Decomposition of primes in number fields defined by trinomials


<http://www.numdam.org/item?id=JTNB_1991__3_1_27_0>
Decomposition of primes in number fields
defined by trinomials.

par P. LLORENTÉ, E. NART AND N. VILA

Abstract — In this paper we deal with the problem of finding the prime-ideal decomposition of a prime integer in a number field $K$ defined by an irreducible trinomial of the type $X^{p^m} + AX + B \in \mathbb{Z}[X]$, in terms of $A$ and $B$. We also compute effectively the discriminant of $K$.

1. Introduction

Let $K$ be the number field defined by an irreducible trinomial of the type:

$$X^{p^m} + AX + B, \quad A, B \in \mathbb{Z}, \quad p \text{ prime}, \quad m \geq 1.$$

In this paper we study the prime-ideal decomposition of the rational primes in $K$. Our results extend those of Vélez in [6], where he deals with the decomposition of $p$ in the case $A = 0$. However, the methods are different, ours being based on Newton’s polygon techniques. The results are essentially complete except for a few special cases which can be handled by an specific treatment (see section 2.3). This is done explicitly for $p^n = 4$ or 5, so that there are no exceptions at all for quartic and quintic trinomials.

Let us remark that the main aim of the paper is to give a complete answer in the case $p|A, p \nmid B$ (Theorems 3 and 4). The results concerning the other cases are easily obtained applying the ideas of [2], where we dealt with the computation of the discriminant of $K$, whereas the case $p|A, p \nmid B$ was not even considered. We give also the $p$-valuation of the discriminant of $K$ in all cases including those not covered by [2].

Mots clefs: Decomposition of primes, Discriminant, Trinomials.
Manuscrit reçu le 20 juillet 1990.
2. Results

Let $K = \mathbb{Q}(\theta)$, where $\theta$ is a root of an irreducible polynomial of the type:

$$f(X) = X^n + AX + B,$$

where $n, A, B \in \mathbb{Z}, n > 3$. For the case $n = 3$ see [1]. Let us denote by $d$ and

$$D = (-1)^{\frac{n(n-1)}{2}}(n^n B^{n-1} + (-1)^{n-1}(n-1)^{n-1} A^n),$$

the respective discriminants of $K$ and $\theta$. For simplicity we shall write in the sequel $N$ for the ideal norm $N_{K/Q}$.

For any prime $q \in \mathbb{Z}$ and integer $u \in \mathbb{Z}$ (or $q$-adic integer $u \in \mathbb{Z}_q$) we shall denote by $v_q(u)$ the greatest exponent $s$ such that $q^s | u$ and we shall write $u_q := u / q^{v_q(u)}$.

It is well-known that we can assume that the conditions:

$$v_q(A) \geq n - 1, \quad v_q(B) \geq n,$$

are not satisfied simultaneously for any prime integer $q$. We shall make this assumption throughout the paper.

Let $F(X) \in \mathbb{Z}[X]$ be a polynomial, $q \in \mathbb{Z}$ a prime integer and let

$$F(X) \equiv \Phi_1(X)^{e_1} \cdots \Phi_s(X)^{e_s} \pmod{q},$$

be the decomposition of $F(X)$ as a product of irreducible factors $(\bmod q)$. An integer ideal $\mathfrak{a}$ of any number field $L$ will be called "$q$ analogous to the polynomial $F(X)$" if the decomposition of $\mathfrak{a}$ into a product of prime ideals of $L$ is of the type:

$$\mathfrak{a} = q_1^{e_1} \cdots q_s^{e_s}, \quad N_{L/Q}(q_i) = q^{d_{\Phi_i}(X)} \text{ for all } i.$$

2.1. Decomposition of the primes $q$ not dividing $n$.

**Theorem 1.** Let $q \in \mathbb{Z}$ be a prime number such that $q \nmid n$. Let us denote $a = (n - 1, v_q(A))$ and $b = (n, v_q(B))$. The decomposition of $q$ into a product of prime ideals of $K$ is as follows:

If $v_q(B) > v_q(A)$ and $q \nmid a$,

$$q = qa^{(n-1)/n}, \quad N(q) = q, \quad q - \text{analogous to } X^a - A_q.$$
If \( v_q(B) \leq v_q(A) \) and \( v_q(A) > 0 \),

\[
q = a^{n/b}, \quad a \quad q - \text{analogous to } X^b - B_q.
\]

