View metadata, citation and similar papers at core.ac.uk
brought to you by CORE
provided by Elsevier - Publisher Connector

Journal of Number Theory **96**, 319–325 (2002)
doi:10.1006/jnth.2002.2796

On Computing Discriminants of Subfields of $\mathbb{Q}(\zeta_{p^r})$

Trajano Pires da Nóbrega Neto[1,2] and J. Carmelo Interlando

Departamento de Matemática, Universidade Estadual Paulista,
15054-000 São José do Rio Preto, SP, Brazil
E-mail: trajano@mat.ibilce.unesp.br, interlando.2@nd.edu

and

José Othon Dantas Lopes

Departamento de Matemática, Universidade Federal do Ceará, 60455-760 Fortaleza, CE, Brazil
E-mail: othon@mat.ufc.br

Communicated by M. Pohst

Received May 30, 2001; revised September 11, 2001

The conductor–discriminant formula, namely, the Hasse Theorem, states that if a number field K is fixed by a subgroup H of $\mathrm{Gal}(\mathbb{Q}(\zeta_n)/\mathbb{Q})$, the discriminant of K can be obtained from H by computing the product of the conductors of all characters defined modulo n which are associated to K. By calculating these conductors explicitly, we derive a formula to compute the discriminant of any subfield of $\mathbb{Q}(\zeta_{p^r})$, where p is an odd prime and r is a positive integer. © 2002 Elsevier Science (USA)

Key Words: characters; conductors; cyclotomic fields; discriminants of number fields; Hasse Theorem.

1. INTRODUCTION

One of the most important invariants of an algebraic number field K is its discriminant, denoted by $\mathrm{Disc}(K)$. In this paper, we are concerned with discriminants of subfields of $\mathbb{Q}(\zeta_{p^r})$ where p is an odd prime and r is a positive integer. For any number field $K \subset \mathbb{Q}(\zeta_{p^r})$, we obtain a closed-form formula to compute $\mathrm{Disc}(K)$ as a function of p and $[K:\mathbb{Q}]$ only. For each divisor d of $\phi(p^r)$, there is a unique subfield K of $\mathbb{Q}(\zeta_{p^r})$ of degree d. Such field K is fixed by exactly one subgroup H of $\mathrm{Gal}(\mathbb{Q}(\zeta_{p^r})/\mathbb{Q})$. Our first task will be to characterize the conductors of Dirichlet characters (Lemma 3.2) and then to calculate them explicitly (Lemma 3.3). From these results, the formula for $\mathrm{Disc}(K)$ is obtained using the Hasse Theorem, which states that

[1] To whom correspondence should be addressed.
[2] Supported in part by the Department of Mathematics of the Federal University of Ceará, Fortaleza, Brazil, and in part by CAPES, Brazil, through PROCAD 0121/01-0.

0022-314X/02 $35.00
© 2002 Elsevier Science (USA)
All rights reserved.

if K is fixed by a subgroup H of $\mathrm{Gal}(\mathbb{Q}(\zeta_n)/\mathbb{Q})$, the discriminant of K is equal to the product of the conductors of all characters associated to K [7].

