Some Reducibility Criteria for
\[ AX^4 + BX^2 + C \]

Natalio H. Guersenzvaig

Let \( Z \) be an arbitrary unique factorization domain. We established the following results in [1].

**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 \( G(X) \) and \( H(X) \) in \( Z[X] \) and a unit \( u \) of \( Z \) (that is, an invertible element of \( Z \setminus \{0\} \)) such that

\[
uf(X) = G^2(X) - XH^2(X).
\]

**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 either \( uA \) is not a square in \( Z \) for each unit \( u \) of \( Z \) or that \( AC \) is not a square in \( Z \). Then \( f(X^2) \) is irreducible in \( Z[X] \).

For domains of characteristic 2 (that is, for domains in which \(-1 = 1\) (see [3, p. 193])), we have a more precise result.

**Corollary 2** Suppose that \( Z \) has characteristic 2. Let \( f(X) \) be any polynomial of \( Z[X] \) which is irreducible in \( Z[X] \). Let \( A \) be the leading coefficient of \( f(X) \). Then the following statements are equivalent.

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

(ii) There exists a unit \( u \) of \( Z \) such that every coefficient of \( uf(X) \) is a square in \( Z \).

**Proof.** The equivalence of (i) and (ii) follows at once from Theorem 1 and

\[ (a_1 + \cdots + a_n)^2 = a_1^2 + \cdots + a_n^2 \]

for any \( a_1, \ldots, a_n \in Z \). \( \Box \)

There are more precise results for biquadratic polynomials in \( Z[X] \); that is, for \( f(X^2) \), where \( f(X) \) is a quadratic polynomial of \( Z[X] \) (for biquadratic polynomials over a field, see [5, pp. 137-139]). In order to give elementary proofs, we recall that a non-zero polynomial of \( Z[X] \) is called **primitive** if the greatest common divisor of its coefficients is a unit of \( Z \). A quadratic polynomial \( f(X) = AX^2 + BX + C \in Z[X] \) is irreducible in \( Z[X] \) if and only if \( f(X) \) is a primitive polynomial whose discriminant, \( B^2 - 4AC \), is not a square in \( Z \).
We have the following characterizations of the biquadratic polynomials of $Z[X]$ which are reducible in $Z[X]$.

**Theorem 2** Let $f(X) = AX^2 + BX + C$ be any primitive quadratic polynomial of $Z[X]$. Let $\tilde{f}(X) = X^2 + 2ABX + A^2(B^2 - 4AC)$. The following three statements are equivalent:

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

(ii) $f(X)$ is reducible in $Z[X]$, or there exists $S \in Z$ with $AC = S^2$ such that $A(2S - B)$ is a square in $Z$;

(iii) $f(X)$ is reducible in $Z[X]$, or some square element of $Z$ is a root of $\tilde{f}(X)$.

**Proof.** Certainly the three statements are all true if $f(X)$ is reducible in $Z[X]$. Thus, we may assume that $f(X)$ is irreducible in $Z[X]$.

We first suppose that (i) is true. It follows from Theorem 1 that there exist polynomials $G(X)$ and $H(X) \in Z[X]$ and a unit $u$ of $Z$ such that

$$u(AX^2 + BX + C) = G^2(X) - XH^2(X).$$

Thus, $G(X)$ is linear and $H(X)$ is constant, say

$$G(X) = \alpha X + \gamma \quad \text{and} \quad H(X) = \beta.$$

Then $uA = \alpha^2$, $uC = \gamma^2$, and $2\alpha\gamma - uB = \beta^2$. Hence, $AC = (u^{-1}\alpha\gamma)^2$ and $u(2u^{-1}\alpha\gamma - B) = \beta^2$. Then (ii) is true with $S = u^{-1}\alpha\gamma$, because

$$A(2S - B) = (u^{-1})^2(uA)(u(2S - B)) = (u^{-1}\alpha\beta)^2.$$

Now suppose that (ii) is true; that is, there exist $S$ and $T$ in $Z$ such that $AC = S^2$ and $A(2S - B) = T^2$. Then (iii) is true with $\tilde{f}(T^2) = 0$, because

$$\tilde{f}(X^2) = (X^2 + AB)^2 - 4A^2S^2$$

$$= (X^2 - 2AS + AB)(X^2 + 2AS + AB)$$

$$= (X^2 - T^2)(X^2 + 2AS + AB).$$

Finally, suppose that (iii) is true. It is clear that the discriminant of $\tilde{f}(X)$ is equal to $16A^4C$, which is a square in $Z$ because $\tilde{f}(X)$ has a root in $Z$. Then there exist $S$ and $T$ in $Z$ such that $AC = S^2$ and $\tilde{f}(T^2) = 0$. Hence,

$$0 = (T^2 + AB)^2 - 4A^2S^2 = (T^2 - A(2S - B))(T^2 - A(2(-S) - B)).$$

Therefore, since $AC = S^2 = (-S)^2$, we may assume that $AC = S^2$ and $A(2S - B) = T^2$. It follows from this that

$$Af(X^2) = A^2X^4 + ABX^2 + AC = (AX^2 + S)^2 - T^2X^2$$

$$= (AX^2 - TX + S)(AX^2 + TX + S)$$

$$= d^2(A'X^2 - T'X + S')(A'X^2 + T'X + S').$$

(1)
where \( d = \gcd(A, T, S) \) and \( A' = A/d, T' = T/d, S' = S/d \). Hence, 
\( A'X^2 - T'X + S' \) and \( A'X^2 + T'X + S' \) are primitive polynomials of \( \mathbb{Z}[X] \).