If \( q \nmid AB \) and \( q | D \), the decomposition of \( f(X) \) into a product of irreducible factors (mod \( q \)) is of the type:

\[
f(X) \equiv (x - u)^2 \Phi_1(X) \cdots \Phi_s(X) \pmod{q},
\]

and we have

\[
q = q_1 \cdots q_s a, \quad N(q_i) = q^{\deg(\Phi_i(X))} \quad \text{for all } i, \quad N(a) = q^2,
\]

where

\[
a = \begin{cases} 
q, & N(q) = q, \text{ if } v_q(D) \text{ even and } \left( \frac{D_q}{q} \right) = (-1)^{n-s} \\
q^2, & N(q) = q^2, \text{ if } v_q(D) \text{ even and } \left( \frac{D_q}{q} \right) = (-1)^{n-s+1} \\
q', & N(q) = q', \text{ if } v_q(D) \text{ even and } \left( \frac{D_q}{q} \right) = (-1)^{n-s} \\
q^2, & N(q) = q, \text{ if } v_q(D) \text{ odd.}
\end{cases}
\]

If \( q \nmid AB \), \( q \) is \( q \)-analogous to \( f(X) \).

\[
v_q(d) = \begin{cases} 
n - 1 - a + \inf\{(n - 1)v_q(B) - nv_q(A), (n - 1)v_q(n - 1)\}, & \text{if } v_q(B) > v_q(A) \text{ and } q \nmid a, \\
n - b, & \text{if } v_q(B) \leq v_q(A) \text{ and } v_q(A) > 0, \\
0, & \text{if } q \nmid AB \text{ and } v_q(D) \text{ even,} \\
1, & \text{if } q \nmid AB \text{ and } v_q(D) \text{ odd.}
\end{cases}
\]

### 2.2. Decomposition of the primes \( p \) dividing \( n \)

**Theorem 2.** If \( p \nmid A \), then \( p \) is \( p \)-analogous to \( f(X) \) and \( v_p(d) = 0 \).

If \( v_p(B) > v_p(A) > 0 \), then

\[
p = a^{(n-1)/a} p, \quad a \quad p - \text{analogous to } X^a + A_p, \quad N(p) = p
\]

and \( v_p(d) = n - a - 1 \), where we have denoted \( a = (n - 1, v_p(A)) \).

If \( 0 < v_p(B) \leq v_p(A) \) and \( p \mid v_p(B) \),

\[
p = p^n, \quad N(p) = p \quad \text{and} \quad v_p(d) = n - 1 + \inf\{nv_p(A) - (n - 1)v_p(B), nm\}.
\]

From now on we assume that \( n = p^m > 3 \) for some prime \( p \in \mathbb{Z} \) and integer \( m \geq 1 \).
THEOREM 3. Suppose that $p > 2$, $p | A$ and $p \not| B$. Let us denote:

$$r_0 = v_p(f(-B)), r_1 = v_p(f'(B)), r = \inf\{m+1, r_1, r_0\}, s_0 = v_p(D) - mn; e = p^{m-r+1}, e_k = p^{m-k}(p-1), 1 \leq k < m, e_m = p-2; J = (n-e)/(p-1), I = \frac{1}{2}(v_p(D) - v_p(d)).$$

Then we have:

$$(2.2.1) \quad p = \begin{cases} p_1^{e_1} \cdot \cdots \cdot p_{r-1}^{e_{r-1}} \cdot a, & N(p_k) = p \text{ for all } k, \text{ if } r \leq m, \\ p_1^{e_1} \cdot \cdots \cdot p_{m-1}^{e_{m-1}} \cdot b, & N(p_k) = p \text{ for all } k, \text{ if } r = m + 1, \end{cases}$$

where

$$a = \begin{cases} p^r, & N(p) = p, \text{ if } r_0 \leq r_1, \\ p^{r-1} \cdot p', & N(p) = N(p') = p, \text{ if } r_0 > r_1. \end{cases} \quad (2.2.2)$$

$$b = \begin{cases} p^3, & N(p) = 3, \text{ if } s_0 = m + 1 \\ p, & N(p) = 27, \\ p \cdot p', & N(p) = 3, N(p') = 9, \\ & \text{if } s_0 = m + 2 \text{ and } D_3 \equiv (-1)^{m-1} \text{ (mod 3).} \end{cases} \quad (2.2.3)$$

