MATH. SCAND. 8 (1960), 65–70

ON THE IRREDUCIBILITY OF CERTAIN TRINOMIALS AND QUADRINOMIALS

WILHELM LJUNGGREN

1.

The purpose of the present paper is to study the irreducibility over the field of rationals of the polynomials

$$f(x) = x^n + \varepsilon_1 x^m + \varepsilon_2 x^p + \varepsilon_3 ,$$

where n, m and p are natural numbers, $n > m > p$, and ε_1, ε_2 ε_3, take the values ± 1. We can suppose without loss of generality that $n \geqq m+p$, since the roots of $f(x)$ are the inverses of the roots of

$$x^n + \varepsilon_2\varepsilon_3 x^{n-p} + \varepsilon_1\varepsilon_3 x^{n-m} + \varepsilon_3 .$$

Further we leave aside the trivial case $n = m+p$ with $\varepsilon_3 = \varepsilon_1\varepsilon_2$, where we have the obvious factorization $f(x) = (x^m + \varepsilon_2)(x^p + \varepsilon_1)$. The complete solution of the problem is given in the following two theorems:

THEOREM 1. *If $f(x)$ has no zeros which are roots of unity, then $f(x)$ is irreducible. If $f(x)$ has exactly q such zeros, then $f(x)$ can be decomposed into two rational factors, one of which is of degree q with all these roots of unity as zeros, while the other is irreducible.*

THEOREM 2. *If $n = n_1 d$, $m = m_1 d$, $p = p_1 d$, and $(n_1, m_1, p_1) = 1$ $(n_1, m_1 - p_1) = d_1$, $(m_1, n_1 - p_1) = d_2$, $(p_1, n_1 - m_1) = d_3$, then all possible roots of unity of $f(x)$ are simple zeros, which are to be found among the zeros of*

$$x^{dd_1} = \pm 1, \quad x^{dd_2} = \pm 1, \quad x^{dd_3} = \pm 1 .$$

In his paper [1] E. S. Selmer has studied the corresponding problem for the trinomials $g(x) = x^n + \varepsilon x^m + \varepsilon'$, $n \geqq 2m$, where ε and ε' take the values ± 1, without obtaining the complete solution, apart from the case $m = 1$. As a corrolary we find that theorem 1 is valid also if $f(x)$ is replaced by $g(x)$. The corresponding form of theorem 2 was already given by Selmer. See theorem 3 below. We could of course have presented a simpler proof by direct application of the method in this note.

Received April 22, 1960.

2.

Assuming irreducibility of $f(x)$, let

$$f(x) = \varphi_r(x)\psi_s(x), \qquad r+s = n\,, \tag{1}$$

where $\varphi_r(x)$ and $\psi_s(x)$ are monic polynomials with integral coefficients, of positive degrees r and s respectively.

At first we prove two lemmas.

LEMMA 1. *In* (1) *one at least of the two factors must be a reciprocal polynomial.*

PROOF. Putting

$$f_1(x) = x^r\varphi_r(x^{-1})\psi_s(x) = \sum_{i=0}^{n} c_i x^{n-i}\,, \tag{2}$$

we get

$$f_2(x) = x^s\psi_s(x^{-1})\varphi_r(x) = x^n f_1(x^{-1}) = \sum_{i=0}^{n} c_{n-i}x^{n-i} \tag{3}$$

and

$$f_1(x)f_2(x) = (x^n+\varepsilon_1 x^m+\varepsilon_2 x^p+\varepsilon_3)(\varepsilon_3 x^n+\varepsilon_2 x^{n-p}+\varepsilon_1 x^{n-m}+1)\,. \tag{4}$$

Equating the coefficients of x^{2n} and of x^n in the two expressions for $f_1(x)f_2(x)$, we find

$$c_0c_n = \varepsilon_3 \quad \text{and} \quad c_0^2+c_1^2+c_2^2+\ldots+c_{n-1}^2 = 4\,,$$

or

$$c_0c_n = \varepsilon_3 \quad \text{and} \quad c_1^2+c_2^2+\ldots+c_{n-1}^2 = 2\,. \tag{5}$$

Now (5) implies that two of the c_i's, $i=1,2,3,\ldots,n-1$, say c_{k_1} and c_{k_2}, $k_1<k_2$, must be equal to ± 1, and the other c_i's must be equal to zero.

The first expression for the reciprocal polynomial $f_1(x)f_2(x)$ is then reduced to

$$\begin{aligned} f_1(x)f_2(x) = {} & c_0c_nx^{2n}+c_{k_1}c_nx^{2n-k_1}+c_{k_2}c_nx^{2n-k_2}+ \\ & +c_0c_{k_1}x^{n+k_1}+c_0c_{k_2}x^{n+k_2}+c_{k_1}c_{k_2}x^{n+k_2-k_1}+4x^n+\ldots \end{aligned} \tag{6}$$

By multiplication (4) yields

$$\begin{aligned} f_1(x)f_2(x) = {} & \varepsilon_3x^{2n}+\varepsilon_2x^{2n-p}+\varepsilon_1x^{2n-m}+ \\ & +\varepsilon_1\varepsilon_3x^{n+m}+\varepsilon_2\varepsilon_3x^{n+p}+\varepsilon_1\varepsilon_2x^{n+m-p}+4x^n+\ldots\,. \end{aligned} \tag{7}$$

In order to compare (6) and (7) we shall arrange the exponents of the various powers of x, according to their magnitude, in two descending sequences, each containing just the first three terms, For (6) we then get the following four possibilities:

(6,1) $k_2 \leqq \frac{n}{2}$: $2n > 2n-k_1 > 2n-k_2$.

