ROCKY MOUNTAIN
JOURNAL OF MATHEMATICS
Volume 40, Number 5, 2010

# ON IRREDUCIBLE POLYNOMIALS OVER Q WHICH ARE REDUCIBLE OVER $\mathbf{F}_p$ FOR ALL $p$

MOHAMED AYAD

ABSTRACT. Examples of polynomials having the property of being irreducible over $\mathbf{Q}$ but reducible over $\mathbf{F}_p$ for all primes $p$ are constructed. If some conditions of linear disjointness are satisfied by two number fields, then any integer generating the compositum of these fields satisfies this property. We study the question of whether the above property is preserved for a given polynomial under translations. It is shown, in particular, that the polynomial $x^n - nax^{n-1} - b$ satisfies the above property, for any even integer $n \geq 4$, any integer $a \neq 0$ and all but finitely $b$ of the form $b = (-1)^{n/2}c^2 - a^n(n-1)^{n-1}$, where $c$ is a positive integer.

**1. Introduction.** Let $f(x)$ be a monic polynomial with integral coefficients. In order to prove that this polynomial is irreducible over $\mathbf{Q}$, one may try to find a prime $p$ such that $f(x)$ is irreducible modulo $p$. But some authors, the first one being Hilbert, have shown that such a prime may as well not exist. Lee [**13**] has shown that if $a$ is a square-free rational integer neither equal to 1 nor to $-1$, then the polynomial

$$f(x) = x^4 + 2(1-a)x^2 + (1+a)^2$$

is irreducible over $\mathbf{Q}$ but reducible modulo $p$ for every prime $p$.

**Definition 1.** A given monic polynomial with integral coefficients has the property $(P)$ if it is irreducible over $\mathbf{Q}$ but reducible over $\mathbf{F}_p$ for every prime $p$.

Golomb [**8**, Theorem 2] proved that the cyclotomic polynomial $\phi_n(x)$ satisfies $(P)$ if and only if $n \neq 1, 2, p^k, 2p^k$ where $p$ is an odd prime and $k$ is a positive integer. Indeed, Lee's and Golomb's examples are

*Keywords and phrases.* Irreducible polynomial, inert prime, Hilbert's irreducibility theorem, linearly disjoint extensions, linear relations connecting roots of polynomials.
Received by the editors on March 17, 2008, and in revised form on April 2, 2008.
DOI:10.1216/RMJ-2010-40-5-1377 

instances of irreducible polynomials over $\mathbf{Z}$ whose Galois groups are abelian but noncyclic, and we will explain in Section 2 why in this case property $(P)$ is satisfied. Brandl [**4**] has shown that, for any positive integer $n > 1$, not prime, there exists a monic polynomial of degree $n$ satisfying $(P)$. This result was proved again by Guralnick et al. [**9**, Theorem 2]. These authors considered in [**9**] the similar problem of finding irreducible polynomials over $\mathbf{Z}$ but reducible over $\mathbf{Q}_p$ for all primes $p$.

In Section 2, we state some conditions which are equivalent to $(P)$. Some of them appear explicitly or implicitly in [**4**] or in [**9**]. Here we prove that the minimal polynomial of any algebraic integer generating the compositum of two number fields, linearly disjoint over $\mathbf{Q}$, and of noncoprime degrees, satisfies $(P)$. The same conclusion holds if we replace "noncoprime degrees" by coprime degrees but such that one of the number fields is not linearly disjoint from the Galoisian closure of the second one. We also show that if the roots of an irreducible polynomial are related by a linear relation of noncyclotomial type then this polynomial satisfies $(P)$, see Definition 3.

In Section 3, we consider the question of whether property $(P)$ is preserved under translations. It turns out that if $h(x) = x^n - nax^{n-1}$ where $a$ is a nonzero integer and $n$ is an even integer $\geq 4$, then for all but finitely many $b \in \mathbf{Z}$ of the form $b = (-1)^{n/2}c^2 - a^n(n-1)^{n-1}$, $h(x) - b$ satisfies $(P)$. Furthermore, we show that there exist infinitely many numbers fields of degree $n$, generated by trinomials $x^n - nax^{n-1} - b$ which satisfy $(P)$. There exist as well infinitely many $b \in \mathbf{Z}$ such that $h(x) - b$ is irreducible over $\mathbf{Z}$ but does not satisfy $(P)$.