If $p = 3$ and $s_0 \leq m + 2,$

$$b = \begin{cases} p^3, & N(p) = 3, \text{ if } s_0 = m + 1 \\ p, & N(p) = 27, \\ p \cdot p', & N(p) = 3, N(p') = 9, \\ & \text{if } s_0 = m + 2 \text{ and } D_3 \equiv (-1)^{m-1} \text{ (mod 3).} \end{cases} \quad (2.2.4)$$

If $p > 3$ or $p = 3$ and $s_0 > m + 2,$

$$b = \begin{cases} p_m^{e_m} \cdot p^2, N(p_m) = N(p) = p, \text{ if } v_p(D) \text{ odd} \\ p_m^{e_m} \cdot p, N(p_m) = N(p) = p^2, \text{ if } v_p(D) \text{ even} \\ \text{and } \left(\frac{-1}{p} \frac{n(n-1)}{2D_p}\right) = -1 \quad (2.2.5) \end{cases}$$

Moreover $I = J$ in cases (2.2.2) and (2.2.4), $I = J + 1$ in case (2.2.3) and $I = J + [(s_0 - m)/2] + 1$ in the rest of the cases.

THEOREM 4. Suppose that $2 | A$, $2 \not| B$ and let $r_0, r_1, r, s_0, e, e_k \ (1 \leq k < m), J$ and $I$ be as in Theorem 3. Let $u = [(s_0 - m + 1)/2]$. Then we have

$$(2.2.7) \quad 2 = \begin{cases} p_1^{r_1} \cdot \cdots \cdot p_{r-2}^{e_{r-2}} \cdot a, & N(p_k) = 2 \text{ for all } k, \text{ if } r \leq m, \\ p_1^{r_1} \cdot \cdots \cdot p_{m-2}^{e_{m-2}} \cdot b, & N(p_k) = 2 \text{ for all } k, \text{ if } r = m + 1, \end{cases}$$
where

\[ a = \begin{cases} 
 p^r, N(p) = 4, & \text{if } r_0 \leq r_1 \\
 p_{m-1}^{m-1} p, N(p_{m-1}) = 2, N(p) = 4, & \text{if } r_1 = m \text{ and } r_0 = m + 1 \\
 p_{r-1}^{r-1} p^{r-1} p', N(p_{m-1}) = N(p) = N(p') = 2, & \text{otherwise} 
\end{cases} \]  
(2.2.8)

\[ b = \begin{cases} 
 p^2, N(p) = 2, & \text{if } v_2(D) - m \text{ even or} \\
 p, N(p) = 4, & \text{if } v_2(D) - m \text{ odd and} \\
 p.p', N(p) = N(p') = 2, & \text{if } v_2(D) - m \text{ odd and} 
\end{cases} \]
\[ D_2 \equiv 1 + 2^n (\text{mod } 4) \]  
(2.2.10)
\[ D_2 \equiv 3 + n^2 + 2^u (\text{mod } 8) \]  
(2.2.11)
\[ D_2 \equiv 7 + n^2 + 2^u (\text{mod } 8) \]  
(2.2.11)

Moreover \( I = J \) in cases (2.2.8), \( I = J + 1 \) in cases (2.2.9), \( I = J + u - 1 \) in cases (2.2.10) and \( I = J + u \) in cases (2.2.11).

### 2.3. Quartic and quintic trinomials

In this section we complete the general theorems above in the cases \( n = 4 \) and \( 5 \). Let \( n = p^m \). Theorems 2, 3 and 4 give the decomposition of \( p \) in all cases except for the following:

(2.3.1) \( p | v_p(B) \) and \( 0 < v_p(B) \leq v_p(A) \).

For the primes \( q \neq p \) the only case not covered by Theorem 1 is:

(2.3.2) \( q | (n - 1, v_q(A)) \) and \( 0 < v_q(A) < v_q(B) \).

