A Simple Irreducibility Criterion for $f(X^2)$

Natalio H. Guersenzvaig

Let k be any field, and let $f(X)$ be an arbitrary polynomial of $k[X]$ which is irreducible in $k[X]$. A well-known result of Wahlen-Capelli (see [1], p. 212) establishes necessary and sufficient conditions for the irreducibility of $f(g(X))$ in $k[X]$, where $g(X)$ is any polynomial of $k[X]$. The proof of this result is not elementary because it uses the theory of field extensions.

In this short article we establish, with a very elementary proof, necessary and sufficient conditions for the reducibility of $f(X^2)$ in $Z[X]$, where Z denotes an arbitrary unique factorization domain. As an immediate consequence we obtain a simple sufficient condition for the irreducibility of $f(X^2)$ in $Z[X]$.

Theorem 1. *Let $f(X)$ be any non-zero polynomial in $Z[X]$. The following statements are equivalent.*

(i) *$f(X^2)$ is reducible in $Z[X]$.*

(ii) *$f(X)$ is reducible in $Z[X]$ or there exist polynomials $G(X)$, $H(X)$ in $Z[X]$ and a unit u of Z (that is, an invertible element of $Z \setminus \{0\}$) such that*

$$uf(X) = G^2(X) - XH^2(X). \qquad (\star)$$

Proof. We first suppose that (ii) is true. It is clear that $f(X^2)$ is reducible in $Z[X]$ if $f(X)$ is. Then suppose that $f(X)$ is irreducible in $Z[X]$. Thus, $(\star)$ is true with $H(X) \neq 0$. As a consequence, (i) follows, because $G(X^2)$ and $XH(X^2)$ have degrees of distinct parity and

$$uf(X^2) = (G(X^2) - XH(X^2))(G(X^2) + XH(X^2)).$$

Now suppose that (i) is true. Assume $f(X)$ is irreducible in $Z[X]$ (otherwise we are done). Then $f(X^2) = g(X)h(X)$, where $g(X)$, $h(X) \in Z[X]$ are not units of Z. Collecting even powers in $g(X)$ and $h(X)$, we obtain

$$g(X) = G(X^2) + XL(X^2), \qquad h(X) = H(X^2) + XT(X^2), \quad (1)$$

for some polynomials G, L, H, and T in $Z[X]$. Hence,

$$f(X^2) = G(X^2)H(X^2) + X^2L(X^2)T(X^2) + XG(X^2)T(X^2) + XL(X^2)H(X^2). \qquad (2)$$

Copyright © 2003 Canadian Mathematical Society

for some polynomials G, L, H, and T in $Z[X]$.

We claim that $L(X)T(X) \neq 0$. We prove this by contradiction. Suppose for example that $L(X) = 0$ (the case $T(X) = 0$ is analogous). Thus, we have

$$f(X^2) - G(X^2)H(X^2) \;=\; XG(X^2)T(X^2)\,. \tag{3}$$

Both sides of this equality are zero because, otherwise, they have degrees of different parity. Thus, $T(X) = 0$; whence, $f(X^2) = G(X^2)H(X^2)$; that is, $f(X) = G(X)H(X)$, which contradicts the assumption that $f(X)$ is irreducible in $Z[X]$.

It can be assumed that the greatest common divisor of $G(X)$ and $L(X)$, say $D(X)$, is equal to 1, because, otherwise, we consider the factorization $f(X^2) = g^*(X)h^*(X)$, with $h^*(X) = D(X^2)h(X)$ and

$$g^*(X) \;=\; \frac{g(X)}{D(X^2)} \;=\; \frac{G(X^2)}{D(X^2)} + X\frac{L(X^2)}{D(X^2)}\,,$$

where such a condition is satisfied. Note that in order to replace $g(X)$ by $g^*(X)$, we need to know that $g^*(X)$ is not a unit of Z. If it were a unit, then $L(X^2) = 0$ from (1) which implies $L(X) = 0$. But this leads to a contradiction, as was shown in the preceding paragraph.

Now, from (2), via the same argument used in (3), we get

$$G(X)T(X) + L(X)H(X) \;=\; 0\,, \tag{4}$$

and

$$f(X) \;=\; G(X)H(X) + XL(X)T(X)\,.$$

As a consequence,

$$L(X)f(X) \;=\; G(X)L(X)H(X) + XL^2(X)T(X)\,.$$

By using (4) this becomes

$$L(X)f(X) \;=\; -T(X)\big(G^2(X) - XL^2(X)\big)\,;$$

whence, $L(X)$ is a divisor of $T(X)$ because $G(X)$ and $L(X)$ are coprime polynomials. Thus,

$$f(X) \;=\; M(X)\big(G^2(X) - XL^2(X)\big)$$

for some $M(X) \in Z[X]$. But we have assumed that $f(X)$ is irreducible in $Z[X]$. Therefore, $M(X)$ is a unit of Z, and $(\star)$ follows. □

Corollary 1. *Let $f(X)$ be any polynomial of $Z[X]$ which is irreducible in $Z[X]$. Assume that $f(X)$ has leading coefficient A and constant term C. In addition suppose that uA is not a square in Z for each unit u of Z or that AC is not a square in Z. Then*

$$f(X^2) \text{ is irreducible in } Z[X].$$

Remark. If $f(X)$ is detected as irreducible via the well-known Eisenstein's Criterion (see [2, pp. 267-268]), which also works in $Z[X]$ (*mutatis mutandis*), it follows immediately that $f(X^m)$ is irreducible in $Z[X]$ for any positive integer m. However, our result works in cases where Eisenstein's Criterion is inapplicable. As an example of this, we consider the polynomial $f(X) = 3X^2 + 2X + 4 \in \mathbb{Z}[X]$, which is certainly irreducible in $\mathbb{Z}[X]$. Using Corollary 1, we note that $AC = 12$ and ± 3 are not squares in $\mathbb{Z}$. From either of these two facts we have that $f\left(X^{2^m}\right) = 3X^{2^m} + 2X^{2^{m-1}} + 4$ is irreducible in $\mathbb{Z}[X]$ for any positive integer m.

References.

[1] P.M. Cohn, *Algebra*, Vol. 2, John Wiley & Sons, 1977.

[2] W.K. Nicholson, *Introduction to Abstract Algebra*, Wiley, 1999.

Natalio H. Guersenzvaig
Universidad CAECE
Buenos Aires
Argentina
nguersen@fibertel.com.ar