**2. New examples.** Before stating properties equivalent to $(P)$ we make the following definition.

**Definition 2.** Let $K$ be a number field, and let $f(x)$ be a monic polynomial with integral coefficients, irreducible over $\mathbf{Q}$. We say that $f$ generates $K$, and we write $K = \mathbf{Q}_f$ if $K = \mathbf{Q}(\alpha)$ for some root $\alpha$ of $f(x)$.

**Proposition 1.** *Let $K$ be a number field of degree $n$, and let $f$ be such that $K = \mathbf{Q}_f$. Then the following conditions are equivalent*:

(i) *No rational prime is inert in* $K$.

(ii) *Any polynomial* $g$ *such that* $K = \mathbf{Q}_g$ *satisfies* $(P)$.

(iii) $f$ *satisfies* $(P)$.

(iv) $\mathrm{Gal}\,(f(x), \mathbf{Q})$ *contains no cycle of length* $n$.

(v) *For all but finitely many* $p$, $f(x)$ *is reducible over* $\mathbf{Q}_p$.

*Proof.* (i) $\Rightarrow$ (ii). Let $p$ be any prime number. Let $g(x)$ be a polynomial such that $K = \mathbf{Q}_g$, and let $\mu$ be a root of $g(x)$ in $K$. If $p$ does not divide the index of $\mu$, then by [**15**, Chapter 3, Theorem 27], $g(x)$ is reducible modulo $p$. If $p$ divides the index of $\mu$, then $p$ divides the discriminant of $g(x)$, so $g(x)$ is reducible modulo $p$ in this case also.

(ii) $\Rightarrow$ (iii). Clear.

(iii) $\Rightarrow$ (iv). See [**20**, Chapter 8.10].

(iv) $\Rightarrow$ (i). Suppose that there exists some rational prime inert in $K$. Let $N$ be the normal closure of $K$ over $\mathbf{Q}$, and let $G$ be the Galois group of $N/\mathbf{Q}$. Let$P$ be a prime ideal of $N$ lying over $p$, and let $\phi = \phi(P/p)$ be the Frobenius automorphism. Let $H = \mathrm{Gal}\,(N/K)$. Since $p$ is inert and since the action of $\phi$ on the set of the roots of $f$ is similar to the action of $\phi$ on the set of the right cosets of the elements of $G$ modulo $H$, then $\phi$ acts as an $n$-cycle and $G$ contains an $n$-cycle.

(i) $\Leftrightarrow$ (v). Let $\Omega$ be the set of rational primes $p$ such that $(p) = P^e$, where $P$ is a prime ideal in $K$ and $e$ is an integer $\geq 2$. It is known that if the decomposition of a rational prime $p$ has the form $(p) = P_1^{e_1} \cdots P_r^{e_r}$ then the factorization of $f(x)$ in the $p$-adic field $\mathbf{Q}_p$ is given by $f(x) = f_1(x) \cdots f_r(x)$, where the polynomials $f_1(x), \ldots, f_r(x)$ are irreducible over $\mathbf{Q}_p$ and $\deg f_i = e_i \deg P_i$. Hence, the equivalence follows if one excludes the finite set $\Omega$.

**Proposition 2.** *Let* $f(x)$ *be a monic polynomial irreducible over* $\mathbf{Q}$, $\theta$ *be a root of* $f$ *and* $G$ *be its Galois group. Suppose that* $K(\theta)$ *is the splitting field of* $f$ *(this happens for example when* $G$ *is abelian). Then* $f$ *satisfies* $P$ *if and only if* $G$ *is noncyclic.*

*Proof.* The proof follows easily from (iv) of Proposition 1. □

*Remark.* Let $K$ and $L$ be number fields such that $K \subset L$, and let $f(x)$ and $g(x)$ be polynomials such that $K = \mathbf{Q}_f$ and $L = \mathbf{Q}_g$. By (i) of Proposition 1, if $f$ satisfies $(P)$, then $g$ satisfies $(P)$.

Suppose that the Galois group of the irreducible polynomial $f(x)$ of degree $n$ is the alternating group and that $n$ is even. Then by Proposition 1 (iv), $f(x)$ satisfies $(P)$. One can find parametric polynomials whose Galois group is $A_n$ in [**14**, page 74] or [**19**, page 44].

