ACTA ARITHMETICA
XLIII (1984)

Discriminants of number fields defined by trinomials

by

P. Llorente, E. Nart and N. Vila (Barcelona)

1. Introduction. In this paper we deal with the problem of the computation of the discriminant of a number field defined by an irreducible trinomial,

$$f(X) = X^n + AX^s + B \in \mathbf{Z}[X]$$

in terms of n, s, A and B. The case $n = 2$ is well known, and the cubic case was completely solved in [2]. The special case $s = 1$ has been considered by Komatsu in [1]. Our main result (Theorem 1) gives, except for a few special cases, a complete solution to this problem, which in the case $s = 1$ improves the main theorem of [1]. The methods are quite different from those of [1] and they can be easily generalized to the relative case.

2. The main theorem. Let $K = \mathbf{Q}(\theta)$, where θ is a root of an irreducible polynomial of the type,

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

where $n, s, A, B \in \mathbf{Z}$, $n > s \geqslant 1$. Let $m = (n, s)$, $n = mn'$ and $s = ms'$. The discriminant of θ is known to be ([4], th. 2):

$$D = (-1)^{n(n-1)/2} m^n B^{s-1} \big((n')^{n'} B^{n'-s'} + (-1)^{n'-1} (n'-s')^{n'-s'} (s')^{s'} A^{n'} \big)^m .$$

If d denotes the discriminant of K we have,

$$D = i(\theta)^2 d, \tag{1}$$

where $i(\theta)$ is the index of θ.

Throughout this paper, for any prime $p \in \mathbf{Z}$, we shall denote:

$v_p(r)$ = the greatest exponent k such that $p^k | r$, $r \in \mathbf{Z}$,
$A_p = A/p^{v_p(A)}$,
$B_p = B/p^{v_p(B)}$,
$t_p = v_p\big((n')^{n'} B_p^{n'-s'} + (-1)^{n'-1} (n'-s')^{n'-s'} (s')^{s'} A_p^{n'}\big)$,
$M_p = (n-s)v_p(B) - nv_p(A)$,
$a_p = \big(n-s, v_p(A)\big)$,
$b_p = \big(n, v_p(B)\big)$,
$c_p = \big(s, v_p(B) - v_p(A)\big)$,
$z_p = \big(n, s, v_p(A), v_p(B)\big)$.

Our main theorem is:

THEOREM 1. *With the preceding notations, let $p \in \mathbf{Z}$ be a prime number such that*

(2) $$p \nmid a_p c_p \qquad \text{if} \quad M_p > 0,$$

(3) $$p \nmid b_p, \quad \text{or} \quad p \mid \frac{n}{b_p} \quad \text{and} \quad -M_p = b_p \qquad \text{if} \quad M_p < 0,$$

(4) $$p \nmid z_p \qquad \text{if} \quad M_p = 0.$$

Then

(5) $$v_p(d) = nv_p(m) + n - \delta,$$

where

$$\delta = \begin{cases} a_p + c_p - \inf\{M_p, \max\{sv_p(s'), (n-s)v_p(n'-s')\}\} & \text{if} \quad M_p > 0 \\ b_p - \inf\{-M_p, nv_p(n')\} & \text{if} \quad M_p < 0, \\ b_p \quad \text{if} \quad M_p = 0 \text{ and } \dfrac{m}{z_p}\cdot t_p \text{ is even}, \\ b_p - z_p \quad \text{if} \quad M_p = 0 \text{ and } \dfrac{m}{z_p}\cdot t_p \text{ is odd}. \end{cases}$$

Therefore, if for every prime $p \in \mathbf{Z}$ dividing D, the corresponding condition (2), (3) or (4) is satisfied, we have $|d| = \prod_{p|D} p^{v_p(d)}$, where $v_p(d)$ is given by (5). Moreover, by (1), $d > 0$ if and only if $D > 0$.

Remark. It is well known that we may assume that $v_p(A) < n-s$ or $v_p(B) < n$. When applying Theorem 1 to a particular trinomial, it can be useful to put it in this situation.

For the proof of Theorem 1 we must discuss separately the cases $p \nmid B$ and $p|B$. In the latter case the proof is also different if $M_p = 0$ or $M_p \neq 0$.

