ISRAEL JOURNAL OF MATHEMATICS **169** (2009), 109–123
DOI: 10.1007/s11856-009-0006-0

ELEMENTARY CRITERIA FOR IRREDUCIBILITY OF $f(X^r)$

BY

NATALIO H. GUERSENZVAIG

Universidad CAECE, Av. Corrientes 3985 6A (1194)
Buenos Aires, Argentina
e-mail: nguersenz@fibertel.com.ar

ABSTRACT

In this paper, very simple sufficient conditions for the irreducibility of $f(X^r)$ over an arbitrary unique factorization domain Z are established.

1. Introduction

We fix throughout this work a unique factorization domain Z with field of fractions Q. The group of units of Z will be denoted by U.

Let $f(X)$ be any polynomial in $Z[X]$ of positive degree that is irreducible in $Z[X]$. Using the well-known Eisenstein's criterion we can easily show that, in some cases, $f(X^r)$ will also be irreducible in $Z[X]$ for any positive integer r. However, this is not true in general. For example, $f(X) = X^3 - X^2 - 2X - 1$ is irreducible in $Z[X]$ for $Z \in \{\mathbb{Z}, \mathbb{Z}_2, \mathbb{Z}_5\}$, while $f(X^2) = (X^3 - X^2 - 1)(X^3 + X^2 + 1)$.

In the main result of this work we will establish sufficient conditions for irreducibility of $f(X^r)$ in $Z[X]$ for any integer $r > 1$ that, besides U, depend only on r, the degree of $f(X)$ and the leading and constant coefficients of $f(X)$. (These conditions can be easily checked if Z is an effective unique factorization domain.) Elementary necessary and sufficient conditions will also be given. (The adjective "elementary" refers to the fact that these conditions will be stated without using proper algebraic extensions of Q.) The cases $f(X) = X - a$

Received March 30, 2007 and in revised form June 13, 2007

and $f(X) = aX^2 + bX + c$ are considered in [1, pp. 63–74]. Related results for polynomials over finite fields can be found in [7, pp. 93–95].

Henceforth we will use, for $S \subseteq Q$ and $t \in \mathbb{N}$, the following notation:

$$S^* = S \setminus \{0\}, \quad S^t = \{s^t : s \in S\}, \quad tS = \{ts : s \in S\}.$$

Our main result is the following theorem. (It will be proved, together with an equivalent dual version, in the last section of this paper.)

THEOREM 1.1: *Let r be any integer, $r > 1$, and let $f(X)$ be an arbitrary polynomial in $Z[X]$ of positive degree m, leading coefficient a and nonzero constant term b that is irreducible in $Z[X]$. Assume that the following condition is satisfied:*

CONDITION: *C(m, a, b, r). For each prime p dividing r and any unit u in U at least one of the two following conditions holds:*

(A) $ua \notin Z^p$;

(B) (i) $(-1)^m ub \notin Z^p$ *and* (ii) $ub \notin Z^2$, *if* $4|r$.

Then

$$f(X^r) \text{ is irreducible in } Z[X].$$

Remark: (I) It is well-known that for any $r \in \mathbb{N}$ the polynomials $f(X^r) = \sum_{j=0}^{m} a_j X^{rj}$ $(a = a_m,\ b = a_0)$ and $\tilde{f}(X^r) = \sum_{j=0}^{m} a_j X^{r(m-j)}$ are both irreducible, or both reducible in $Z[X]$. However, we cannot expand Theorem 1.1 using this fact, because both C(m, a, b, r) and C(m, b, a, r) are logically equivalent to the following symmetrical (with respect to a and b) condition:

CONDITION: *C'(m, a, b, r). For each prime p dividing r and any unit u in U the two following conditions are satisfied:*

(A′) (i) $ua \notin Z^p$ *or* (ii) $(-1)^m ub \notin Z^p$;

(B′) *(B′) [(i)* $ua \notin Z^2$ *or (ii)* $ub \notin Z^2$*], if* $4|r$.

(II) For any integer t, any two of the three following statements implies the third:

$$ua \in Z^t, \quad \pm ub \in Z^t, \quad \pm b/a \in Q^t.$$

Therefore we can replace condition (B) of $C(m, a, b, r)$ by the following one (this is obvious if condition (A) holds):

(B′) (i) $(-1)^m \frac{b}{a} \notin Q^p$ and (ii) $\frac{b}{a} \notin Q^2$, if $4|r$.

2. Basic facts

In this section we review some elementary facts which we will use later without specific reference.

First, we remind the reader that the characteristic of Z, say $\chi(Z)$, is the only nonnegative integer that satisfies the following two conditions:

$$\text{(a) } \chi(Z)\cdot 1 = 0; \quad \text{(b) if } k \in \mathbb{Z} \text{ and } k\cdot 1 = 0, \text{ then } \chi(Z)|k.$$

The following basic fact is needed to prove Corollary 4.6 below.