**Theorem 1.** *Let $f(x)$ and $g(x)$ be two monic polynomials with integral coefficients. Let $\theta$, $m$ ($\phi$, $n$) be the root and degree of $f(x)$ and $g(x)$, respectively. Suppose that $f(x)$ and $g(x)$ are irreducible over $\mathbf{Q}$ and that the fields $\mathbf{Q}(\theta)$ and $\mathbf{Q}(\phi)$ are linearly disjoint over $\mathbf{Q}$. Suppose furthermore that one of the following conditions holds*:

(i) $\gcd(m, n) > 1$.

(ii) $\gcd(m, n) = 1$ *and the splitting field of $g(x)$ is not linearly disjoint from $\mathbf{Q}(\theta)$ over $\mathbf{Q}$.*

*Let $\gamma$ be an algebraic integer which is a primitive element of $\mathbf{Q}(\theta, \phi)$, and let $h(x)$ be its minimal polynomial over $\mathbf{Q}$. Then $h(x)$ satisfies the property $(P)$.*

*Proof.* Write $\gamma$ in the form

$$\gamma = \gamma'/d = u(\theta, \phi)/d,$$

where $\gamma'$ is an algebraic integer, $d$ is a rational integer and $u(x, y)$ is a polynomial with integral coefficients. By Proposition 1 (ii), we may replace $\gamma$ by $\gamma'$ and thus suppose $d = 1$. Fix a prime $p$ and denote as usual by $\overline{u}(x)$ the reduced polynomial of $u(x)$ modulo $p$. Let $\Theta_1, \ldots, \Theta_m$, respectively $\Phi_1, \ldots, \Phi_n$, be the roots of $\overline{f}(x)$, respectively $\overline{g}(x)$ in an algebraic closure of $\mathbf{F}_p$, and let $d = \gcd(m, n)$. Suppose first that we are in the case (i). Set $\gamma_1 = \overline{u}(\Theta_1, \Phi_1)$. Since $\gamma_1$ is a root of $\overline{h}(x)$, the minimal polynomial of $\gamma_1$ over $\mathbf{F}_p$ divides $\overline{h}(x)$. Since $\Theta_1 \in \mathbf{F}_{p^{m_1}}$ and $\Phi_1 \in \mathbf{F}_{p^{n_1}}$, where $1 \leq m_1 \leq m$ and $1 \leq n_1 \leq n$, we deduce that $\gamma_1 \in \mathbf{F}_{p^{m_1}} \cdot \mathbf{F}_{p^{n_1}} = \mathbf{F}_{p^k}$ where $k = \operatorname{lcm}(m_1, n_1)$. If $m_1 < m$ or $n_1 < n$, then $k \leq m_1 n_1 < mn$. If $m_1 = m$ and $n_1 = n$, then $k = \operatorname{lcm}(m, n) = mn/d < mn$. In all cases we have $k < mn$; hence, the minimal polynomial of $\gamma_1$ over $\mathbf{F}_p$ is of degree smaller than $mn$. This implies that $\overline{h}(x)$ is reducible over $\mathbf{F}_p$.

Suppose now that we are in the case (ii). We have $[\mathbf{F}_p(\Phi_1) : \mathbf{F}_p] \leq n$. Let $E$ be the splitting field of $g(x)$ over $\mathbf{Q}$, and let $f_1(x)$ be the minimal polynomial of $\theta$ over $E$. Then $\deg f_1 < m$. Reducing modulo $p$, and writing each $\Phi_i$ as a polynomial in $\Phi_1$ with coefficients in $\mathbf{F}_p$ shows that $[\mathbf{F}_p(\Phi_1, \Theta_1) : \mathbf{F}_p(\Phi_1)] < m$; hence, $\overline{h}(x)$ is reducible over $\mathbf{F}_p$.

**Example 1.** Let $f(x) = x^3 - 2$ and $g(x) = x^2 + x + 1$. Then these polynomials satisfy the conditions of Theorem 1, case (ii).

**Example 2.** Let $f(x) = x^2 - 2$, $g(x) = x^3 - x + 1$ and $\alpha$ be a root of $f$, let $\beta$ be a root of $g$ and let $\gamma = \alpha\beta$. Then $\gamma$ is a root of $h(x) = x^6 - 4x^4 + 4x^2 - 8$, but $h(x)$ does not satisfy $(P)$, since it is irreducible modulo 3. Here the splitting field of $g(x)$ is linearly disjoint from the field generated by a root of $f(x)$. The same assertion is true if we permute $f(x)$ and $g(x)$.

It is easy to find examples satisfying case (i) of Theorem 1 (see Corollary 2 hereafter).

From Theorem 1 we deduce the following corollaries. The second one produces examples similar to those of Lee.