Equations satisfying (2.3.1) or (2.3.2) can be handled by an specific treatment but the results are too disperse to fit them into a reasonable theorem. For instance, for \( n = 4 \), (2.3.2) is not possible and (2.3.1) occurs only for \( p = 2 \) and equations:

(2.3.3) \( X^4 + 2^{2+\epsilon} AX + 2^2 B, \) \( 2 \not| AB, \) \( e \geq 0 \).

For \( n = 5 \), (2.3.1) is not possible and (2.3.2) occurs only for \( q = 2 \) and equations:

(2.3.4) \( X^5 + 2^2 BX + 2^{3+\epsilon} C, \) \( 2 \not| BC, \) \( e \geq 0 \).
Theorem 5. The decomposition of 2 in the number field defined by (2.3.3) or (2.3.4) is
\[ 2 = \begin{cases} a, & \text{if } n = 4, \\ \tau a, & \text{if } n = 5, \end{cases} \]
where \( a \) is an integer ideal having the following decomposition:
\[ a = p^4, \quad \text{if } e = 0 \text{ or } 1. \]

For \( e \geq 2 \) and \( B \equiv 1(\text{mod } 4) \):
\[ a = \begin{cases} p^4, & \text{if } e = 2, B \equiv 1(\text{mod } 8) \text{ or } e \geq 3, B \equiv 5(\text{mod } 8), \\ p^2p_1^2, & \text{if } e = 2, B \equiv 13(\text{mod } 16) \text{ or } e \geq 3, B \equiv 1(\text{mod } 16), \\ p_2^2, & \text{if } e = 2, B \equiv 5(\text{mod } 16) \text{ or } e \geq 3, B \equiv 9(\text{mod } 16). \end{cases} \]

Whereas for \( e \geq 2 \) and \( B \equiv 3(\text{mod } 4) \):
\[ a = \begin{cases} p^2p_1^2, & \text{if } B \equiv 7(\text{mod } 8), \\ p_2^2, & \text{if } B \equiv 3(\text{mod } 8). \end{cases} \]

In all cases \( N(p) = N(p_1) = 2 \) and \( N(p_2) = 4 \). Moreover, \( v_2(d) = 4 \) when \( e = 0 \) and in the cases (2.3.5), (2.3.6) and \( v_2(d) = 6 \) in the rest of the cases.

3. Proofs

The proofs of the Theorems of Section 2 are essentially based on an old technique developed by Ore concerning Newton's polygon of the trinomial \( f(X) \) (cf. [3] and [4]). For commodity of the reader we sum up the results we need of [3] and [4] in Theorem 6 below.

We recall first some definitions about Newton's polygon. Let \( F(X) = X^n + a_1X^{n-1} + \ldots + a_n \in \mathbb{Z}[X] \) and \( p \in \mathbb{Z} \) be a prime number. The lower convex envelope \( \Gamma \) of the set of points \( \{(i, v_p(a_i)), 0 \leq i \leq n\}(a_0 = 1) \) in the euclidean 2-space determines the so-called "Newton's polygon of \( F(X) \) with respect to \( p \)». Let \( S_1, \ldots, S_t \) be the sides of the polygon and \( \ell_i, h_i \) the length of the projections of \( S_i \) to the \( X \)-axis and \( Y \)-axis respectively. Let \( \varepsilon_i = (\ell_i, h_i) \) and \( \ell_i = \varepsilon_i. \lambda_i \) for all \( i \). If \( S_i \) begins at the point \( (s, v_p(a_s)) \) let \( s_j = s + j\lambda_i \) and:
\[ b_j = \begin{cases} (a_{x_j})_p & \text{if the point } (s_j, v_p(a_{x_j})) \text{ belongs to } S_i, \\ 0 & \text{otherwise}, \end{cases} \]
for all $0 \leq j \leq \varepsilon_i$. The polynomial:

$$F_i(Y) = b_0 Y^{\varepsilon_i} + b_1 Y^{\varepsilon_i-1} + \ldots + b_{\varepsilon_i},$$

is called the "associated polynomial of $S_i$". We define $F(X)$ to be "$S_i$-regular" if $p$ does not divide the discriminant of $F_i(Y)$. $F(X)$ will be called "$\Gamma$-regular" if it is $S_i$-regular for all $i$.