- either $\chi(Z) = 0$, or $\chi(Z) = p$ is a prime number in which case we have $(x_1 + \cdots + x_n)^p = x_1^p + \cdots + x_n^p$ for all $n \in \mathbb{N}$ and any $x_1, \ldots, x_n \in Z$.

We also recall that a nonzero polynomial $f(X) \in Z[X] \setminus U$ is called *reducible in* $Z[X]$ if there exist nonzero polynomials $g(X)$, $h(X)$ in $Z[X] \setminus U$ such that $f(X) = g(X)h(X)$. Otherwise $f(X)$ is called **irreducible in** $Z[X]$. The **content** of $f(X)$, say $c(f)$, is the greatest common divisor of their coefficients (modulo units of Z), and $f(X)$ is called **primitive** if $c(f) = 1$. Replacing Z by Q in this definition yields (since in this case $U = Q^*$) that $f(X)$ is irreducible in $Q[X]$ if and only if $f(X)$ has positive degree and there are no polynomials $g(X)$, $h(X)$ in $Q[X]$ of positive degree such that $f(X) = g(X)h(X)$.

The following result is also well-known the following result (see, for example, [6, pp. 80–84]):

- if $f(X) \in Z[X]$ has positive degree, then, $f(X)$ is irreducible in $Z[X]$ if and only if $f(X)$ is primitive (in $Z[X]$) and irreducible in $Q[X]$.

As a consequence, when $f(X) \in Z[X]$ has positive degree and it is irreducible in $Z[X]$ we can replace $Z[X]$ by $Q[X]$ without risk in any of the expressions, "$f(X^r)$ is reducible in $Z[X]$", "$f(X^r)$ is irreducible in $Z[X]$". To simplify, in these situations we will write "$f(X^r)$ is reducible" or "$f(X^r)$ is irreducible", respectively. For the same reason, except where the contrary is explicitly stated, the terms "primitive" and "prime" will be understood to apply to the sets $Z[X]$ and $\mathbb{N}$, respectively.

We will use matrices and determinants as well. $M_m(Q)$, $|A|$ and $\Delta_A(X)$ will respectively denote the ring of square matrices of order m with coefficients in Q, the determinant of $A \in M_m(Q)$ and the characteristic polynomial of A. In particular, we will consider a well-known type of matrices associated to polynomials.

Let $f(X)$ be an arbitrary polynomial in $Q[X]$ of positive degree m, say $f(X) = \sum_{j=0}^{m} a_j X^j$, and let $f^*(X)$ denote the monic polynomial associate to $f(X)$, that is, $f^*(X) = \sum_{j=0}^{m} c_j X^j$, where $c_j = a_j/a_m$ for j = 0, 1, ..., m. The **companion matrix** of $f^*(X)$, say C_{f^*}, is the matrix in $M_m(Q)$ defined by

$$C_{f^*} = \begin{bmatrix} 0 & 1 & \dots & 0 & 0 \\ 0 & 0 & \dots & 0 & 0 \\ \vdots & \vdots & \ddots & \vdots & \vdots \\ 0 & 0 & \dots & 0 & 1 \\ -c_0 & -c_1 & \dots & -c_{m-2} & -c_{m-1} \end{bmatrix}.$$

We will freely use the following properties of C_{f^*}:

- $f^*(X)$ is both the minimum polynomial of C_{f^*} over Q and the characteristic polynomial of C_{f^*} (so $f(X) = a_m|XI_m - C_{f^*}|$).
- If $f(X)$ is irreducible, then the ring $Q[C_{f^*}] = \{h(C_{f^*}) : h(X) \in Q[X]\}$ is an extension field of Q of degree m with $f(C_{f^*}) = a_m f^*(C_{f^*}) = O$. (In this situation, as usual, we will write $Q(C_{f^*})$ instead of $Q[C_{f^*}]$.)

3. Preliminary results

Our irreducibility criteria strongly depend on two beautiful theorems of A. Capelli (which are included in the author's Ph.D. Thesis, Melbourne University, 1955; see [1, pp. 63–64] and [2, Vol. 2, p. 212]). The first one gives non-elementary, necessary and sufficient conditions for irreducibility of $f(g(X))$ in $Q[X]$.

Capelli's Theorem 1: *Let $f(X)$, $g(X)$ be arbitrary polynomials of $Q[X]$ of positive degree. Let F be any splitting field of $f(X)$ over Q, and let α be any root of $f(X)$ in F. Then $f(g(X))$ is irreducible in $Q[X]$ if and only if $f(X)$ is irreducible in $Q[X]$ and $g(X) - \alpha$ is irreducible in $Q(\alpha)[X]$.*

The second establishes simple conditions for reducibility of $X^n - a$ in $Q[X]$.

