ and $f(X) = X^2 + 10X + 17$. This polynomial appears in [7] as an example for which $f_2(X)$ is reducible. Here we have $l = -10$; $d = 32$, $d_0 = 8$, $\delta = -d - 2l = -12$, $\delta_0 = -3$, $g_0 = -\delta_0 = 3$, $g_0^2 - d_0 = 1$ so $\varrho_0 = \pm 1; a_0^2 = (g_0 + \varrho_0)/2 = (3 \pm 1)/2 = 2$ or 1, so $a_0 = \pm 1$. Thus $\beta_2 = l/2 \pm a_0 \pm \sqrt{d_0}/(2a_0) = -5 \pm 1 \pm \sqrt{2}$, that is, $\beta_2 = 4 \pm \sqrt{2}$ or $\beta_2 = -6 \pm \sqrt{2}$ and so

$$f_2(X) = (X^2 + 8X + 14)(X^2 + 12X + 34).$$

3. Stability over $\mathbb{Q}$. In this section we suppose that $K = \mathbb{Q}$ and $f(X) = X^2 - lX + m$ is an irreducible polynomial in $\mathbb{Z}[X]$. Now $d \equiv \delta \equiv 0 \pmod 4$ when l is even and $d \equiv \delta \equiv 1 \pmod 4$ when l is odd. In the even case, we have $d_0 = d/4 \in \mathbb{Z}$ and $\delta_0 = \delta/4 \in \mathbb{Z}$, thus $g_r \in \mathbb{Z}$ for every $r \geq 0$. In the odd case we have $g_0 = -\delta/4$ and $g_1 = (\delta^2 + 4\delta)/4^2$ and in general $g_r = h_r/4^{2^r}$ where $h_r \in \mathbb{Z}$ and $h_r \equiv \delta^{2^r} \equiv 1 \pmod 4$.

THEOREM 2. *If $d \equiv 1 \pmod 4$, then $f(X)$ is stable over $\mathbb{Q}$.*

Proof. Let $n \geq 1$ and suppose $f_n(X)$ is irreducible but $f_{n+1}(X)$ is reducible in $\mathbb{Q}[X]$. By Theorem 1, there exists an element $\varrho_{n-1} \in \mathbb{Q}$ such that $g_{n-1}^2 - \varrho_{n-1}^2 = d/4$. Since $g_{n-1}^2 = h_{n-1}^2/4^{2^n}$ it follows that $\varrho_{n-1} = u_{n-1}/4^{2^{n-1}}$ where u_{n-1} is an odd integer. Setting $b_r = 4^{2^r}$ we have

$$\left(\frac{h_{n-1} + u_{n-1}}{b_{n-1}}\right)\left(\frac{h_{n-1} - u_{n-1}}{b_{n-1}}\right) = \frac{d}{4}.$$

Set

$$\frac{h_{n-1} + u_{n-1}}{b_{n-1}} = \frac{a}{b} \quad \text{and} \quad \frac{h_{n-1} - u_{n-1}}{b_{n-1}} = \frac{r}{s}$$

where a and r are odd integers and both b and s are powers of 2. Thus $ar/(bs) = d/4$ and hence $ar = d$, $bs = 4$. Now adding the equations above yields

$$h_{n-1} = \frac{1}{2}\left(\frac{a}{b} + \frac{r}{s}\right)b_{n-1} = \frac{(as + br)b_{n-1}}{8};$$

when $n \geq 2$, the right side is even and we have a contradiction. If $n = 1$ then $b_{n-1} = 4$ and so $h_{n-1} = (as + br)/2$. Again this is impossible since $bs = 4$ and a and r are both odd. In all cases we are led to a contradiction, hence f is stable over $\mathbb{Q}$.

The example given above shows that Theorem 2 no longer holds when d is even; however we have:

THEOREM 3. *If* $d = 0 \pmod 4$ *but* $d \neq 0 \pmod{16}$ *then* $f(X)$ *is stable over* $\mathbb{Q}$.

Proof. Suppose $f_n(X)$ is irreducible and $f_{n+1}(X)$ is reducible in $\mathbb{Q}[X]$ for some $n \geq 1$. By Theorem 1 again, there exists an element $\varrho_{n-1} \in \mathbb{Q}$ such that $g_{n-1}^2 - \varrho_{n-1}^2 = d_0 = d/4$. Now $g_{n-1} \in \mathbb{Z}$, $d_0 \in \mathbb{Z}$ and so $\varrho_{n-1} \in \mathbb{Z}$. If $d_0 \equiv 2 \pmod 4$, we have an immediate contradiction. If d_0 is odd then $g_{n-1}+\varrho_{n-1}$ and $g_{n-1}-\varrho_{n-1}$ are both odd and hence neither $(g_{n-1}+\varrho_{n-1})/2$ nor $(g_{n-1} - \varrho_{n-1})/2$ can be a square in $\mathbb{Q}$, contradicting Theorem 1. Thus Theorem 3 is proved.