**Theorem 6.** (Ore [4], Theorems 6 and 8). Let $F(X) \in \mathbb{Z}[X]$ be a monic irreducible polynomial and let $L = \mathbb{Q}(\alpha)$, $\alpha$ a root of $F(X)$. Let $p \in \mathbb{Z}$ be a prime with the above notations about Newton's polygon $\Gamma$ of $F(X)$ with respect to $p$, we have the following decomposition of $p$ into a product of integer ideals of $L$:

$$p = a_1^{\lambda_1} \ldots a_t^{\lambda_t}.$$

For each $i$, the ideal $a_i$ is $p$-analogous to $F_i(Y)$ if $F(X)$ is $S_i$-regular. Moreover, if $F(X)$ is $\Gamma$-regular we have:

$$v_p(i(\alpha)) = \sum_{i=2}^{t} \ell_i \left( \sum_{j=1}^{i-1} h_j \right) + \frac{1}{2} \sum_{i=1}^{t} (\ell_i h_i - \ell_i - h_i + \varepsilon_i),$$

where $i(\alpha)$ denotes the index of $\alpha$. This expression for $v_p(i(\alpha))$ also coincides with the number of points with integer coordinates below the polygon except for the points on the X-axis and on the last ordinate.

For the proof of theorem 1 we need a well-known lemma (cf.[5]):

**Lemma 1.** Let $L$ be a number field of degree $[L : \mathbb{Q}] = n$. Let $q$ be a prime integer unramified in $L$ and let $s$ be the number of prime ideals of $L$ lying over $q$. Then, the discriminant $d$ of $L$ satisfies

$$\frac{d}{q} = (-1)^{n-s}.$$

**Proof of theorem 1.** The assertions (2.1.1) and (2.1.2) are a straightforward application of Theorem 6. For (2.1.3) see the proof of [2 Theorem 2]. (2.1.4) is consequence of Lemma 1 and the fact that in this case $v_q(d) = 1$ if $q$ ramifies [2, Theorem 2]. (2.1.5) is obvious and the assertions concerning the computation of $v_q(d)$ are contained in [2, Theorem 1].
Theorem 2 follows from Theorem 6 and [2, Theorem 1]. We shall deal with the proof of Theorems 3 and 4 altogether. The proof of Theorem 5 is similar to those of the general theorems.

**Proof of Theorem 3 and 4.** Since $p|A$ and $p \not| B$, we have $f(X) \equiv (X + B)^n \pmod{p}$. Let $\Gamma$ be the Newton’s polygon of the polynomial:

$$F(X) := f(X - B) = \sum_{i=0}^{n} A_i X^{n-i},$$

where $A_0 = 1$, $A_i = \binom{n}{i} (-B)^i$ for $1 \leq i \leq n - 2$, $A_{n-1} = f'(-B)$ and $A_n = f(-B)$.

It is easy to see that:

$$v_p(A_i) = v_p\left(\binom{n}{i}\right) = m - v_p(i), \quad 1 \leq i \leq n - 2.$$

Let us determine first which would be the partial shape of $\Gamma$ if the two final points $(n - 1, r_1), (n, r_0)$ were omitted. By (3.2.1) we find that in that case $\Gamma$ would have $m - 1$ sides $S_1, \ldots, S_{m-1}$ if $p = 2$ and one more side $S_m$ if $p > 2$, each side $S_k$ ending at the point $(e_k, k)$ (see figure 1). In fact, $i = e_k$ is the greatest subindex with $v_p(A_i) = k$ and the slope of $S_k$ is $1/e_k$ so that these slopes are strictly increasing. Now, when we consider the two final points of $\Gamma$ we find that we can always assure that $\Gamma$ contains the sides $S_1, \ldots, S_{m-1}$ if $r > m$, the sides $S_1, \ldots, S_{r-1}$ if $r \leq m$ and $p > 2$, and the sides $S_1, \ldots, S_{r-2}$ if $r \leq m$ and $p = 2$.