Capelli's Theorem 2: *Let a be any nonzero element of Q, and let n be any integer greater than 1. Then $X^n - a$ is reducible in $Q[X]$ if and only if either* (i) *$a = c^t$ for some $c \in Q$ and $t|n$ with $t > 1$, or* (ii) *$4|n$ and $a = -4c^4$ for some $c \in Q$.*

4. Necessary and sufficient conditions

In order to prove the main theorem of this section we first establish a result involving primitive polynomials which is interesting in its own right.

LEMMA 4.1: *Suppose that* $P(X) = \sum_{k=0}^{m} a_k X^k$ *is a primitive polynomial of* $Z[X]$ *of degree* m *with* $a_0 \neq 0$. *Let* $L(X)$ *be any monic polynomial in* $Z[X]$ *of positive degree* n *and nonzero roots* $\lambda_1, \ldots, \lambda_n$ *in some extension field of* Q *(counting multiplicities). In addition, suppose that the constant coefficient of* $L(X)$, *say* c_0, *is relatively prime to* a_0. *Then*

$$\prod_{j=1}^{n} P(\lambda_j X) \text{ is a primitive polynomial of } Z[X].$$

Proof. Since $L(X)$ is a monic polynomial of $Z[X]$, from the well-known Fundamental Theorem on Symmetric Polynomials it follows that $\prod_{j=1}^{n} P(\lambda_j X)$ is a polynomial in $Z[X]$, say

$$P^*(X) = \sum_{j=0}^{mn} a_j^* X^j.$$

Looking for a contradiction suppose $c(P^*) \neq 1$. Let q be any prime of Z that divides $c(P^*)$. As $c(P^*)$ divides $a_0^* = a_0^n$, so $q | a_0$ and $q \not| c_0$. Thus, since $P(X)$ is primitive, there is a positive integer k, $k \leq m$, such that $q | a_j$ for $0 \leq j < k$ and $q \not| a_k$. Realizing the product $\prod_{j=1}^{n} P(\lambda_j X)$ we get

$$a_{nk}^* = a_k^n \lambda_1^k \cdots \lambda_n^k + \sum_{\substack{i_1 + \cdots + i_n = nk \\ i_j \geq 0,\, j=1,\ldots,n \\ (i_1,\ldots,i_n) \neq (k,\ldots,k)}} a_{i_1} \cdots a_{i_n} \lambda_1^{i_1} \cdots \lambda_n^{i_n}.$$

Notice that in each summand $a_{i_1} \cdots a_{i_n} \lambda_1^{i_1} \cdots \lambda_n^{i_n}$ we have $i_j < k$ for at least one j, which makes each such summand a multiple of q. But a_{nk}^* is also a multiple of q. This contradicts the fact that $a_k^n \lambda_1^k \cdots \lambda_n^k = (-1)^{nk} c_0^k a_k^n$ is not divisible by q. ∎

In addition we will use the following result, which is an immediate consequence of two well-known identities (see, for example, [3, (3.1.1)–(3.1.4), pp. 66–68] and [5, (22)–(25), pp. 1, 83–84]).

LEMMA 4.2: *Let* F *be an arbitrary field and let* n *be any positive integer. Let* $\Psi(Y) = Y^n - 1$ *and let* w *denote an arbitrary generator of the cyclic group*

constituted by the zeros of $\Psi(Y)$ *in some extension field of* F. *Let* $g(Y) = \sum_{j=0}^{n} c_j Y^j \in F(Y)$. *We have,*

$$\prod_{j=0}^{n-1} g(w^j) = |g(C_\Psi)| = \begin{vmatrix} c_0 & c_1 & \dots & c_{n-2} & c_{n-1} \\ c_{n-1} & c_0 & \dots & c_{n-3} & c_{n-2} \\ \vdots & \vdots & \ddots & \vdots & \vdots \\ c_1 & c_2 & \dots & c_{n-1} & c_0 \end{vmatrix}.$$

Now, the following theorem can be proved.

THEOREM 4.3: *Let* r *be any integer,* $r > 1$, *and let* $f(X)$ *be any irreducible polynomial in* $Z[X]$ *of positive degree* m *and leading coefficient* a. *The two following statements are equivalent.*

(a) $f(X^r)$ *is reducible.*

(b) *There exist a prime* p *that divides* r, *a unit* u *in* U *and polynomials* $S_0(X)$, $S_1(X)$, …, $S_{p-1}(X)$ *in* $Z[X]$ *such that either*

$$(-1)^{m(p-1)} u f(X^p) = \begin{vmatrix} S_0(X^p) & XS_1(X^p) & \dots & X^{p-1}S_{p-1}(X^p) \\ X^{p-1}S_{p-1}(X^p) & S_0(X^p) & \dots & X^{p-2}S_{p-2}(X^p) \\ \vdots & \vdots & \ddots & \vdots \\ XS_1(X^p) & X^2S_2(X^p) & \dots & S_0(X^p) \end{vmatrix}, \tag{1}$$

or else

$$4|r \text{ and } u f(X^4) = \begin{vmatrix} S_0(X^2) & XS_1(X^2) \\ XS_1(X^2) & S_0(X^2) \end{vmatrix}. \tag{2}$$

Proof. Assume (a). When $f(0) = 0$, since $f(X)$ is irreducible, we have $f(X) = aX$ with $a \in U$, so (1) follows with any prime p that divides r, $u = a^{-1}$, $S_1(X) = 1$ and $S_j(X) = 0$ for $j = 0, \dots, p-1$, $j \neq 1$. Therefore, we may also assume $f(0) \neq 0$.