**Corollary 1.** *Consider the polynomial*

$$h(x) = \mathrm{Res}_y(f(y), g(x - y)),$$

*where the polynomials $f(x)$ and $g(x)$ fulfill the conditions of Theorem 1 and $\mathrm{Res}_y$ denotes the resultant with respect to $y$. Then $h(x)$ satisfies property $(P)$.*

For the proof of Corollary 1 we need the following result of Isaacs [**11**].

**Lemma 1.** *Let $F$ be a field of characteristic 0, and let $F(\gamma)$ and $F(\beta)$ be algebraic separable extensions of $F$ of degrees $n$ and $m$, respectively, such that $[F(\gamma, \beta) : F] = mn$. Then $\gamma + \beta$ is a primitive element of $F(\gamma, \beta)$.*

*Proof.* See [**11**]. The author in [**11**] assumes that $(m,n)=1$ but he uses only the fact that $[F(\beta,\gamma):F]=mn$. He also proved this result for fields of characteristic $p>0$ under some conditions. One can also consult [**5, 6**]. □

*Proof of Corollary* 1. Let $\alpha_1,\ldots,\alpha_m$, respectively $\beta_1,\ldots,\beta_n$, be the roots of $f(x)$, respectively $g(x)$, and let $\gamma=\alpha_1+\beta_1$. By Lemma 1, $\gamma$ is a primitive element of $\mathbf{Q}(\alpha_1,\beta_1)$. Let $h(x)$ be the minimal polynomial of $\gamma$. Then by Theorem 1 this polynomial satisfies property $(P)$. We can express this polynomial via the resultant as follows:

$$h(x)=\prod_{i=1}^{m}\prod_{j=1}^{n}(x-\alpha_i-\beta_j)=\prod_{i=1}^{m}g(x-\alpha_i)=\mathrm{Res}_y(f(y),g(x-y).$$

**Corollary 2.** *Let $a$ and $b$ be distinct square-free rational integers, not equal to* 1. *Then the polynomial*

$$h(x)=x^4-2(a+b)x^2+(a-b)^2$$

*satisfies property $(P)$.*

*Proof of Corollary* 2. Apply Corollary 1 to $f(x)=x^2-a$ and $g(x)=x^2-b$. If one puts $b=-1$ one recovers Lee's examples. Setting $a+b=-a'$ and $a-b=b'$, one finds Hilbert's examples mentioned in [**9**]. □

**Definition 3.** Let $f(x)$ be a monic irreducible polynomial with rational coefficients and let $\alpha_1,\ldots,\alpha_n$ be its roots. These roots are said to be linearly related if there exist coefficients $a_1,\ldots,a_n\in\mathbf{Z}$, not all zero such that $a_1\alpha_1+\cdots+a_n\alpha_n=0$. The linear relation is said to be of cyclotomial type if the polynomial $p(x)=a_1+a_2x+\cdots+a_nx^{n-1}$ is not coprime with $x^n-1$.

**Example.** Let $K/\mathbf{Q}$ be a cyclic extension of degree $n$, and let $\alpha$ be a primitive element of $K$. It can be shown that $\alpha$ generates no normal basis of $K/\mathbf{Q}$ if and only if there exists a linear relation between the conjugates of $\alpha$ of cyclotomial type [**2**, 'enoncé 7. 2].

**Proposition 3.** *Let $f(x)$ be a monic irreducible polynomial with rational coefficients of degree $n$, and suppose that its roots satisfy a linear relation of non-cyclotomial type. Then $f$ satisfies $(P)$.*

*Proof.* Suppose the contrary. Then the Galois group of $f$ contains a cycle $\sigma$ of length $n$. Suppose that the roots $\alpha_1, \dots, \alpha_n$ are labeled such that $\sigma = (\alpha_1, \dots, \alpha_n)$. Suppose that the roots of $f$ satisfy the linear relation: $a_1\alpha_1 + \cdots + a_n\alpha_n = 0$, where $a_1, \dots, a_n$ are integers not all zero. Applying successively $\sigma, \dots, \sigma^{n-1}$ to this relation we get the following system of homogeneous linear equations:

$$\begin{aligned} a_1\alpha_1 + a_2\alpha_2 + \cdots + a_n\alpha_n &= 0 \\ a_n\alpha_1 + a_1\alpha_2 + \cdots + a_{n-1}\alpha_n &= 0 \\ \cdots\cdots\cdots\cdots\cdots\cdots\cdots\cdots & \\ a_2\alpha_1 + a_3\alpha_2 + \cdots + a_1\alpha_n &= 0. \end{aligned}$$

The determinant of this system is known as a circulant determinant. Its value is given by $\Delta = P(\xi_1)\dots P(\xi_n)$, where $P(x) = a_1 + a_2x + \cdots + a_nx^{n-1}$ and $\xi_1, \dots, \xi_n$ are the roots of $x^n - 1$. Since this system has a non trivial solution, then $P(x)$ has a common root with $x^n - 1$ and the linear relation is of cyclotomial type contradicting our hypothesis.