![Figure 1](image-url)
Let $\Gamma'$ denote, in each case, the rest of the sides of $\Gamma$. By Theorem 6, the assertions (2.2.1) and (2.2.7) are proved. In order to find the further decomposition of the respective ideals $a$ and $b$ of Theorem 3 and 4 we shall study the shape and associated polynomials of $\Gamma'$. We must distinguish several cases. Before, note that for each $1 \leq k \leq m$, the number of points with integer coordinates below the sides $S_1 \cup \cdots \cup S_k$ except for the points on the $X$-axis and on the last ordinate is

$$I_k = p^{m-k} \left( \frac{p^k - 1}{p - 1} - k \right) \text{ for } 1 \leq k < m,$$

and

$$I_m = \frac{n - 1}{p - 1} - 2m + 1.$$

*Case $r \leq m, r_0 \leq r_1 : \Gamma'$ has only one side with lengths of the projections to the axis: $\ell = p^{m-r_0+1} = e$, $h = 1$ if $p > 2$ and $\ell = 2e$, $h = 2$ if $p = 2$ (see fig. 2). Therefore $\varepsilon := (\ell, h) = 1$ or 2 according to $p > 2$ or $p = 2$. In the latter case the associated polynomial is congruent (mod 2) to $Y^2 + Y + 1$, which is irreducible. By Theorem 6, (2.2.2) and (2.2.8) are proved. Since $F(X)$ is $\Gamma$-regular we have:

$$I = I_{r-1} + e(r - 1) \quad \text{if } p > 2,$$

$$I = I_{r-2} + e(2r - 3) \quad \text{if } p = 2,$$

hence, $I = J$ in both cases, as desired.

![Figure 2](image-url)
Case $r \leq m, r_0 > r_1$ : If $p > 2$, $\Gamma'$ has two sides $S, S'$ with projections to the axis $\ell = e - 1, h = 1$ and $\ell' = 1, h' = r_0 - r_1$ respectively (see fig. 3). If $p = 2$, $\Gamma'$ contains the side $S_{r-1}$ and two more sides with the same dimensions of $S$ and $S'$ above, except for the case $r_1 = m, r_0 = m + 1$ in which besides $S_{m-1}$ there is only one side with projections to the axis $\ell = h = 2$ and associated polynomial congruent (mod 2) to $Y^2 + Y + 1$, which is irreducible (see fig. 3). By Theorem 6, (2.2.3) and (2.2.9) are proved. Since $F(X)$ is $\Gamma$-regular in any case, we have:

$$I = I_{m-1} + 2m - 1 \quad \text{if } p = 2, r_1 = m \text{ and } r_0 = m + 1,$$

$$I = I_{r-1} + e(r-1) + 1 \quad \text{otherwise,}$$

hence $I = J + 1$ in both cases, as desired.

This ends the discussion of the case $r \leq m$.

Assume from now on that $r = m + 1$. If we study $\Gamma'$ in this case as above, we are led to many $p$-irregular cases. For this reason, instead of the polynomial $f(X - B)$ we seek an opportune substitute providing a much more regular situation.

Since $r_1 = v_p(n(-B)^{n-1} + A) > m$, we have:

$$v_p(A) = m \quad \text{and } A_p \equiv -1 (\text{mod } p).$$
Thus, from \( r_0 = v_p((-B)^{n-1} + A - 1) > m \), we get:

\[(3.2.2.) \quad (-B)^{n-1} \equiv 1 + p^m \pmod{p^{m-1}}.\]

Let \( \beta = -nB/(n - 1)A \). Since \( v_p(\beta) = 0 \), \( \beta \) is a \( p \)-adic integer and it is clear that Theorem 6 is also applicable to the polynomial:

\[G(X) := f(X + \beta) = \sum_{i=0}^{n-2} \binom{n}{i} \beta^i X^{n-i} + f'(\beta)X + f(\beta).\]

Computation leads to:

\[f(\beta) = (-1)^{\frac{n(n+1)}{2}} \frac{BD}{(n - 1)^n A^n}, \quad f'(\beta) = (-1)^{\frac{n(n+1)}{2}-1} \frac{D}{(n - 1)^{n-1} A^{n-1}},\]

hence, \( s_0 := v_p(f(\beta)) = v_p(D) - nm \) and \( s_1 := v_p(f'(\beta)) = s_0 + m \). It is easy to check that:

\[A_p^n \equiv (-1)^n \pmod{p^{m+1}} \quad \text{and} \quad (n - 1)^{n-1} \equiv (-1)^{n-1}(1 + n) \pmod{p^{m+1}},\]

hence, by (3.2.2):