Let $\alpha = C_{f^*}$. From Capelli's Theorem 1 it follows that $X^r - \alpha$ is reducible in $Q(\alpha)[X]$. We first assume that (i) holds. Therefore we have $\alpha = \gamma^t$, for some $\gamma \in Q(\alpha)$ and $t|r$, $t > 1$.

Let p be any prime that divides t. Then we can write $\alpha = \beta^p$, where $\beta = \gamma^{t/p} \in Q(\alpha)$. Hence, $X^p - \alpha$ is reducible in $Q(\alpha)[X]$, so $f(X^p)$ is reducible by Capelli's Theorem 1.

Let $\Psi(X) = X^p - 1$ and let w denote an arbitrary generator of the cyclic group constituted by the zeros of $\Psi(X)$ in some extension field of $Q(\alpha)$. Then

$\Psi(X) = \prod_{j=0}^{p-1}(X - w^j)$, and, therefore,

$$X^p - \alpha = X^p - \beta^p = \beta^p \Psi(\beta^{-1}X) = \prod_{j=0}^{p-1}(X - w^j\beta) = w^{\frac{p(p-1)}{2}} \prod_{j=0}^{p-1}(w^{-j}X - \beta)$$

$$= (-1)^{p-1} \prod_{j=0}^{p-1}(w^j X - \beta).$$

Consequently, taking determinants on both sides, we obtain

$$f(X^p) = (-1)^{m(p-1)} a \prod_{j=0}^{p-1} \Delta_\beta(w^j X), \tag{3}$$

where $\Delta_\beta(X) = |XI_m - \beta|$, the characteristic polynomial of β, is a monic polynomial in $Q[X]$ of degree m. From unique factorization in Z it follows that there exists $d \in Z$ such that $P(X) = d\Delta_\beta(X)$ belongs to $Z[X]$ and is primitive. Since $P(X)$ has leading coefficient d, letting $u = d^p/a$, we can rewrite (3) as follows:

$$(-1)^{m(p-1)} u f(X^p) = \prod_{j=0}^{p-1} P(w^j X). \tag{4}$$

The right hand side is a primitive polynomial of $Z[X]$, by Lemma 4.1. Hence, since $f(X^p)$ is also primitive (because $f(X)$ is), $u \in U$.

On the other hand, assuming $P(X) = \sum_{k=0}^{m} a_k X^k$ and expressing each index k in the form $k = ip + j$ with $0 \le j < p$, we can write $a_k X^k = a_{ip+j} X^{ip} X^j$ for $k = 0, \ldots, m$. As a result, grouping the monomials associated to each X^j with $0 \le j < p$, we obtain the polynomials

$$S_j(X) = \sum_{i \ge 0} a_{ip+j} X^i \in Z[X], \quad j = 0, 1, \ldots, p-1,$$

which satisfy

$$P(X) = \sum_{j=0}^{p-1} X^j S_j(X^p). \tag{5}$$

Hence, since C_Ψ^p is the identity matrix of order p, we get

$$P(XC_\Psi) = \sum_{j=0}^{p-1} X^j S_j(X^p) C_\Psi^j. \tag{6}$$

Thus (1) follows from the case $n = p$, $F = Q(X)$, $g(Y) = P(XY)$ of Lemma 4.2.

Now assume that condition (ii) of Capelli's Theorem 2 holds. Then we have $4|r$ and $\alpha = -4\gamma^4$ for some $\gamma \in Q(\alpha)$. We may assume $f(X^2)$ is irreducible; otherwise, the first case applies.

From the identity

$$X^4 + 4\gamma^4 = (X^2 - 2\gamma X + 2\gamma^2)(X^2 + 2\gamma X + 2\gamma^2)$$

it follows

$$f(X^4) = a|X^4 I_m - \alpha| = a|X^2 I_m - 2\gamma X + 2\gamma^2||X^2 I_m + 2\gamma X + 2\gamma^2|.$$

Hence, $f(X^4)$ is reducible in $Q[X]$. Consequently, condition (i) of Capelli's Theorem 2 is satisfied with $n = 2$ and $g(X) = f(X^2)$ instead of $f(X)$. By the first case for $g(X)$ there exist a unit u in U and $S_0(X)$, $S_1(X)$ in $Z[X]$ satisfying (1) with $p = 2$. Since this is the same as (2) (note that the degree of $g(X)$ is $2m$), we have completed the proof of (b).