Conversely, a well-known result of Gauss (see [3, p. 317]) establishes that the product of primitive polynomials is also a primitive polynomial. Then, since \( f(X^2) \) is primitive, from (1), we get \( A = d^2 \), from which (i) follows. \( \Box \)

**Remark.** The polynomial \( f(X^2) \) has exactly four roots in \( \mathbb{Z} \) (counting multiplicities) if there exist \( S \) and \( T \) in \( \mathbb{Z} \) such that \( S^2 = AC, f(T^2) = 0 \), and \( T^2 - 4AS \) is a square in \( \mathbb{Z} \); otherwise, it has no roots. Of special importance is the case when \( T^2 - 4AS \) is not a square in \( \mathbb{Z} \), since \( f(X^2) \) then has two irreducible quadratic factors, but no roots.

Now we prove, without using complex numbers, that any "generalized" biquadratic polynomial of \( \mathbb{R}[X] \) is reducible in \( \mathbb{R}[X] \).

**Corollary 3** Let \( m \) be any positive integer, and let

\[
F(X) = AX^{4m} + BX^{2m} + C
\]

be a polynomial in \( \mathbb{R}[X] \) with \( A \neq 0 \). Then \( F(X) \) is reducible in \( \mathbb{R}[X] \).

**Proof.** It is clear, via the change of variable \( Y = X^m \), that it suffices to prove the case \( m = 1 \). We may also assume \( A > 0 \). Now suppose that \( F(X) \) is irreducible in \( \mathbb{R}[X] \). It follows from (ii) of Theorem 2 that \( B^2 - 4AC < 0 \) and that, for any real number \( S \), we have \( AC < S^2 \) or \( A(2S - B) < 0 \). Since this is clearly equivalent to the contradiction \( B^2 < 4AC \) and \( C < 0 \), the proof is complete. \( \Box \)

As an application of Theorem 2, we consider (for any \( a, b \in \mathbb{Z} \)) the polynomial

\[
F_{a,b}(X) = X^4 - 2(a + b)X^2 + (a - b)^2.
\]

We first determine necessary and sufficient conditions on \( a \) and \( b \) so that \( F_{a,b}(X) \) is reducible in \( \mathbb{Z}[X] \) (generalizing this way problem A3 of the 2001 Putnam Competition [2, pp. 829–831]).

If \( Z \) has characteristic 2, it is clear that \( F_{a,b}(X) = (X^2 + a - b)^2 \). Next suppose that the characteristic of \( Z \) is different from 2. From Theorem 2, it follows at once that \( F_{a,b}(X) \) is reducible in \( \mathbb{Z}[X] \) if and only if at least one of the elements \( 4((a + b)^2 - (a - b)^2) = 16ab, 2(a - b) + 2(a + b) = 4a, \) and \(-2(a - b) + 2(a + b) = 4b \) is a square in \( \mathbb{Z} \); that is, if and only if at least one of the elements \( a, b, \) and \( ab \) is a square in \( \mathbb{Z} \).

We note the following consequences:

1. The polynomial \( F_{a,b}(X) \) is reducible in \( \mathbb{Z}_p[X] \) for any prime \( p \), because, by the law of quadratic reciprocity, the product of non-squares in \( \mathbb{Z}_p \) is always a square in \( \mathbb{Z}_p \). (Thus, it is easy to find irreducible polynomials of \( \mathbb{Z}[X] \) which are reducible in \( \mathbb{Z}_p[X] \) for any prime integer \( p \); the case \( a = 5, b = 41 \) is considered in [4, pp. 133–134, 330]).
2. $X^4 - 2(Y + W)X^2 + (Y - W)^2$ is irreducible in $\mathbb{Q}[X, Y, W]$.

3. Let $\alpha$ and $\beta$ denote arbitrary square roots of $a$ and $b$, respectively, in some extension field of the field of quotients of $Z$, say $\mathbb{Q}_Z$ (see [3, pp. 210, 344]). Since $F_{a,b}(\alpha + \beta) = 0$, we have also given an elementary proof that $F_{a,b}(X)$ is the minimal polynomial of $\alpha + \beta$ over $\mathbb{Q}_Z$ if and only if none of the elements $a, b, ab$ is a square in $Z$ (which constitutes, for specific values of $a, b \in Z$, a very common exercise in any introductory course on extension fields).

With more generality, by taking $A = 1$ we get from Theorem 2 the following characterization of the elements of some algebraic closure of $\mathbb{Q}_Z$ (see [4, pp. 351, 359–360]) whose minimal polynomial over $\mathbb{Q}_Z$ is a biquadratic polynomial of $Z[X]$.

**Corollary 4** Suppose that $Z$ does not have characteristic 2. Let $\overline{Q}_Z$ be an algebraic closure of $\mathbb{Q}_Z$, and let $\xi$ be any element of $\overline{Q}_Z$. Let $F(X)$ be the minimal polynomial of $\xi$ over $\mathbb{Q}_Z$. The following statements are equivalent:

(i) $F(X) = X^4 + BX^2 + C$ is a biquadratic polynomial of $Z[X]$.

(ii) We can write $\xi$ in some of the following four ways:

$$\pm \sqrt{\frac{B \pm \sqrt{B^2 - 4C}}{2}}.$$

where $B$ and $C$ are elements of $Z$ such that $B^2 - 4C$ is not a square in $Z$, and $B \pm 2\sqrt{C}$ are not squares in $Z$ if $C$ is a square in $Z$.

**References**


--

Universidad CAECE
Buenos Aires
Argentina
nguersen@fibertel.com.ar

Natalio H. Guersenzeaig