The converse of this proposition is false. One can see this by taking an algebraic integer with zero trace whose minimal polynomial satisfies $(P)$. Here is a "less trivial" example. Let $f(x) = x^4 - 2x^2 + 9$ whose roots are $\alpha_1 = i + \sqrt{2}$, $\alpha_2 = -\alpha_1$, $\alpha_3 = i - \sqrt{2}$ and $\alpha_4 = -\alpha_3$. Then, by Corollary 2, $f(x)$ satisfies $(P)$ and the relation $\alpha_2 + \alpha_1 = 0$ is linear of cyclotomial type.

**3. Perturbing the constant term of a polynomial.** Letting $f(x)$ be a monic polynomial with integral coefficients, we look at the values of $t^\star \in \mathbf{Z}$ such that $f(x) - t^\star$ satisfies or does not satisfy the property $(P)$. We will need the following:

**Lemma 2.** *Let $n \geq 4$ be an even integer. Let $a \in \mathbf{Z} \setminus \{0\}$ and $\varepsilon \in \{-1, 1\}$ be fixed. Then the Diophantine equation:*

$$\varepsilon x^2 - a^n(n-1)^{n-1} = y^n - nay^{n-1}$$

*has at most a finite number of integer solutions $(x, y)$.*

*Proof.* The Diophantine equation may be written in the form:

$$x^2 = \varepsilon\big(y^n - nay^{n-1} + a^n(n-1)^{n-1}\big).$$

Suppose first that $n > 4$. Simple calculations of $P'(y)$ and $P''(y)$ show that $P(y)$ has only one multiple root. Namely, $y = (n-1)a$ is a double root of $P(y)$. So $P(y)$ has at least 3 distinct roots if $n > 4$. By a well-known result of Siegel the equation has a finite number of integer solutions [**17**, Theorem 3, Chapter 28]. Suppose now that $n = 4$. The Diophantine equation takes the form:

$$x^2 = \varepsilon\big(y^4 - 4ay^3 + 27a^4\big) = \varepsilon(y-3a)^2\big((y+a)^2 + 2a^2\big).$$

Since the conclusion of Lemma 2 is evident if $\varepsilon = -1$, we suppose now that $\varepsilon = 1$. This equation implies that $(y+a)^2 + 2a^2 = z^2$ is a square, hence $(z-y-a)(z+y+a) = 2a^2$. We deduce that $z - y - a = d_1$ and $z + y + a = d_2$, where $d_1$, $d_2$ are divisors of $2a^2$ and $d_1 d_2 = 2a^2$. We conclude that $y = (d_1 + d_2)/2 - a$ and that the Diophantine equation has a finite number of solutions in the case $n = 4$. □

**Lemma 3.** *Let $m$ and $n$ be positive integers, relatively prime such that $n \geq m + 1$ and let $f(x) = x^n + ax^m + b$, where $a, b \in \mathbf{C}$, $a \neq 0$. Then $f(x)$ is (functionally) indecomposable over $\mathbf{C}$.*

*Proof.* See [**1**, Theorem 2] or [**18**, Lemma 1, Chapter 3] for a more general result. □

**Lemma 4.** *Let $h(x)$ be a nonconstant polynomial with rational coefficients of degree not equal to 5. Suppose that $h(x)$ is (functionally) indecomposable. Let*

$$R = \{t \in \mathbf{Z},\ \ h(x) - t \text{ is reducible over } \mathbf{Q}\}.$$

*Then $R = h(\mathbf{Z}) \cup A$, where $A$ is a finite set.*

*Proof.* See [**7**]. □

**Theorem 2.** *Let $f(x)$ be a monic polynomial with integer coefficients. Then there exist infinitely many $t^\star \in \mathbf{Z}$ such that $f(x) - t^\star$ is irreducible over $\mathbf{Q}$ and does not satisfy $(P)$.*