3. The case $p \nmid B$. If $p|A$, then $M_p < 0$ and $b_p = n$. In this case Theorem 1 asserts that

$$p \nmid n \Rightarrow v_p(d) = 0,$$

which is obvious since if $p \nmid n$ we have $v_p(D) = 0$. If $p \nmid A$, $t_p = \dfrac{v_p(D)}{m} - n\cdot v_p(m)$ and the assertions of Theorem 1 can be summarized in:

THEOREM 2. *With the above notation, if $p \in \mathbf{Z}$ is a prime number such that $p \nmid ABm$, then*

$$v_p(d) = \begin{cases} 0 & \text{if} \quad v_p(D)/m \text{ is even}, \\ m & \text{if} \quad v_p(D)/m \text{ is odd}. \end{cases}$$

Proof. We consider first the case $m = 1$. If $p|ns(n-s)$, then $p \nmid D$ and the result is clear. Therefore we assume that $p \nmid ns(n-s)$. In particular $p > 2$.

Since $p \nmid sn(n-s)A$, $f'(X) = X^{s-1}(nX^{n-s} + sA)$ has no multiple factors mod p other than X. Hence, every irreducible factor of $f(X)$ (mod p) has multiplicity less than three. Let η be a multiple root of $f(X)$ (mod p) in an algebraic closure of $\mathbf{Z}/p\mathbf{Z}$. We have

$$\eta^{n-s} = -\frac{sA}{n} \quad \text{and} \quad \eta^s = -\frac{B}{\eta^{n-s}+A} = -\frac{nB}{(n-s)A},$$

hence $\eta \in \mathbf{Z}/p\mathbf{Z}$, since $(n-s, s) = (n, s) = 1$. If $\xi \in \mathbf{Z}/p\mathbf{Z}$ is another multiple root of $f(X)$ (mod p), from $(\xi/\eta)^s = (\xi/\eta)^{n-s} = 1$ and being $(s, n-s) = 1$ we conclude that $\xi = \eta$.

Therefore we have proved that if $p|D$ then the factorization of $f(X)$ into irreducible factors (mod p) is:

$$f(X) \equiv (X-\eta)^2\cdot\varphi_1(X)\cdot\ldots\cdot\varphi_r(X) \pmod p,$$

where the $\varphi_i(X)$ are all different. By Hensel's lemma $f(X)$ has a factorization in $\mathbf{Q}_p[X]$ which leads to $p = \mathfrak{a}\cdot\mathfrak{p}_1\cdot\ldots\cdot\mathfrak{p}_r$, where the $\mathfrak{p}_i$ are prime ideals of K with $N_{K/\mathbf{Q}}(\mathfrak{p}_i) = p^{\deg(\varphi_i(X))}$ and $\mathfrak{a}$ is an ideal of K with $N_{K/\mathbf{Q}}(\mathfrak{a}) = p^2$. Therefore, when $p|d$, p ramifies and the decomposition of p into a product of prime ideals of K must be

$$p = \mathfrak{p}^2\cdot\mathfrak{p}_1\cdot\ldots\cdot\mathfrak{p}_r,$$

with $N_{K/\mathbf{Q}}(\mathfrak{p}) = p$, and since $p > 2$ this implies that $v_p(d) = 1$. By (1) we distinguish this case from $v_p(d) = 0$ according to $v_p(D)$ being odd or even.

In the general case $(n, s) = m > 1$, we consider the polynomial

$$g(Y) = Y^{n'} + AY^{s'} + B.$$

If D' denotes the discriminant of $g(Y)$, we have $D = \pm B^{m-1}m^n(D')^m$, hence $v_p(D') = v_p(D)/m$. Since $g(X^m) = f(X)$, $g(Y)$ is irreducible over $\mathbf{Q}$ and $\omega = \theta^m$ is an algebraic integer of K which is a root of $g(Y)$. Let $L = \mathbf{Q}(\omega)$, we have

(6) $$d = (d')^m\cdot N_{L/\mathbf{Q}}(\mathscr{D}_{K/L}),$$

where d' denotes the discriminant of L and $\mathscr{D}_{K/L}$ the discriminant of K/L. For every prime ideal $\mathfrak{p}$ of L lying over p we have $m\omega \notin \mathfrak{p}$, since $p \nmid mB$. Hence the polynomial $X^m - \omega$ is separable (mod $\mathfrak{p}$) and $\mathfrak{p}$ is non-ramified in K/L. Therefore $p \nmid N_{L/\mathbf{Q}}(\mathscr{D}_{K/L})$ and $v_p(d) = m\cdot v_p(d')$. And we have already shown that $v_p(d') = 0$ or 1 according to $v_p(D')$ being even or odd.