We now consider polynomials $f(X)$ with discriminant $d \equiv 0 \pmod{16}$.

THEOREM 4. *If* $d \equiv 0 \pmod{16}$ *and* $|\delta| \geq |d|$, *then* $f(X)$ *is stable over* $\mathbb{Q}$.

Proof. Suppose $f_n(X)$ is irreducible and $f_{n+1}(X)$ is reducible over $\mathbb{Q}$ for some $n \geq 1$. By Theorem 1, there is an element $\varrho_{n-1} \in \mathbb{Z}$ such that $g_{n-1}^2 - \varrho_{n-1}^2 = d_0 = d/4$. We can assume $\varrho_{n-1} > 0$. Then

$$\begin{aligned} |d_0| &= ||g_{n-1}|^2 - \varrho_{n-1}^2| = ||g_{n-1}| + \varrho_{n-1}| \cdot ||g_{n-1}| - \varrho_{n-1}| \\ &= (|g_{n-1}| + \varrho_{n-1})||g_{n-1}| - \varrho_{n-1}|. \end{aligned}$$

Thus $|d_0| > |g_{n-1}|$. We get a contradiction as follows. Suppose first that $\delta > 0$; then $|g_r| \geq \delta_0$ for all r and since $\delta_0 \geq |d_0|$ by assumption we have a contradiction. Suppose now that $\delta < 0$. Since $|d| \geq 16$ our assumption gives $|\delta_0| \geq 4$ and hence $|g_0| = |\delta_0|$, $|g_1| = \delta_0^2 + d_0 > |\delta_0|$ and in general $|g_r| \geq |\delta_0|$. Again we have a contradiction and the theorem is proved.

It remains to consider the situation when $d \equiv 0 \pmod{16}$ and $|\delta| < |d|$. This last condition is equivalent to the condition that d and l have opposite sign (recall $\delta = -d - 2l$) and $0 < |l| < |d|$. We note that since d and δ determine l and m we have:

COROLLARY. *When* $d \equiv 0 \pmod{16}$, *there are only finitely many polynomials* $f(X) = X^2 - lX + m$ *with integer coefficients of discriminant* d *such that* $f_n(X)$ *is reducible over* $\mathbb{Q}$ *for some* $n \geq 2$.

REMARK 2. We note that when $d \equiv 0 \pmod{16}$, there are always polynomials $f(X) = X^2 - lX + m$ in $\mathbb{Z}[X]$ of discriminant d such that $f_n(X)$ is reducible for some n. Indeed there are always polynomials such that $f_2(X)$ is reducible and we can determine all of these explicitly.

Suppose that $f(X) = X^2 - lX + m$ is irreducible and has discriminant $d \equiv 0 \pmod{16}$. If $f_2(X)$ is reducible, then by Theorem 1, there exist $a_0, \varrho_0 \in \mathbb{Q}$ such that $\delta_0^2 - \varrho_0^2 = \delta_0$ and $a_0^2 = (-\delta_0 + \varepsilon\varrho_0)/2$, $\varepsilon = \pm 1$. Note that ϱ_0 and $a_0 \in \mathbb{Z}$ since $\delta_0, d_0 \in \mathbb{Z}$, $-d_0 = 4a_0^2(a_0^2 + \delta_0)$ and $4 \mid \delta_0$. Since δ_0

and ϱ_0 have the same parity we can consider the integer $b_0 = (-\delta_0 - \varepsilon\varrho_0)/2$ and we see that

$$a_0^2 b_0 = d_0/4 = d/16, \quad \delta_0 = -(a_0^2 + b_0),$$
$$\varepsilon\varrho_0 = a_0^2 - b_0, \quad l = 2(-\delta_0 - d_0) = 2(a_0^2 + b_0 - 4a_0^2 b_0)$$

and of course $m = (l^2 - d)/4$.