Assume (b). Let $P(X) = \sum_{j=0}^{p-1} X^j S_j(X^p)$. Adding all other rows to the first row of the determinant of (1) we get the row $[P(X) \dots P(X)]$. Hence we can replace the determinants of (1) and (2) (with $p = 2$ in this case) by $P(X)P^*(X)$, where

$$P^*(X) = \begin{vmatrix} 1 & 1 & \dots & 1 \\ X^{p-1}S_{p-1}(X^p) & S_0(X^p) & \dots & X^{p-2}S_{p-2}(X^p) \\ \vdots & \vdots & \ddots & \vdots \\ XS_1(X^p) & X^2S_2(X^p) & \dots & S_0(X^p) \end{vmatrix}. \tag{7}$$

Therefore, since $P^*(X) = P(-X)$ for $p = 2$, (a) follows from

$$uf(X^r) = \begin{cases} \left\{ \begin{array}{ll} P(X^{r/p})P^*(X^{r/p}) & \text{if } p \text{ is odd,} \\ (-1)^m P(X^{r/2})P(-X^{r/2}) & \text{if } p = 2, \end{array} \right\} & \text{if (1) holds} \\ P(X^{r/4})P(-X^{r/4}) & \text{otherwise.} \end{cases} \tag{8}$$

This completes the proof of the theorem. ∎

Our next theorem provides complementary information about the unit u and the polynomials $P(X)$, $P^*(X)$ considered in Theorem 4.3.

THEOREM 4.4: *Let r and $f(X)$ be as in Theorem 4.3 and assume that condition* (b) *of this theorem holds. Let $P(X) = \sum_{j=0}^{p-1} X^j S_j(X^p)$ and let α, w, $P^*(X)$ be as defined above.*

(I) *$u = d^p/a$, where d denotes the leading coefficient of $P(X)$.*

(II) *$P(X)$ is irreducible.*

(III) *$P^*(X)$ is irreducible if and only if $\Phi(X) = \sum_{j=0}^{p-1} X^j$ is irreducible and $Q(w) \cap Q(\alpha) = Q$.*

Proof. With $\Psi(X)$ as defined in Theorem 4.3 we obtain from Lemma 4.2,

$$P(X)P^*(X) = |P(XC_\Psi)| = \prod_{j=0}^{p-1} P(w^j X).$$

Hence, for $i \in \{1, 2\}$, if case (i) holds we get (note that $p = 2$ if $i = 2$)

$$(-1)^{im(p-1)} u f(X^{ip}) = \prod_{j=0}^{p-1} P(w^j X).$$

Now, since $\prod_{j=0}^{p-1} w^j = (-1)^{p-1}$ and $f(X^i)$ has degree im, we get (I) by comparing the leading coefficients of both sides of this equality.

In order to prove (II) we suppose that $P(X)$ is reducible. Therefore, since $P(X)$ has degree im, $P(X)$ has a root, say γ, in some extension field of Q of degree $< im$ over Q. Then $f(X^i)$ has also a root in $Q(\gamma)$, namely γ^p, contradicting the fact that $f(X^i)$ is irreducible.

Finally we prove (III). This is clear if $p = 2$, since $P^*(X) = P(-X)$ and $P(X)$ is irreducible; so we can assume p odd. We can also suppose that $\Phi(X)$ is irreducible (see [7, pp. 62–63]), because for any factorization $\Phi(X) = \Phi_1(X)\Phi_2(X)$ in $Z[X]$, from $\Phi(X) = \prod_{j=1}^{p-1}(X - w^j)$ and Lemma 4.2 it follows $P^*(X) = |P(XC_\Phi)| = |P(XC_{\Phi_1})||P(XC_{\Phi_2})|$.

Let $\delta = w\beta$, where β is defined as in Theorem 4.3. Then, since $P(\beta) = 0$, $P^*(\delta) = \prod_{j=2}^{p} P(w^j\beta) = 0$. Hence, $P^*(X)$ is irreducible if and only if the minimum polynomial of δ over Q has degree $m(p-1)$.

On the other hand, we have $\delta \in Q(w, \beta) \subseteq Q(w, \alpha)$. Furthermore, since $\delta^p = \beta^p = \alpha$, $\alpha \in Q(\delta)$ and $Q(\alpha) = Q(\beta)$. Hence, $w = \beta^{-1}\delta \in Q(\delta)$. This proves $Q(\delta) = Q(w, \alpha)$, and therefore that the minimum polynomial of δ over Q has degree

$$[Q(\delta) : Q] = [Q(w, \alpha) : Q(w)][Q(w) : Q] = [Q(w, \alpha) : Q(w)](p - 1).$$

From the well-known theorem of natural irrationalities (see, for example, [8, p. 55]) we get $[Q(w, \alpha) : Q(w)] = [Q(\alpha) : Q(w) \cap Q(\alpha)]$, and hence

$$[Q(\delta) : Q] = [Q(\alpha) : Q(w) \cap Q(\alpha)](p - 1).$$

Now (III) follows immediately from $[Q(\alpha) : Q] = m$. ∎

Remark: In particular, $P^*(X)$ is irreducible if $\Phi(X)$ is irreducible and

$$\gcd(m, p-1) = 1.$$

It should be noticed that in the course of the proof of Theorem 4.3 we have also proved, incidentally, the following result.