(6,2) $k_2 > \frac{n}{2}$, $k_1 \leqq n-k_2$: $2n > 2n-k_1 \geqq n+k_2$,

(6,3) $k_2 > \frac{n}{2}$, $\frac{n}{2} \geqq k_1 > n-k_2$: $2n > n+k_2 > 2n-k_2$,

(6,4) $k_2 > \frac{n}{2}$, $k_1 > \frac{n}{2}$: $2n > n+k_2 > n+k_1$.

For (7) we have only to distinguish between two cases:

(7,1) $n \geqq 2m$: $2n > 2n-p > 2n-m$,

(7,2) $2m > n \geqq n+p$: $2n > 2n-p \geqq n+m$.

Combining (6,1), (6,2), (6,3) and (6,4) with (7,1), we find in order the following four possibilities:

(8) $(k_1,k_2) = (p,m)$, $(p,n-m)$, $(m,n-p)$ or $(n-m,n-p)$.

If (7,1) is replaced by (7,2), the result is

(8') $(k_1,k_2) = (p,n-m)$, (p,m), $(n-m,n-p)$ or $(m,n-p)$.

Putting $(k_1,k_2)=(p,m)$, we obtain from (6) and (7)

$$c_0c_n = \varepsilon_3, \quad c_pc_n = \varepsilon_2 \quad \text{and} \quad c_mc_n = \varepsilon_1,$$

whence

$$f_1(x) = c_n(\varepsilon_3x^n + \varepsilon_2x^{n-p} + \varepsilon_1x^{n-m} + 1) = c_nx^nf(x^{-1}),$$

from which it readily follows that

$$\psi_s(x) = c_nx^s\psi_s(x^{-1}).$$

If $(k_1,k_2)=(n-m,n-p)$ we find by the same reasoning

$$c_0c_n = \varepsilon_3, \quad c_0c_{n-m} = \varepsilon_1 \quad \text{and} \quad c_0c_{n-p} = \varepsilon_2,$$

$$f_1(x) = c_0(x^n + \varepsilon_1x^m + \varepsilon_2x^p + \varepsilon_3) = c_0f(x),$$

$$\varphi_r(x) = c_0x^r\varphi_r(x^{-1}).$$

In the cases $(k_1,k_2)=(p,n-m)$ and $(k_1,k_2)=(m,n-p)$ a closer examination shows that both imply $n=2m$, the final result being the same as before, i.e. either $\varphi_r(x)$ or $\psi_s(x)$ is a reciprocal polynomial.

LEMMA 2. *If λ and λ^{-1} are both roots of $f(x)$, then we must have one of the following three possibilities:*

$$1^\circ \quad \lambda^n = -\varepsilon_3 \quad \text{and} \quad \lambda^{m-p} = -\varepsilon_1\varepsilon_2\,,$$
$$2^\circ \quad \lambda^m = -\varepsilon_1\varepsilon_3 \quad \text{and} \quad \lambda^{n-p} = -\varepsilon_2\,,$$
$$3^\circ \quad \lambda^p = -\varepsilon_2\varepsilon_3 \quad \text{and} \quad \lambda^{n-m} = -\varepsilon_1\,.$$

PROOF. From the two equations

$$\lambda^n+\varepsilon_1\lambda^m+\varepsilon_2\lambda^p+\varepsilon_3 = 0, \quad \lambda^n+\varepsilon_2\varepsilon_3\lambda^{n-p}+\varepsilon_1\varepsilon_3\lambda^{n-m}+\varepsilon_3 = 0$$

it follows by subtraction

$$\varepsilon_2\varepsilon_3\lambda^{n-p}+\varepsilon_1\varepsilon_3\lambda^{n-m}-\varepsilon_1\lambda^m-\varepsilon_2\lambda^p = 0\,,$$

or

$$(\varepsilon_2\lambda^{m-p}+\varepsilon_1)(\varepsilon_3\lambda^{n-m}-\varepsilon_1\varepsilon_2\lambda^p) = 0\,, \tag{9}$$

hence either $\lambda^p = -\varepsilon_1\varepsilon_2\lambda^m$ or $\lambda^p = \varepsilon_1\varepsilon_2\varepsilon_3\lambda^{n-m}$. Inserting these values in the equation $f(\lambda)=0$, we conclude either $\lambda^n = -\varepsilon_3$ or $(\lambda^m+\varepsilon_1\varepsilon_2)(\lambda^{n-m}+\varepsilon_1)=0$, from which the lemma readily follows.