4. The case $p|B$ and $M_p = 0$. For the proof of Theorem 1 in this case, we apply the results of the preceding section and the following lemma.

LEMMA 1. *Let L be a number field, r a positive integer and $\beta \in L$ an algebraic integer such that $g(X) = X^r - \beta$ is irreducible over L. Let η be a root of $g(X)$, $M = L(\eta)$ and $\mathscr{D}_{M/L}$ the discriminant of M/L. For every prime ideal $\mathfrak{p}$ of L not dividing $(r, v_\mathfrak{p}(\beta))$, we have*

$$v_\mathfrak{p}(\mathscr{D}_{M/L}) = r\cdot v_\mathfrak{p}(r) + r - (r, v_\mathfrak{p}(\beta)).$$

Proof. Let $\mathfrak{p}$ be a prime ideal of L and denote $\sigma = v_\mathfrak{p}(\beta)$ and $\tau = (r, \sigma)$. We prove the lemma first when $\tau = 1$. In this case $\mathfrak{p}$ is totally-ramified in M since if $\mathfrak{P}$ is any prime ideal of M lying over $\mathfrak{p}$ and $e = e(\mathfrak{P}/\mathfrak{p})$ denotes the ramification index, from $g(\eta) = 0$ we have,

$$r\cdot v_\mathfrak{P}(\eta) = v_\mathfrak{P}(\beta) = \sigma e,$$

hence r divides e. Therefore $e = r$, $\mathfrak{p} = \mathfrak{P}^r$ and $v_\mathfrak{P}(\eta) = \sigma$. Let $\pi \in \mathfrak{p}$ be such that $v_\mathfrak{p}(\pi) = 1$; let u, v be positive integers such that $\sigma u - rv = 1$ and let $\omega = \eta^u/\pi^v$. Since $(r, u) = 1$, we have $M = L(\eta^u) = L(\omega)$. Moreover, $\omega^r \in L$ and $h(X) = X^r - \omega^r$ is the minimal polynomial of ω over L. Now, if $\delta_{M/L}$ denotes the different of M/L, since $v_\mathfrak{P}(\omega) = 1$ we have,

$$v_\mathfrak{p}(\mathscr{D}_{M/L}) = v_\mathfrak{P}(\delta_{M/L}) = v_\mathfrak{P}(h'(\omega)) = v_\mathfrak{P}(r) + r - 1 = r\cdot v_\mathfrak{p}(r) + r - 1,$$

as required.

In the general case $\tau > 1$, we denote $r' = r/\tau$, $\sigma' = \sigma/\tau$, $\beta' = \beta/\pi^\sigma$ and $j(Y) = Y^\tau - \beta'$. Since $\pi^\sigma j(X^{r'}/\pi^{\sigma'}) = g(X)$, $j(Y)$ is irreducible over L and $\xi = \eta^{r'}/\pi^{\sigma'}$ is a root of $j(Y)$. Let $N = L(\xi)$. Clearly the minimal polynomial of η over N is $X^{r'} - \pi^{\sigma'}\xi$. Hence, we know that for every prime ideal $\mathfrak{P}$ of N lying over $\mathfrak{p}$,

$$v_\mathfrak{P}(\mathscr{D}_{M/N}) = r' v_\mathfrak{P}(r') + r' - 1,$$

since $v_\mathfrak{P}(\xi) = 0$ and $(r', \sigma') = 1$. On the other hand, since $v_\mathfrak{p}(\tau\beta') = 0$, $j(Y)$ is separable (mod $\mathfrak{p}$) and $\mathfrak{p}$ is not ramified in N/L, hence,

$$v_\mathfrak{P}(r') = v_\mathfrak{p}(r') = v_\mathfrak{p}(r) \quad \text{for all } \mathfrak{P}|\mathfrak{p},$$

and

$$v_\mathfrak{p}(\mathscr{D}_{M/L}) = v_\mathfrak{p}(N_{N/L}(\mathscr{D}_{M/N})) = \tau(r' v_\mathfrak{p}(r) + r' - 1) = r\cdot v_\mathfrak{p}(r) + r - \tau$$

and Lemma 1 is proved.