Conversely, start with any factorization of $d/16$ of the form $d/16 = a_0^2 b_0$ for some $a_0, b_0 \in \mathbb{Z}$ with $a_0 > 0$. Define $l = 2(a_0^2 + b_0 - 4a_0^2 b_0)$, $m = (l^2 - d)/4$ and let $f(X) = X^2 - lX + m$. Then $\delta_0 = -d_0 - l/2 = -(a_0^2 + b_0)$ and

$$g_0^2 - d_0 = \delta_0^2 - d_0 = (a_0^2 + b_0)^2 - 4a_0^2 b_0 = (a_0^2 - b_0)^2 = \varrho_0^2$$

say where $\varrho_0 = a_0^2 - b_0$. Then $(g_0 + \varrho_0)/2 = (-\delta_0 + \varrho_0)/2 = a_0^2$ and so by Theorem 1, $f_2(X)$ is reducible over $\mathbb{Q}$. For instance if we take $d = 32$, then $d/16 = 2$ and the only factorization of $d/16$ of the form $a_0^2 b_0, a_0 > 0$, gives $a_0 = 1, b_0 = 2$, then $l = -10$, $m = 17$, $f(X) = X^2 + 10X + 17$ and we recover Odoni's example.

Remark 3. The same argument shows that if $d = 16e$, where e is square-free, $e \neq 1$, there is only one polynomial $f(X)$ of discriminant d such that $f_2(X)$ is reducible. Similarly when $d/16 = r^2 s$ where $r > 0$, s is square-free, $s \neq 1$. Thus the number of polynomials $f(X)$ of discriminant d such that $f_2(X)$ is reducible is just the number of divisors of r and they can all be described explicitly.

Remark 4. When considering the case $d \equiv 0 \pmod{16}$ and $|\delta| < |d|$ we note these facts:

(i) if $\delta = 0$ then $g_r = 0$ for all $r \geq 0$,

(ii) if $\delta = -8$ then $g_r = 2$ for all $r \geq 0$,

(iii) if $\delta = -4$ then $g_0 = 1$ and $g_r = 0$ when r is odd, and $g_r = -1$ when r is even and positive.

However if $\delta \neq 0, -4, -8$ then $|g_r|$ is increasing and hence given d there exists an integer N (minimal) such that $|g_{n-1}| \geq |d_0|$ when $n \geq N$. On the other hand, we have seen in the proof of Theorem 4 that if $f_n(X)$ is irreducible and $f_{n+1}(X)$ is reducible then $|d_0| > |g_{n-1}|$. Hence if $f_N(X)$ is irreducible then $f(X)$ is stable over $\mathbb{Q}$.

Finally, we consider the situation when $d \equiv 0 \pmod{16}$ and $\delta = 0, -8$. Here as noted above, g_r is constant for all $r \geq 0$. We show that if $f_2(X)$ is irreducible then $f(X)$ is stable over $\mathbb{Q}$. Indeed, suppose that for some $n \geq 2$, $f_n(X)$ is irreducible while $f_{n+1}(X)$ is reducible over $\mathbb{Q}$. Then by Theorem 1, there exist elements $a_{n-1}, \varrho_{n-1} \in \mathbb{Q}$ such that $g_{n-1}^2 - \varrho_{n-1}^2 = d_0$ and $a_{n-1}^2 = (g_{n-1} + \varrho_{n-1})/2$. Since $g_{n-1} = g_0$ we conclude by the converse part of Theorem 1 applied to the case $n = 1$ that $f_2(X)$ is reducible. This

contradiction proves what we want. We note that Remark 2 allows us to describe all $f(X)$ above for which $f_2(X)$ is reducible. The case $d \equiv 0 \pmod{16}$, $\delta = -4$ remains open.

4. Stability over finite fields. Let $\mathbb{F}_q$ be a finite field of characteristic $p \geq 3$ and let $f(X) = X^2 - lX + m$ be an irreducible polynomial over $\mathbb{F}_q$. In this section we investigate the stability of $f(X)$ over $\mathbb{F}_q$. If F is a finite field and $x \in F^*$, we denote by $\left(\frac{x}{F}\right)$ the quadratic character of x, that is, $\left(\frac{x}{F}\right) = 1$ if x is a square in F and $\left(\frac{x}{F}\right) = -1$ if not. Before stating the main result of this section we recall a result of O. Ore about a quadratic reciprocity law [4], [8].