COROLLARY 4.5: *Let $f(X)$ be any irreducible polynomial in $Z[X]$ of positive degree. Let r be any integer, $r > 1$, and let $\sigma(r)$ be the square-free part of r. The three following statements are equivalent.*

(a) *$f(X^r)$ is reducible;*
(b) *either $f(X^{\sigma(r)})$ is reducible, or else $4|r$ and $f(X^4)$ is reducible;*
(c) *there exists a positive divisor of r, say t, with t prime or $t = 4$, such that $f(X^t)$ is reducible.*

In particular, for any positive integer s, we have:

(i) *$f(X^{2^s})$ is reducible if and only if either $f(X^2)$ is reducible, or else $s \geq 2$ and $f(X^4)$ is reducible;*
(ii) *if p is an odd prime, then*

$$f(X^{p^s}) \text{ is reducible if and only if } f(X^p) \text{ is reducible.}$$

For example, since X^p can be replaced by X in both sides of (1), we have:

(i) $f(X^{2^s})$ is reducible if and only if there exist $S_0(X)$, $S_1(X)$ in $Z[X]$ and $u \in U$ with $ua \in Z^2$ such that either

$$(-1)^m u f(X) = S_0^2(X) - X S_1^2(X),$$

or else

$$s \geq 2 \text{ and } uf(X^2) = S_0^2(X) - X S_1^2(X).$$

(ii) $f(X^{3^s})$ is reducible if and only if there exist $S_0(X)$, $S_1(X)$, $S_2(X)$ in $Z[X]$ and $u \in U$ with $ua \in Z^3$ such that

$$uf(X) = S_0^3(X) + X S_1^3(X) + X^2 S_2^3(X) - 3X S_0(X) S_1(X) S_2(X).$$

On the other hand, from (II) of Theorem 4.4 it easily follows that (4) yields a factorization of $f(X^p)$ in $Z[X]$ into p irreducible factors if and only if $w \in Z$. From the case $w = 1$, by using (i) and (ii) of Corollary 4.5 and the fact that

$$uf(X^2) \in Z^2[X] \text{ if and only if } uf(X) \in Z^2[X],$$

the following result can also be easily derived.

COROLLARY 4.6: *Assume $\chi(Z) = p$ is a prime number. Let $f(X)$ be any irreducible polynomial in $Z[X]$ of positive degree and let s be any positive integer.*

(a) *$f(X^p)$ is reducible if and only if there exist $u \in U$ and $P(X) \in Z[X]$, $P(X)$ irreducible, such that*

$$uf(X^p) = P^p(X);$$

(b) *$f(X^{p^s})$ is reducible if and only if there exists $u \in U$ such that*

$$uf(X) \in Z^p[X].$$

5. Sufficient conditions

First, we use Theorem 4.3 to prove Theorem 1.1.

Proof. The conclusion follows, because, otherwise, the assumption that $f(X^r)$ is reducible leads to a contradiction. Indeed, in such case, from Theorem 4.3 it follows that there exist a prime p that divides r, a unit u in U with $ua \in Z^p$, and $S_0(X), \ldots, S_{p-1}(X), P(X), P^*(X)$ in $Z[X]$ satisfying (5), (7) and (8). Therefore, since for p odd we have $ub \in Z^p$ if and only if $(-1)^m ub \in Z^p$, putting $X = 0$ in both sides of (8) we contradict (B) (i) if (1) holds (since $ub = (S_0(0))^p$), and (B) (ii) otherwise. Thus, since we have contradicted $\mathrm{C}(m, a, b, r)$, the proof is complete. ∎

At this point it should be noted that Theorem 1.1 essentially establishes that for a given positive integer r, if an arbitrary triple $(m, a, b) \in \mathbb{N} \times \mathbb{Z}^* \times \mathbb{Z}^*$ satisfies $\mathrm{C}(m, a, b, r)$, then, for any $f(X) = aX^m + \cdots + b \in Z[X]$,

$$f(X^r) \text{ is irreducible if and only if } f(X) \text{ is irreducible.}$$

It is also of interest to determine, for a given irreducible polynomial $f(X) = aX^m + \cdots + b \in Z[X]$ of positive degree m, an appropriate set of positive integers, say $\mathbb{N}(m, a, b)$, such that $f(X^r)$ is irreducible for each $r \in \mathbb{N}(m, a, b)$.