\[\frac{(-1)^{\frac{n(n-1)}{2}}}{n^n} D = B^{n-1} + (-1)^{n-1}(n - 1)^{n-1} A_p^n \equiv 0 \pmod{p^{m+1}},\]

so that \( s_0 = v_p(D/n^n) > m \). Thus, Newton's polygon \( \Gamma_\beta \) of \( G(X) \) with respect to \( p \) can be also expressed as:

\[\Gamma_\beta = S_1 \cup \cdots \cup S_{m-1} \cup \Gamma'_\beta,\]

and we need only to study \( \Gamma'_\beta \) in order to find the prime-ideal decomposition of the respective ideals \( \mathfrak{b} \) of Theorems 3 and 4. Again, we have to distinguish several cases:

Case \( r = m + 1, p > 3 \) or \( p = 3 \) and \( s_0 > m + 2 \) : \( \Gamma'_\beta \) contains \( S_m \) and one more side of dimensions \( \ell = 2, h = s_0 - m \) (see fig. 4). For this latter side, \( \varepsilon = (\ell, h) = 1 \) or 2 according to \( s_0 - m \) odd or even. In the latter case the associated polynomial is:

\[\frac{n-1}{2} \beta^{n-2} Y^2 + \frac{f(\beta)}{p^{s_0}} \equiv \frac{B^{n-2}}{2} Y^2 + (-1)^{\frac{n(n+1)}{2}} BD_p \pmod{p},\]
and its discriminant is congruent to $(-1)^{n(n-1)/2}2D_p$. Since $v_p(D) \equiv s_0 - m \pmod{2}$, (2.2.6) is proved by Theorem 6. Moreover, since we are in a regular case we have:

$$I = I_m + 2m - 1 + \frac{s_0 - m + \varepsilon}{2} = J + \left[\frac{s_0 - m}{2}\right] + 1,$$

as desired.

\[\begin{array}{c}
p > 3 \text{ or } p = 3 \text{ and } s_0 > m + 2 \\
p = 3 \text{ and } s_0 \leq m + 2
\end{array}\]

Figure 4

Case $r = m+1, p = 3$ and $s_0 \leq m + 2$: $\Gamma'_\beta$ has only one side with $\ell = 3$ and $h = 2$ or 3 according to $s_0 = m + 1$ or $m + 2$ (see fig. 4). In the latter case $\varepsilon = 3$ and the associated polynomials is

$$\frac{(n-1)(n-2)}{2} \beta^{n-3}Y^3 + \frac{n-1}{2} \beta^{n-2}Y^2 + \frac{f(\beta)}{3^{s_0}} \equiv B^{n-3}Y^3 - B^{n-2} + (-1)^{m-1}BD_3 \pmod{3}.$$  

Since $(-1)^{n(n+1)/2} = (-1)^{m-1}$ in this case, multiplying by $B^2$ we get the polynomial $\Phi(Y) = Y^3 - By^2 + (-1)^{m-1}BD_3$, which is irreducible (mod 3) if $D_3 \equiv (-1)^{m-1} \pmod{3}$ and factorizes:

$$\phi(Y) \equiv (Y + B)(Y^2 + BY - 1) \pmod{3},$$
if \( D_3 \equiv (-1)^m \pmod{3} \). By Theorem 6, (2.2.5) is proved. Since we are in a regular case we have:

\[
I = I_{m-1} + 3m - 2 = J \quad \text{if} \quad s_0 = m + 1,
\]
\[
I = I_{m-1} + 3m = J + 2 \quad \text{if} \quad s_0 = m + 2.
\]

Case \( r = m + 1, p = 2 \) : \( \Gamma'_\beta \) has only one side with \( \ell = 2 \) and \( h = s_0 - m + 1 \) (see fig.5), hence \( \varepsilon = 1 \) or 2 according to \( s_0 - m + 1 \) odd or even, or equivalently according to \( v_2(D) - m \) even or odd. In the latter case, the associated polynomial is congruent \( \pmod{2} \) to \( Y^2 + 1 \), hence, it is an irregular case. In the former case Theorem 6 proves (2.2.10) and:

\[
I = I_{m-1} + 2m - 2 + \frac{s_0 - m}{2} = J + u - 1,
\]

as desired.