*Let $h(x) = x^n - nax^{n-1}$, where $a$ is a nonzero integer and $n \geq 4$ is an even rational integer. Then, for all but finitely many $t^\star \in \mathbf{Z}$ of the form $t^\star = (-1)^{n/2}c^2 - a^n(n-1)^{n-1}$, where $c$ is a positive integer, the polynomial $h(x) - t^\star$ is irreducible over $\mathbf{Q}$ and satisfies $(P)$.*

*Proof.* Let $F(t,x) = f(x) - t$, and let $\theta$ be a root of $F$ in $\overline{\mathbf{Q}(t)}$. Let $\gamma$ be a primitive element for the splitting field $\Sigma$ of $F(t,x)$ over $\mathbf{Q}(t)$, and let $\widehat{F}(t,x)$ be its minimal polynomial over $\mathbf{Q}(t)$. Let $\gamma_1, \ldots, \gamma_N$ be the conjugates of $\gamma$ over $\mathbf{Q}(t)$. Set $\theta = P(t,\gamma)/S(t)$ and $\gamma_i = P_i(t,\gamma)/S_i(t)$ for $i = 2, \ldots, N$, where $P$ and $P_i \in \mathbf{Z}[t,x]$ and $S$, $S_i \in \mathbf{Z}[t]$. Consider the set $A$ of rational integers $t^\star$ such that $\widehat{F}(t^\star, x)$ is irreducible over $\mathbf{Q}$, $S(t^\star) \neq 0$ and $S_i(t^\star) \neq 0$. By Hilbert's irreducibility theorem, the set $A$ is infinite and $\mathrm{Gal}\,(F(t^\star,x),\mathbf{Q}) \backsimeq \mathrm{Gal}\,(F(t,x),\mathbf{Q}(t))$. It is known that this last group contains an $n$-cycle [**18**, Lemma 6, Chapter 1.5]. Moreover, since $S(t^\star) \neq 0$, then $f(x) - t^\star$ is irreducible over $\mathbf{Q}$. The conclusion relative to the property $(P)$ follows from Proposition 1 (iv).

To prove the second part of the theorem, we first compute the discriminant $D(H(t))$ of the polynomial $H(t,x) = h(x) - t$ as a polynomial in $x$. We have:

$$\begin{aligned}\mathrm{Res}_x\left(\frac{\partial H}{\partial x}, H\right) &= n^n(-t)^{n-2}\big[\big((n-1)a\big)^n - na\big((n-1)a\big)^{n-1} - t\big] \\ &= (-1)^{n-1}n^n t^{n-2}\big[a^n(n-1)^{n-1} + t\big].\end{aligned}$$

It follows that

$$\begin{aligned}D(h)(t) &= (-1)^{n/2}n^n t^{n-2}\big[a^n(n-1)^{n-1} + t\big] \\ &= \varepsilon n^n t^{n-2}\big[a^n(n-1)^{n-1} + t\big],\end{aligned}$$

where $\varepsilon = (-1)^{n/2}$. Let

$$B = \{t^\star \in \mathbf{Z} \setminus \{0\},\ t^\star = \varepsilon c^2 - a^n(n-1)^{n-1} \text{ for some integer } c\}.$$

Then $D(H(t^\star)) = n^n t^{\star n-2}c^2$. We deduce that $D(H(t^\star))$ is a nonzero square and so $\mathrm{Gal}\,(H(t^\star,x),\mathbf{Q})$ is contained in the alternating group for any $t^\star \in B$. We show that, for all but finitely many $t^\star \in B$, $H(t^\star,x)$ is irreducible over $\mathbf{Q}$. Let $C$ be the set of rational integers $t^\star$ such that $H(t^\star,x)$ is reducible over $\mathbf{Q}$. By Lemma 3, $h$ is not the composition of

two polynomials of degree $\geq 2$. Since $\deg h \neq 5$, we can apply Lemma 4 and then get $C = C_1 \cup h(\mathbf{Z})$, where $C_1$ is a finite set. By Lemma 2, $B \cap h(\mathbf{Z})$ is finite. Hence, $B \setminus C$ is infinite and the conclusion of the theorem follows by Proposition 1 (iv). □

Consider the set $\Lambda$ of $(a,b) \in \mathbf{Z}^2$ such that the polynomial $f_{(a,b)}(x) = x^n - nax^{n-1} - b$ satisfies $(P)$. For any $(a,b) \in \Lambda$, let $K_{(a,b)}$ be the field generated by some root of $f_{(a,b)}$. From Theorem 2, $\Lambda$ is infinite, but it is not clear whether the family of number fields $(K_{(a,b)})_{(a,b)\in\Lambda}$ contains infinitely many distinct fields.