LEMMA 3 (Ore). *Let $u(X), v(X) \in \mathbb{F}_q[X]$ be monic and irreducible polynomials over the field $\mathbb{F}_q$ of characteristic $p \geq 3$. Suppose that $u(X) \neq v(X)$ and let α (resp. β) be a root of u (resp. v) in an algebraic closure of $\mathbb{F}_q$. Then*

$$\left(\frac{u(\beta)}{\mathbb{F}_q(\beta)}\right)\left(\frac{v(\alpha)}{\mathbb{F}_q(\alpha)}\right) = (-1)^{\frac{q-1}{2}\cdot \deg u \cdot \deg v}.$$

In fact, the statement of this result given in [4] and [8] is more general.

THEOREM 5. *Let $\mathbb{F}_q$ be a finite field of characteristic $p \neq 2$ and let $f(X) = X^2 - lX + m$ be a polynomial with coefficients in $\mathbb{F}_q$ and with discriminant $d = l^2 - 4m$. Suppose that $f(X)$ is irreducible over $\mathbb{F}_q$. Then $f(X)$ is stable over $\mathbb{F}_q$ if and only if $f_n(-d/4)$ is not a square in $\mathbb{F}_q$ for every $n \geq 1$.*

Proof. Suppose that $f_n(X)$ is irreducible and $f_{n+1}(X)$ is reducible over $\mathbb{F}_q$ for some $n \geq 1$. Let β_n be a root of $f_n(X)$ in an algebraic closure of $\mathbb{F}_q$; then by Capelli's lemma $f(X) - \beta_n$ is reducible over $\mathbb{F}_q(\beta_n)$. This implies that its discriminant is a square in $\mathbb{F}_q(\beta_n)^*$, so $\beta_n + d/4$ is a square in $\mathbb{F}_q(\beta_n)^*$. Set $u(X) = X + d/4$, $v(X) = f_n(X)$ and apply the preceding lemma. We obtain

$$\left(\frac{\beta_n + d/4}{\mathbb{F}_q(\beta_n)}\right)\left(\frac{f_n(-d/4)}{\mathbb{F}_q}\right) = (-1)^{\deg f_n \cdot (q-1)/2} = (-1)^{2^{n-1}(q-1)} = 1$$

since q is odd. We conclude that $f_n(-d/4)$ is a square in $\mathbb{F}_q^*$.

Conversely, suppose that for some $n \geq 1$, $f_n(-d/4)$ is square in $\mathbb{F}_q$. If $f_n(X)$ is reducible then the conclusion follows. Suppose that $f_n(X)$ is irreducible and let β_n be a root of $f_n(X)$ in an algebraic closure of $\mathbb{F}_q$. Set $u(X) = X + d/4$, $v(X) = f_n(X)$ and again apply the preceding lemma. We have

$$\left(\frac{\beta_n + d/4}{\mathbb{F}_q(\beta_n)}\right)\left(\frac{f_n(-d/4)}{\mathbb{F}_q}\right) = (-1)^{\deg f_n \cdot (q-1)/2} = 1.$$

We deduce that $\beta_n+d/4$ is a square in $\mathbb{F}_q(\beta_n)$ and also $4\beta_n+d$ is a square. This implies that the polynomial $f(X)-\beta_n$ is reducible over $\mathbb{F}_q(\beta_n)$. By Capelli's lemma $f_{n+1}(X)$ is reducible over $\mathbb{F}_q$.

Let $q=p^e$ be a prime power where p is odd and let $f(X)=X^2-lX+m$ be an irreducible polynomial over $\mathbb{F}_q$. Let $d=l^2-4m$ be its discriminant. Since the field $\mathbb{F}_q$ is finite, the set $V=\{f_n(-d/4) : n \geq 1\}$ is also finite. Let k be the smallest integer for which there exists an index $i<k$ such that $f_k(-d/4)=f_i(-d/4)$. Then it is clear that

$$V=\{f_1(-d/4),\dots,f_{k-1}(-d/4)\}.$$

It follows that if none of the elements $f_1(-d/4),\dots,f_{k-1}(-d/4)$ is a square in $\mathbb{F}_q$, then $f(X)$ is stable over $\mathbb{F}_q$.

Example 2. We can apply the above considerations to the polynomial considered by Odoni in [6], $f(X)=X^2-X+1$ of discriminant $d=-3$. Let p be a prime number. Then $f(X)$ is irreducible over $\mathbb{F}_p$ if and only if $p\equiv 2 \pmod 3$. For instance take $p=5$, then $f_1(3/4)=-2$, $f_2(3/4)=2$, $f_3(3/4)=-2$ so $f_n(3/4)$ is never a square in $\mathbb{F}_5$, hence $f(X)$ is stable over $\mathbb{F}_5$. We conclude that $f(X)$ is also stable over $\mathbb{Q}$.