Finally, in order to deal with the case \( v_2(D) - m \) odd it is necessary to change again Newton's polygon. Let \( 2u = s_0 - m + 1 \) and \( \delta = (2^n - B)/(n - 1)A_2 \). Computation leads to:

\[
(3.2.3) \quad (n - 1)^n A_2^n f(\delta) = \sum_{i=0}^{n-2} \binom{n}{i} 2^{(n-i)u} (-B)^i + (B - 2^{n+m})D_0,
\]
where $D_0 = D/n^n = B^{n-1} - (n - 1)^{n-1}A^n$. Since $v_2(D_0) = s_0 = 2u + m - 1 > m, u > 0$ and there are exactly two summands in (3.2.3) with $v_2$ minimum and equal to $2u + m - 1$, hence, $v_2(f(\delta)) \geq 2u + m$. From the relation:

$$nf(X) - Xf'(X) = (n - 1)AX + nB,$$

and being $v_2((n - 1)A\delta + nB) = u + m$, we conclude that $v_2(f'(\delta)) = u + m$. Thus Newton’s polygon $\Gamma_\delta$ with respect to $p$ of the polynomial $f(X + \delta)$ is again expressible as: $\Gamma_\delta = S_1 \cup \cdots \cup S_{n-1} \cup \Gamma'_\delta$. We have now three possibilities (see fig.5):

a) $v_2(f(\delta)) = 2u + m$. $\Gamma'_\delta$ has only one side with $\ell = 2, h = 2u + 1$ hence $\varepsilon = (\ell, h) = 1$ and $a = p^2, N(p) = 2$. Moreover $I = I_{m-1} + 2(m - 1) + u = J + u - 1$.

b) $v_2(f(\delta)) = 2u + m + 1$. $\Gamma'_\delta$ has only one side with associated polynomial congruent (mod 2) to $Y^2 + Y + 1$, which is irreducible, hence $a = p^4, N(p) = 4$. Moreover $I = I_{m-1} + 2(m - 1) + u + 1 = J + u$.

c) $v_2(f(\delta)) > 2u + m + 1$. $\Gamma'_\delta$ has two sides and $a = p^2p', N(p) = N(p') = 2, I = J + u$ like in case b).

Taking congruence (mod $2^{2u+m+2}$) of (3.2.3) we shall be able to decide in which case falls our polynomial. All summands of (3.2.3) vanish (mod $2^{2u+m+2}$) except for the following:

$$\left(\begin{array}{c} n \\ 4 \end{array}\right)2^4n(-B)^{n-4} + \left(\begin{array}{c} n \\ 3 \end{array}\right)2^{3n}(-B)^{n-3} + \left(\begin{array}{c} n \\ 2 \end{array}\right)2^{2n}(-B)^{n-2} + BD_0.$$

Dividing by $2^{2u+m+1}$ and taking congruence (mod 8) we obtain:

$$(3.2.4) \quad 2^{2u+m+1} - 2^{2u-1} + 2^{u+1} + 2^{m-1} + BD_2 \quad (\text{mod 8})$$

From (3.2.2) we get $B \equiv -1 + 2^m$ (mod $2^{m+1}$), hence (3.2.4) is equal to:

$$2^{2u+m-2} - 2^{2u-1} + 2^{u+1} - 1 - D_2 \quad (\text{mod 8})$$

which is equal to $-1 - D_2$ (mod 8) if $u > 1$ and to $2^m + 1 - D_2$ if $u = 1$. Therefore cases a) b) and c) are equivalent to the following respective conditions:

\[ a) \Leftrightarrow \begin{cases} D_2 \equiv 1 \pmod 4 & \text{if } u > 1 \\ D_2 \equiv -1 \pmod 4 & \text{if } u = 1 \end{cases} \]

\[ b) \Leftrightarrow \begin{cases} D_2 \equiv 3 \pmod 8 & \text{if } u > 1 \\ D_2 \equiv 5 + n \pmod 8 & \text{if } u = 1 \end{cases} \]

\[ c) \Leftrightarrow \begin{cases} D_2 \equiv -1 \pmod 8 & \text{if } u > 1 \\ D_2 \equiv 1 + n \pmod 8 & \text{if } u = 1 \end{cases} \]
This ends the proof of (2.2.10) and (2.2.11).

REFERENCES