**Conjecture.** *Let $F$ be a field (of characteristic 0?), and let $f_1(x)$ and $f_2(x)$ be monic and irreducible polynomials over $F$ of the form:*

$$f_1(x) = x^n - a_1x^{n-1} - b_1 \text{ and } f_2(x) = x^n - a_2x^{n-1} - b_2,$$

*where $n \geq 5$. Then there exists a root $\theta_1$ of $f_1$, respectively $\theta_2$ of $f_2$, such that $F(\theta_1) = F(\theta_2)$ if and only if $\theta_2 = \lambda\theta_1$ for some $\lambda \in F$.*

It seems that this conjecture is true (see [**3**] for some contribution toward this conjecture). Although this conjecture is not proved, it is however possible to get the following:

**Corollary 3.** *For any even integer $n \geq 4$, there exist infinitely many number fields of degree $n$ generated by trinomials $f_{(a,b)}(x) = x^n - nax^{n-1} - b$ which satisfy $(P)$.*

For the proof of this result, we will use the following auxiliary lemmas.

**Lemma 5.** *Let $n$ be an even positive integer. Set $d = (-1)^{n/2}(n-1)^{n-1}$. Let*

$$Y = \{p \in \mathbf{Z},\ p \text{ odd prime, such that } d \text{ is a square in } \mathbf{F}_p \text{ and } p \nmid n-1\}.$$

*Then $Y$ is infinite.*

*Proof.* Note that $d$ is not a square. Consider the rational primes $p$ which decompose in the quadratic field $\mathbf{Q}(\sqrt{d})$. □

**Lemma 6.** *Let $p$ be a prime number, $K$ a number field, $\theta$ an algebraic integer of $K$, primitive over $\mathbf{Q}$, and let $f(x)$ be its minimal polynomial. Suppose that*

$$f(x) \equiv f_1(x)^{e_1} \cdots f_r(x)^{e_r} \pmod{p},$$

*where $f_1, \ldots, f_r$ are monic polynomials with integer coefficients irreducible over $\mathbf{F}_p$. Write $f(x)$ in the form:*

$$f(x) = f_1(x)^{e_1} \cdots f_r(x)^{e_r} + pg(x),$$

*where $g(x)$ is an integer polynomial. Then $p$ divides the index of $\theta$ if and only if $f_i(x) \mid g(x)$ for some $i \in \{1, \ldots, r\}$ with $e_i \geq 2$.*

*Proof.* [**10**, art. 95, pages 172–175].

*Proof of Corollary* 3. We keep the notations introduced in Lemma 5 above of $d$ and $Y$. We show that the family of number fields $(K_{(a,b)})_{(a,b)\in\Lambda}$ contains infinitely many which are distinct.

*Step* 1. We show that for any $p \in Y$ there exists an $(a, b) \in \Lambda$ such that $p \mid b$ and $p^2 \nmid b$.

Let $p \in Y$ (hence $p$ is odd). Let $\zeta$ be a primitive root of unity modulo $p^2$. Since $d$ is a square modulo $p$, it is a square modulo $p^2$, hence $d \equiv \zeta^k \pmod{p^2}$ with $k$ even. Let $a_p$ and $c_p$ be integers such that $a_p \equiv \zeta^j$, $c_p \equiv \zeta^i \pmod{p^2}$, where $j$, $i$ are integers, $j$ arbitrary and $i = k/2 + jn/2 + (p-1)/2$. Set $b_p = (-1)^{n/2}(c_p^2 - da_p^n)$. It is easy to verify that $b_p \equiv 0 \pmod{p}$, but $b_p \not\equiv 0 \pmod{p^2}$.