5. Stability over number fields. In this section we deal with the stability of quadratic polynomials over number fields and state a result similar to Theorem 5.

Theorem 6. *Let K be a number field, and A its ring of integers. Let $f(X)=X^2-lX+m$ be a polynomial with coefficients in A, irreducible over K and of discriminant $d=l^2-4m$. Then $f(X)$ is stable over K if and only if $f_n(-d/4)$ is never a square for every $n\geq 1$.*

Proof. Suppose that $f_n(X)$ is irreducible while $f_{n+1}(X)$ is reducible over K for some $n\geq 1$. Let β_n be a root of $f_n(X)$ in $\mathbb{C}$. Then by Capelli's lemma $f(X)-\beta_n$ is reducible over $K(\beta_n)$. This implies that its discriminant is a square in this field, so $4\beta_n+d$ is also a square in the integral closure B of A. Set $4\beta_n+d=g^2(\beta_n)$ where g is a polynomial with coefficients in K. It follows that $f_n(X)$ divides $4X+d-g^2(X)$ in $K[X]$. Let $\wp$ be any prime ideal of A lying above an odd rational prime and not containing the common denominator of the coefficients of g. Let $V(X)$ be an irreducible unitary factor of $f_n(X)$ over the finite field $A/\wp$ and let β be a root of $V(X)$. Then we have $4\beta+d=g^2(\beta)$ so $\beta+d/4$ is a square in $(A/\wp)(\beta)$.

By Lemma 3 we have

$$\left(\frac{\beta+d/4}{(A/\wp)(\beta)}\right)\left(\frac{V(-d/4)}{A/\wp}\right)=(-1)^{\deg V\cdot(p^h-1)/2}$$

where h is the residual degree of $\wp$. Hence

$$\left(\frac{V(-d/4)}{A/\wp}\right) = (-1)^{\deg V\cdot(p^h-1)/2}.$$

We deduce that

$$\left(\frac{f_n(-d/4)}{A/\wp}\right) = (-1)^{\deg f_n\cdot(p^h-1)/2} = (-1)^{2^{n-1}(p^h-1)} = 1,$$

hence $f_n(-d/4)$ is a square in $A/\wp$. Hensel's lemma ([3, Chap. 4] or [5, Chap. 3]) implies that $f_n(-d/4)$ is a square in the $\wp$-adic completion $K_\wp$ of K. Before completing the proof, we recall Grunwald's theorem [1, Chap. 9, Th. 1] (see also Chap. 10, Th.1).

THEOREM 7 (Grunwald–Wang). *Let F be a global field, $m = 2^t m'$ (m' odd) an integer, and S a finite set of primes. Let $\alpha \in F$ and assume $\alpha \in F_y^m$ for all $y \notin S$.*

(a) *If F is a function field or if F is a number field and the field $F(\zeta_{2^t})/F$ is cyclic where ζ_{2^t} is a primitive 2^t-root odd of unity (this condition is satisfied if $t \le 2$) then $\alpha \in F^m$.*

(b) *Otherwise at least $\alpha \in F^{m/2}$.*

We apply this theorem to our situation, where $F = K$ is a number field, $m = 2$, $t = 1$, $m' = 1$, $\alpha = f_n(-d/4)$, and S is the finite set containing the primes lying above 2 or containing the common denominator of the coefficients of the polynomial $g(X)$. We conclude that $f_n(-d/4)$ is a square in K.

The converse part of Theorem 6 may be proved similarly.

We have shown in Section 4 that the polynomial $f(X) = X^2 - X + 1$ is stable over $\mathbb{F}_5$, hence stable over $\mathbb{Q}$. We can get the stability over $\mathbb{Q}$ directly by using Theorem 6. To this end we will prove two simple lemmas.

LEMMA 4. *Let $f(X) = X^2 - X + 1$ and set $U_0 = 3/4$ and $U_n = f(U_{n-1}) = f_n(3/4)$ for every $n \ge 1$. Then for every $n \ge 0$, we have $3/4 \le U_n < 1$.*

Proof. We note that f is an increasing function in $[1/2, \infty[$. The proof may be completed easily by induction.