To illustrate the case that $f(X^r)$ is irreducible for all $r \in \mathbb{N}$ we consider Schur's polynomials, which are defined for each positive integer m by

$$f_m(X) = 1 + a_1 \frac{X}{1!} + a_2 \frac{X^2}{2!} + \cdots + a_{m-1} \frac{X^{m-1}}{(m-1)!} \pm \frac{X^m}{m!} \quad \text{for each } a_i \in \mathbb{Z}.$$

It is well-known that all these polynomials are irreducible in $\mathbb{Q}[X]$ (see [4, pp. 373–374]). Clearly

$$m!f_m(X) = \pm X^m + ma_{m-1}X^{m-1} + \cdots + \frac{m!a_2}{2!}X^2 + \frac{m!a_1}{1!}X + m!$$

is a primitive polynomial of $\mathbb{Z}[X]$, so it is irreducible. Assume $m \geq 2$. In some cases (for example, when m is prime) we get that $m!f_m(X^r)$ is irreducible for any $r \in \mathbb{N}$ from Eisenstein's Criterion, but, in general, this does not happen (consider, for example, $m = 2^n > 3$ and $a_{m-1} = 1$). In any case we have $\pm m! \notin \mathbb{Z}^p$ for each prime p, because the largest prime not exceeding m has such a property. Then, since condition (B) of $\mathrm{C}(m, a, b, r)$ is always satisfied, $\mathrm{m}!f_m(X^r)$ is irreducible (that is, $f_m(X^r)$ is irreducible in $\mathbb{Q}[X]$) for any positive integer r.

In order to include the precedent example in a more general result we assume that a, b are arbitrary nonzero elements of Z. First, we define the (a, b)-admissible primes. We shall say that a prime number p is (a, b)**-admissible** if there is no unit u in U such that both ua, ub are in Z^p. Otherwise we shall say that p is (a, b)**-inadmissible**.

There is a simple procedure to determine the (a, b)-inadmissible primes. First, we define the exponent of (a, b), say $e(a, b)$. Assume that a has the factorization $a = u_a p_1^{\alpha_1} \cdots p_s^{\alpha_s}$ in Z, where $u_a \in U$ and (in the case $a \notin U$) $p_1, \ldots, p_s$ are non-associate primes of Z with positive exponents $\alpha_1, \ldots, \alpha_s$. Let $e(a) = 0$ if $a = u_a$, and $e(a) = \gcd(\alpha_1, \ldots, \alpha_s)$, otherwise. Assume a similar factorization for b, and let $e(a, b) = 0$ if $e(a) = e(b) = 0$ and $e(a, b) = \gcd(e(a), e(b))$, otherwise. Then we can establish the following.

LEMMA 5.1: *Let a, b be nonzero elements of Z and let p be a prime number. Then*

$$p \text{ is } (a, b)\text{-inadmissible if and only if } p | e(a, b) \text{ and } u_a \equiv u_b \pmod{U^p}.$$

Proof. To begin we express a and b in the form

$$a = u_a a_0^{e(a)}, \quad b = u_b b_0^{e(b)},$$

where each one of a_0, b_0 is either equal 1, or a product of non-associate prime-powers of Z.

Assume $p|e(a,b)$ and $u_a^{-1}u_b \in U^p$, say $u_a^{-1}u_b = u_0^p$. Letting $e = e(a,b)$ we can write

$$a = u_a\alpha^e, \quad b = u_b\beta^e,$$

where $\alpha = a_0^{e(a)/e}$, $\beta = b_0^{e(b)/e}$. Hence,

$$u_a^{e-1}a = (u_a\alpha)^e, \quad u_a^{e-1}b = (u_a^{-1}u_b)(u_a\beta)^e.$$

Thus p is (a,b)-inadmissible, because

$$u_a^{e-1}a = ((u_a\alpha)^{e/p})^p \quad \text{and} \quad u_a^{e-1}b = (u_0(u_a\beta)^{e/p})^p.$$

Now assume that p is (a,b)-inadmissible. Therefore, there exist $u \in U$ and α, $\beta \in Z$ such that $ua = \alpha^p$, $ub = \beta^p$. Proceeding as previously with a and b, we can write $\alpha = u_\alpha\alpha_0^{e(\alpha)}$, $\beta = u_\beta\beta_0^{e(\beta)}$, whence

$$uu_a a_0^{e(a)} = u_\alpha^p\alpha_0^{pe(\alpha)}, \quad uu_b b_0^{e(b)} = u_\beta^p\beta_0^{pe(\beta)}.$$

Hence, from the unique factorization property of Z, it follows $pe(\alpha) = e(a)$, $pe(\beta) = e(b)$ and both uu_a, $uu_b \in U^p$. Thus, $p|e(a,b)$ and $u_a^{-1}u_b \in U^p$. ∎

Next we define the (a,b)-admissible odd integers. For convenience we agree that 1 is (a,b)-admissible. Let $\mathbb{N}_o$ denote the set of odd positive integers. We shall say that $r \in \mathbb{N}_o$ is (a,b)-admissible if each of their prime divisors is (a,b)-admissible. Otherwise we shall say that r is (a,b)-inadmissible.