Suppose now that $M_p = 0$. Then $v_p(B) = n'u$ and $v_p(A) = (n'-s')u$, where u is a positive integer. We have $z_p = (m, u)$ and $b_p = n'z_p$. Let

$$g(Y) = Y^{n'} + A_p Y^{s'} + B_p.$$

Clearly, if D' denotes the discriminant of $g(Y)$, we have $v_p(D') = t_p$. Since $p^{v_p(B)} g(X^m/p^u) = f(X)$, $g(Y)$ is irreducible over $\boldsymbol{Q}$ and the algebraic integer of K, $\omega = \theta^m/p^u$ is a root of $g(Y)$. Let $L = \boldsymbol{Q}(\omega)$ and let d' be the discriminant of L. By the proof of Theorem 2, if $v_p(D')$ is even p is not ramified in L and if $v_p(D')$ is odd, the decomposition of p into prime ideals of L is

$$(7) \qquad p = \mathfrak{p}_1^2\cdot\mathfrak{p}_2\cdot\ldots\cdot\mathfrak{p}_r.$$

In any case, for every prime ideal $\mathfrak{p}$ of L lying over p, if $e_\mathfrak{p}$ denotes the ramification index $e_\mathfrak{p} = e(\mathfrak{p}/p)$, we have $\omega \notin \mathfrak{p}$ and

$$p \nmid (m, e_\mathfrak{p} u) = z_p\left(e_\mathfrak{p}, \frac{m}{z_p}\right),$$

since $p \nmid z_p$ by hypothesis, $e_\mathfrak{p} = 1$ or 2 and when $p = 2$, $v_2(D')$ is always zero. In this way we can apply Lemma 1 to $X^m - p^u\omega$, which is the minimal polynomial of θ over L and we have, if $\mathscr{D}_{K/L}$ denotes the discriminant of K/L,

$$(8) \qquad v_\mathfrak{p}(\mathscr{D}_{K/L}) = m\cdot v_\mathfrak{p}(m) + m - (m, e_\mathfrak{p} u),$$

for all $\mathfrak{p}|p$. The relation (6) holds and gives

$$(9) \qquad v_p(d) = m\cdot v_p(d') + v_p(N_{L/\boldsymbol{Q}}(\mathscr{D}_{K/L})).$$

Now, if $v_p(D')$ is even, $v_p(d') = 0$ and $e_\mathfrak{p} = 1$ for all $\mathfrak{p}|p$. By (8) and (9),

$$v_p(d) = n'(mv_p(m) + m - z_p) = n\cdot v_p(m) + n - b_p.$$

If $v_p(D')$ is odd, $v_p(d') = 1$ and by (7), (8) and (9) we have,

$$v_p(d) = n\cdot v_p(m) + n - b_p + 2z_p - z_p\left(2, \frac{m}{z_p}\right),$$

and the assertions of Theorem 1 are proved.

5. The case $p|B$ and $M_p \neq 0$. In this case we shall make use of a formula of Ore which computes $v_p(i(\theta))$ in terms of Newton's polygon of $f(X)$. We recall some definitions about Newton's polygon.

Let $g(X) = X^n + a_1 X^{n-1} + \ldots + a_n \in \boldsymbol{Z}[X]$ and let $p \in \boldsymbol{Z}$ be a prime number. The lower convex envelope of the set of points $\{(i, v_p(a_i)),\ 0 \leqslant i \leqslant n\}$ $(a_0 = 1)$ in the euclidean 2-space determines the so-called Newton's polygon of $f(X)$ with respect to p. Let $S_1, \ldots, S_k$ be the sides of the polygon and l_i, h_i the length of the projections of S_i to the X-axis and Y-axis, respectively. Let $\zeta_i = (l_i, h_i)$ and $l_i = \zeta_i\lambda_i$ for all i. If S_i begins in the point $(r, v_p(a_r))$ let $r_j = r + j\lambda_i$ and

$$b_j = \begin{cases} a_{r_j}/p^{v_p(a_{r_j})} & \text{if the point } (r_j, v_p(a_{r_j})) \text{ belongs to } S_i, \\ 0 & \text{otherwise,} \end{cases}$$

for all $0 \leqslant j \leqslant \zeta_i$. The polynomial

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

is called the "associated polynomial of S_i". We define $g(X)$ to be "p-regular" if p does not divide the discriminant of any of the polynomials $g_1(Y), \ldots, g_k(Y)$. In the regular case, the shape of the polygon determines $v_p(i(\omega))$, being ω a root of $g(X)$:

THEOREM 3 (Ore [3], th. 8). *Let $g(X) \in \mathbf{Z}[X]$ be a monic irreducible polynomial and let $L = \mathbf{Q}(\omega)$, where ω is a root of $g(X)$. If $p \in \mathbf{Z}$ is a prime such that $g(X)$ is p-regular* [1] *then*

$$v_p(i(\omega)) = \sum_{i=2}^{k} l_i \Big(\sum_{j=1}^{i-1} h_j\Big) + \tfrac{1}{2} \sum_{i=1}^{k} (l_i h_i - l_i - h_i + \zeta_i),$$

and this is also the number of points with integer coordinates below Newton's polygon of $g(X)$ with respect to p, except for the points on the X-axis and on the last ordinate.

Suppose now that $M_p \neq 0$. Newton's polygon of $f(X)$ with respect to p has one or two sides according to $M_p < 0$ or $M_p > 0$. The associated polynomials are, respectively,

$$Y^{b_p} + B_p \qquad \text{if} \quad M_p < 0,$$

$$Y^{a_p} + A_p \quad \text{and} \quad A_p Y^{c_p} + B_p \qquad \text{if} \quad M_p > 0.$$

Hence, $f(X)$ is p-regular if and only if

(10) $$p \nmid b_p \quad \text{if} \quad M_p < 0, \qquad \text{or} \qquad p \nmid a_p c_p \quad \text{if} \quad M_p > 0.$$

Under these assumptions, by Theorem 3 we have

$$2v_p(i(\theta)) = \begin{cases} (n-1)v_p(B) - n + b_p & \text{if} \quad M_p < 0, \\ nv_p(A) - n + (s-1)v_p(B) + a_p + c_p & \text{if} \quad M_p > 0. \end{cases}$$

Moreover, if we denote,

$$S = n' v_p(n') + (n'-s') v_p(B),$$

$$T = s' v_p(s') + (n'-s') v_p(n'-s') + n' v_p(A),$$

the conditions (10) of p-regularity imply in any case that $S \neq T$, so that always

$$v_p(D) = (s-1) v_p(B) + n v_p(m) + m \cdot \inf\{S, T\},$$

[1] Although our definition of p-regularity is more restrictive than Ore's, which involves all the irreducible factors $(\bmod p)$ of $g(X)$, it is enough for our purposes. Anyway Theorem 3 is valid as stated.

and $v_p(d) = v_p(D) - 2v_p(i(\theta))$ has the desired values. There is one case left with $M_p \neq 0$; when $p \mid \dfrac{n}{b_p}$ and $-M_p = b_p$. In this case $p = \mathfrak{a}^{n/b_p}$ for some ideal in K since Newton's polygon has only one side with slope $v_p(B)/n$ ([3], th. 1). Hence, p is wildly-ramified in K and $v_p(d) \geqslant n$. On the other hand, it is easy to see that in this case $p \nmid m$ and $v_p(D) = (s-1)v_p(B) + nv_p(A)$. Being always $2v_p(i(\theta)) \geqslant (n-1)v_p(B) - n + b_p$, we have $v_p(d) \leqslant n$, so that $v_p(d) = n$ as desired.

References

[1] K. Komatsu, *Integral bases in algebraic number fields*, J. Reine Angew. Math. 278/279 (1975), pp. 137–144.

[2] P. Llorente and E. Nart, *Effective determination of the decomposition of the rational primes in a cubic field*, Proc. Amer. Math. Soc. 87 (1983), pp. 579–585.

[3] Ö. Ore, *Newtonsche Polygone in der Theorie der algebraischen Körper*, Math. Ann. 99 (1928), pp. 84–117.

[4] R. G. Swan, *Factorization of polynomials over finite fields*, Pacific J. Math. 12 (1962), pp. 1099–1106.

SECCIÓ DE MATEMÀTIQUES
UNIVERSITAT AUTÒNOMA DE BARCELONA
Bellaterra, Barcelona, Catalunya, Espanya

Received on 15.6.1982
and in revised form on 22.12.1982 (1311)