3.

In this section we prove our two theorems. If a reciprocal polynomial has a zero λ, then it has also the zero λ^{-1}, and theorem 1 now follows immediately from the two lemmas.

Since $(n, m-p) = dd_1$, it is possible to find two integers u and v such that $dd_1 = nu+(m-p)v$, hence $\lambda^{dd_1} = \pm 1$. In the same way it is found that $\lambda^{dd_2} = \pm 1$ and $\lambda^{dd_3} = \pm 1$. Then it remains to show that such a root is always a simple root. Combining the expressions in 1°, 2° and 3° with the equation

$$n\lambda^n+m\lambda^m+p\lambda^p = 0\,,$$

we obtain, omitting some trivial calculations, the following necessary conditions that λ should be a multiple root: $n = m+p$ and $\varepsilon_3 = \varepsilon_1\varepsilon_2$. But we have left aside this case, and theorem 2 is proved.

4.

Then we shall give the conditions which have to be imposed on n, m, p, ε_1, ε_2 and ε_3, in order that the two equations in 1° should be compatible. We restrict ourselves to consider this first case, since the remaining ones give similar conditions.

$$(1^\circ, 1) \quad n_1/d_1 \text{ odd}, (m_1-p_1)/d_1 \text{ odd and } \varepsilon_3 = \varepsilon_1\varepsilon_2\colon \ \lambda^{dd_1} = -\varepsilon_3\,,$$
$$(1^\circ, 2) \quad n_1/d_1 \text{ even} \quad \text{and } \varepsilon_3 = -1\colon \ \lambda^{dd_1} = -\varepsilon_1\varepsilon_2\,,$$
$$(1^\circ, 3) \quad (n_1-p_1)/d_1 \text{ even} \quad \text{and } \varepsilon_1\varepsilon_2 = -1\colon \ \lambda^{dd_1} = -\varepsilon_3\,.$$

5.

THEOREM 3. *If* $n=n_1d$, $m=m_1d$, $(n_1,m_1)=1$, $n\geqq 2m$, *then the polynomial*

$$g(x) = x^n+\varepsilon x^m+\varepsilon', \qquad \varepsilon = \pm 1, \quad \varepsilon' = \pm 1,$$

is irreducible, apart from the following three cases, where $n_1+m_1\equiv 0 \pmod 3$:

n_1, m_1 *both odd,* $\varepsilon=1$; n_1 *even,* $\varepsilon'=1$; m_1 *even,* $\varepsilon'=\varepsilon$, $g(x)$ *then being a product of the polynomial*

$$x^{2d}+\varepsilon^m\varepsilon'^n x^d+1$$

and a second irreducible polynomial.

PROOF. If $n=2m$ and $\varepsilon'=1$, there is nothing to prove. If $n=2m$ and $\varepsilon'=-1$, or if $n>2m$, we can make use of our theorems 1 and 2, noticing that

$$(x^n+\varepsilon x^m+\varepsilon')(x^n-\varepsilon') = x^{2n}+\varepsilon x^{n+m}-\varepsilon\varepsilon' x^m-1,$$

where $2n>n+m>m$ and in case $n=2m$, $\varepsilon_3\neq\varepsilon_1\varepsilon_2$. Here we have

$$(2n,n+m,m) = (m,n) = d,$$

$$d_1 = (2n_1,n_1) = n_1, \quad d_2 = (n_1+m_1,2n_1-m_1),$$

and

$$d_3 = (m_1,n_1-m_1) = 1.$$

For d_2 we find the values 1 or 3 according as $n_1+m_1\equiv 0 \pmod 3$ or not. It is obvious that a possible root of unity, λ of $g(x)$, cannot satisfy an equation $\lambda^d=\pm 1$.

If $d_2=1$, then $g(x)$ must be irreducible.

The equations corresponding to case 2°, lemma 2, are here

$$\lambda^{n+m} = \varepsilon \quad \text{and} \quad \lambda^{2n-m} = \varepsilon\varepsilon'$$

or

$$\lambda^{3n} = \varepsilon' \quad \text{and} \quad \lambda^{3m} = \varepsilon\varepsilon'.$$

If $d_2=3$, we conclude $\varepsilon=1$, $\lambda^{3d}=\varepsilon'$ or $\varepsilon'=1$, $\lambda^{3d}=\varepsilon$ or $\varepsilon=\varepsilon'$, $\lambda^{3d}=\varepsilon'$, from which we get the last statement in the theorem.

6.

It is a tedious but straight-forward job to find all cases where $f(x)$ is irreducible. We therefore restrict ourselves to state the following simple result:

If n_1,m_1 *and* p_1 *are all odd integers, then the polynomials* $x^n+x^m+x^p\pm\varepsilon_3$ *are irreducible.*

By means of the simple method used in this paper we may also derive other criteria of irreducibility. However, we don't enter into this here.

REFERENCE

1. E. S. Selmer, *On the irreducibility of certain trinomials*, Math. Scand. 4 (1956), 287–302.

UNIVERSITY OF OSLO, NORWAY