LEMMA 5. *Let a be an odd integer, $n \ge 1$ be an integer, $b = 4^{2^n}$, and $f(X) = X^2 - X + 1$. If $3/4 \le a/b < 1$, then $f(a/b) \notin \mathbb{Q}^2$.*

Proof. Suppose that $f(a/b)$ is a square in $\mathbb{Q}$. Then there exists a positive integer c such that

$$a^2 - ab + b^2 = c^2.$$

We deduce that

$$(2a - b)^2 + 3b^2 = 4c^2 \quad \text{and} \quad (2a - b + 2c)(2a - b - 2c) = -3b^2.$$

Now $2a-b+2c > 2a-b-2c$ and so we have either

(i) $$2a-b+2c = 3\cdot 2^s \quad \text{and} \quad 2a-b-2c = -2^t$$

or

(ii) $$2a-b+2c = 2^s \quad \text{and} \quad 2a-b-2c = -3\cdot 2^t$$

where $2^{s+t} = b^2 = 2^{2^{n+2}}$. Adding we get either

(iii) $$4a-2b = 3\cdot 2^s - 2^t$$

or

(iv) $$4a-2b = 2^s - 3\cdot 2^t.$$

Since $3/4 \le a/b$ we get $4a-3b \ge 0$ and $4a-2b > 0$. We conclude that in either case t is the smallest of s and t, and indeed $t=2$ since a is odd. Thus $2^s = 2^{2^{n+2}-2}$, $2^t = 4$. Divide by $4b$ and get either

(v) $$\frac{a}{b} = \frac{1}{2} - \frac{1}{b} + \frac{3\cdot 2^{s-2}}{b} > \frac{2^{s-2}}{b}$$

or

(vi) $$\frac{a}{b} = \frac{1}{2} - \frac{3}{b} + \frac{2^{s-2}}{b} > \frac{2^{s-2}}{b}.$$

Now $2^{s-2}/b = 2^{2^{n+2}-4-2^{n+1}} = 2^{2^{n+1}-4} \ge 1$, and we deduce that $a/b > 1$, which contradicts our assumption.

It is now easy to get the stability over $\mathbb{Q}$ of the polynomial $f(X) = X^2 - X + 1$.

Proposition. *Let $f(X) = X^2 - X + 1$. Then $f(X)$ is stable over $\mathbb{Q}$.*

Proof. This polynomial is irreducible over $\mathbb{Q}$ and its discriminant is equal to -3. Set $U_0 = 3/4$ and $U_n = f(U_{n-1}) = f_n(3/3)$ for $n \ge 1$. Then by Lemma 4, we have $3/4 \le U_n < 1$. We can write U_n in the form $U_n = a_n/4^{2^n}$ for every $n \ge 0$, where $a_n \in \mathbb{Z}$ is odd. Lemma 5 implies that for every $n \ge 1$, $U_n \notin \mathbb{Q}^2$. We conclude by Theorem 6 that $f(X)$ is stable over $\mathbb{Q}$.

References

[1] E. Artin and J. Tate, *Class Field Theory*, Benjamin, New York, 1968.

[2] M. Ayad, *Théorie de Galois, 122 exercices corrigés, niveau I*, Ellipses, Paris, 1997.

[3] Z. I. Borevitch et I. R. Chafarevitch, *Théorie des nombres*, Gauthier-Villars, Paris, 1967.

[4] Y. Hellegouarch, *Loi de réciprocité, critère de primalité dans $\mathbb{F}_q[t]$*, C. R. Math. Rep. Acad. Sci. Canada 8 (1986), 291–296.

[5] P. J. McCarthy, *Algebraic Extensions of Fields*, Blaisdell, Waltham, 1966.

[6] R. W. K. Odoni, *On the prime divisors of the sequence* $w_{n+1} = 1 + w_1 \dots w_n$, J. London Math. Soc. 32 (1985), 1–11.

[7] —, *The Galois theory of iterates and composites of polynomials*, Proc. London Math. Soc. 51 (1985), 385–414.

[8] O. Ore, *Contributions to the theory of finite fields*, Trans. Amer. Math. Soc. 36 (1934), 243–274.

[9] N. G. Tschebotarör, *Grundzüge der Galois'schen theorie* (translated from Russian by H. Schwerdtfeger), Noordhoff, Groningen, 1950.

Université du Littoral Cote d'Opale
50, Rue Ferdinand Buisson, BP699
62228 Calais Cedex, France
E-mail: ayad@lma.univ-littoral.fr

Department of Mathematics
University College Dublin
Belfield 4, Dublin, Ireland
E-mail: don.mcquillan@ucd.ie

Received on 11.6.1999
and in revised form on 9.9.1999 (3625)