*Step* 2. Apply Lemma 4. Let $f_{(a_p,b_p)}(x) = x^n - na_p x^{n-1} - b_p$, and let $\theta_p$ be a root of $f_{(a_p,b_p)}$. Write $f_{(a_p,b_p)}$ in the form $f_{(a_p,b_p)}(x) = x^{n-1}(x - na_p) - p(b_p/p)$. We see by Lemma 6 that $p$ does not divide the index of $\theta_p$. On the other hand, the discriminant of $\theta_p$ is given by $D(\theta_p) = n^n b_p^{n-2} c_p^2$ (see the proof of Theorem 2). It follows that there are infinitely many primes, each of them ramified in some number field belonging to the family $(K_{(a,b)})_{(a,b)\in\Lambda}$, and the proof of Corollary 3 is complete. □

*Remarks.* Notice that in the examples of polynomials $f(x)$ satisfying $(P)$, constructed in [**4, 8, 9, 13**], $\mathrm{Gal}\,(f(x), \mathbf{Q})$ contains no element of degree $n$, hence no $n$-cycle. This appears directly from the examples or from their proofs. For our examples, we have proved that the Galois group of $h(x) - t^\star$ is contained in the alternating group operating on a set of $n$ elements. It is clear that, if $n$ is a power of 2, then the alternating group, hence also the Galois group, contains no element of order $n$. If $n$ is even and at least equal to 10, but not a power of 2, set $n = m2^e$. Choose in the alternating group a permutation which is a product of 3 disjoint cycles of respective orders: $m$, $2^e$ and 2, then this permutation has order $n$. But it is not clear whether or not our Galois group contains an element of order $n$. It might be interesting to construct examples of polynomials with property $(P)$ having odd degree or having Galois groups containing elements of order $n$ but no $n$-cycle.

If one has in mind to prove that some polynomial $f(x)$ is irreducible over $\mathbf{Q}$, and if $f$ is reducible modulo all primes $p$, one may try to use the criteria proposed in [**16**, Chapter 1, Theorem 1.8.1].

**Acknowledgments.** The author is indebted to the referee for suggesting some corrections.

## REFERENCES

**1.** M. Ayad, *Critical points, critical values of a prime polynomial*, Complex Variable Elliptic Equations **51** (2006), 143–160.

**2.** ———, *Théorie de Galois*, 122 *exercices corrigés, niveau* I, Ellipses, Paris, 1997.

**3.** M. Ayad and F. Luca, *Fields generated by roots of* $x^n + ax + b$, submitted, 2007.

**4.** R. Brandl, *Integer polynomials that are reducible modulo all primes*, Amer. Math. Monthly **93** (1986), 286–288.

**5.** J. Browkin, B. Diviš and A. Schinzel, *Addition of sequences in general fields*, Monat. Math. **82** (1976), 261–268.

**6.** B. Diviš, *On the degrees of the sum and product of two algebraic elements*, in *Number theory and algebra*: *Collected papers*, H. Zassenhaus, ed., Academic Press, New York, 1977.

**7.** M. Fried, *On Hilbert's irreducibility theorem*, J. Number Theory **6** (1974), 211–231.

**8.** S.W. Golomb, *Cyclotomic polynomials and factorization theorems*, Amer. Math. Monthly **85** (1978), 734–737.

**9.** R. Guralnick, M. Schacher and J. Sonn, *Irreducible polynomials which are locally reducible everywhere*, Proc. Amer. Math. Soc. **133** (2005), 3171–3177.

**10.** H. Hancock, *Foundations of the theory of algebraic numbers*, Vol. 2, Mac Millan, New York, 1964.

**11.** J.M. Isaacs, *Degrees of sums in a separable field extension*, Proc. Amer. Math. Soc. **25** (1970), 638–641.

**12.** G.J. Janusz, *Algebraic number fields*, Graduate Stud. Math., Amer. Math. Soc., 1996.

**13.** M.A. Lee, *Some irreducible polynomials which are reducible* mod$p$ *for all* $p$, Amer. Math. Monthly **76** (1969), 1125.

**14.** G. Malle and B.H. Matzat, *Inverse Galois theory*, Springer-Verlag, New York, 1999.

**15.** D.A. Marcus, *Number fields*, Springer-Verlag, New York, 1977.

**16.** M. Mignotte and D. Stefanescu, *Polynomials: An algorithmic approach*, Springer, New York, 1999.

**17.** J. Mordell, *Diophantine equations*, Pure Appl. Math. **30**, Academic Press, 1969.

**18.** A. Schinzel, *Polynomials with special regards to reducibility*, Cambridge Univ. Press, Cambridge, 2001.

**19.** J-P. Serre, *Topics in Galois theory*, Jones and Barlett Publishers, Boston, 1992.

**20.** B.L. Van der Warden, *Algebra*, Vol. 1, Springer-Verlag, New York, 1966.

Université du Littoral Côte d'Opale, 50 rue F. Buisson, F-62228 Calais Cedex, France
**Email address: ayad@lmpa.univ-littoral.fr**