Let $\mathbb{N}_o(a,b)$ denote the set of (a,b)-admissible odd integers. The set $\mathbb{N}(m,a,b)$ of (m,a,b)-*admissible* integers is defined then as follows:

$$\mathbb{N}(m,a,b) = \begin{cases} \mathbb{N}_o(a,b) & \text{if 2 is } (a,(-1)^m b)\text{-inadmissible,} \\ \mathbb{N}_o(a,b) \cup 2\mathbb{N}_o(a,b) & \text{if 2 is both } (a,(-1)^m b)\text{-admissible} \\ & \text{and } (a,b)\text{-inadmissible,} \\ \cup_{k=0}^{\infty} 2^k\mathbb{N}_o(a,b) & \text{if 2 is both } (a,(-1)^m b)\text{-admissible} \\ & \text{and } (a,b)\text{-admissible.} \end{cases}$$

Let r be any integer greater than 1. Writing $r = 2^s q$, with q odd and s a nonnegative integer, we easily get the following:

(1) If $\mathbb{N}(m,a,b) = \mathbb{N}_o(a,b)$, then

$$r \in \mathbb{N}(m,a,b) \iff s = 0 \text{ and } \mathrm{C}(m,a,b,r);$$

(2) If $\mathbb{N}(m,a,b) = \mathbb{N}_o(a,b) \cup 2\mathbb{N}_o(a,b)$, then

$$r \in \mathbb{N}(m,a,b) \iff s \leq 1 \text{ and } \mathrm{C}(m,a,b,r);$$

(3) If $\mathbb{N}(m,a,b) = \bigcup_{k=0}^{\infty} 2^k \mathbb{N}_{\mathrm{o}}(a,b)$, then

$$r \in \mathbb{N}(m,a,b) \iff s \geq 0 \text{ and } \mathrm{C}(m,a,b,r).$$

Hence,

$$r \in \mathbb{N}(m,a,b) \text{ if and only if } \mathrm{C}(m,a,b,r).$$

Consequently we reformulate Theorem 1.1 as follows.

THEOREM 5.2: *Let r be any integer greater than 1 and let $f(X)$ be an irreducible polynomial in $Z[X]$ of positive degree m, leading coefficient a and nonzero constant term b. Assume $r \in \mathbb{N}(m,a,b)$. Then*

$$f(X^r) \text{ is irreducible in } Z[X].$$

Finally we use Lemma 5.1 to illustrate Theorem 5.2. Let $Z = \mathbb{Z}[i]$, where $i = \sqrt{-1}$, and assume $f(X) = X^m + \cdots + 8i$ is irreducible in $Z[X]$.

We have $U = \{\pm 1, \pm i\}$, $a = 1 = u_a$, $e(a) = 0$ and

$$b = -(2i)^3 = -(1+i)^6 \quad \text{with } u_b = -1,\ e(b) = 6.$$

Then, since $e(a,b) = 6$ and $u_a^{-1}u_b = -1 \in U^p$ for each prime p, we have that 2 and 3 are the unique $(1, 8i)$-inadmissible primes. On the other hand, since $(-1)^m u_a^{-1} u_b = (-1)^{m+1} \in U^2$, we also have that 2 is $(1, (-1)^m 8i)$-inadmissible for all m. Therefore, we have

$$\mathbb{N}(m,1,8i) = \mathbb{N}_{\mathrm{o}}(1,8i) = \{r \in \mathbb{N}_{\mathrm{o}} : 3 \not| r\},$$

which says that $f(X^r)$ is irreducible for each positive integer r that is relatively prime to 6.

ACKNOWLEDGMENT. I thank the referee for his constructive remarks which helped improve a previous version of this paper.

References

[1] M. C. R. Butler, *Reducibility Criteria for Polynomials of Two General Classes*, Proceedings of the London Mathematical Society **7** (1957), 63–74.
[2] P. M. Cohn, *Algebra*, John Wiley & Sons, London–New York–Sydney, 1977.
[3] P. J. Davis, *Circulant Matrices*, 2nd edition, Chelsea Publishing Co., New York, 1994.
[4] H. L. Dorwart, *Irreducibility of polynomials,* American Mathematical Monthly **42** (1935), 369–381.
[5] F. R. Gantmacher, *Matrix Theory*, Chelsea Publishing Co., 1959.
[6] A. G. Kurosh, *General Algebra*, Chelsea Publishing Co., 1965.

[7] R. Lidl and H. Niederreiter; *Introduction to finite fields and their applications*, Cambridge University press, Cambridge, 1994.
[8] P. R. Morandi, *Fields and Galois Theory*, Springer-Verlag, New York, 1996.