2. CHARACTERS AND CONDUCTORS

A character of a finite Abelian group G is a homomorphism from G into $\mathbb{C}^*$ [1, 7]. A Dirichlet character defined modulo m is a multiplicative homomorphism $\chi : (\mathbb{Z}/m\mathbb{Z})^* \to \mathbb{C}^*$. If m divides n, χ induces a character modulo n by composition with the natural map $(\mathbb{Z}/n\mathbb{Z})^* \to (\mathbb{Z}/m\mathbb{Z})^*$. Therefore, we can regard the same character defined as either modulo m or modulo n since they are essentially the same map. It is convenient to choose n minimal and call it the conductor of χ, denoted by f_χ. It is sometimes advantageous to think of Dirichlet characters as being characters of Galois groups of cyclotomic fields. If we identify $\mathrm{Gal}(\mathbb{Q}(\zeta_n)/\mathbb{Q})$ with $(\mathbb{Z}/n\mathbb{Z})^*$, then a Dirichlet character modulo n is a Galois character [7]. In general, if χ is a character modulo n, then χ is a character of $\mathrm{Gal}(\mathbb{Q}(\zeta_n)/\mathbb{Q})$. If K is the fixed field of the kernel of χ, then $K \subseteq \mathbb{Q}(\zeta_n)$, and if n is minimal, then $n = f_\chi$. The field K is exclusively dependent on χ and is called the field belonging to χ. More generally, if X is a finite group of Dirichlet characters and n is the least common multiple of the conductors of the characters in X, then X is a subgroup of the characters of $\mathrm{Gal}(\mathbb{Q}(\zeta_n)/\mathbb{Q})$. If H is the intersection of the kernel of these characters and K is the fixed field of H, then X is precisely the set of all homomorphisms from $\mathrm{Gal}(K/\mathbb{Q})$ to $\mathbb{C}^*$. The field K is called the field belonging to X, and we have $[K : \mathbb{Q}] =$ order of X. If X is cyclic and generated by χ, then K is precisely the same field belonging to χ.

3. PRELIMINARIES

In this section, we present the supporting lemmas to obtain the main result.

Given an odd prime p and a positive integer r, $(\mathbb{Z}/p^r\mathbb{Z})^*$ is a cyclic multiplicative group [3]. By Galois Theory, given a divisor d of $\phi(p^r) = (p-1)p^{r-1}$, there is a unique subfield K of $\mathbb{Q}(\zeta_{p^r})$ fixed by a subgroup of $(\mathbb{Z}/p^r\mathbb{Z})^*$ of order d [5].

LEMMA 3.1. *Let p be an odd prime number, r a positive integer, and g an integer such that $\bar{g} = g \bmod p^r$ is a generator of $(\mathbb{Z}/p^r\mathbb{Z})^*$. Then for $0 < j \leqslant r$, $g^k \equiv 1 \pmod{p^j}$ if and only if $k \equiv 0 \pmod{(p-1)p^{j-1}}$.*

Proof. If $g^k = 1 + p^j t$, then $g^{kp} = 1 + p^{j+1} t_1$ where t and t_1 are integers. Repeating this reasoning, we have $g^{kp^{r-j}} = 1 + p^r t_{r-j}$ where t_{r-j} is an integer. With this, if $g^k \equiv 1 \pmod{p^j}$, then $g^{kp^{r-j}} \equiv 1 \pmod{p^r}$ and therefore

$(p-1)p^{r-1}$ divides kp^{r-j}, that is, $k \equiv 0 \pmod{(p-1)p^{j-1}}$. Conversely, suppose $k \equiv 0 \pmod{(p-1)p^{j-1}}$. Then $(\mathbb{Z}/p^j\mathbb{Z})^*$ has order $(p-1)p^{j-1}$; since g and p are relatively prime, $g^k \equiv 1 \pmod{p^j}$, concluding the proof. ∎

LEMMA 3.2. *Let n and m be positive integers and χ a Dirichlet character defined modulo n. The conductor of χ is m if and only if m is the least integer dividing n and the following condition holds true*: $\forall a \in \mathbb{Z}$ *with* $(a,n)=1$, *if* $a \equiv 1 \pmod{m}$, *then* $\chi(\bar{a}) = 1$.

Proof. Suppose m is the conductor of χ and $a \in \mathbb{Z}$ is such that $(a,n)=1$. Since $a \equiv 1 \pmod{m}$, $(a,n)=1$, and χ can be defined modulo m, then $(a,m)=1$ and $\chi(\bar{a})=1$. Conversely, let a and b be relatively prime to n, and consequently, relatively prime to m. If $a \equiv b \pmod{m}$, then $ab^{-1} \equiv 1 \pmod{m}$ and thus $\chi(\overline{ab^{-1}}) = 1$, that is, $\chi(\bar{a}) = \chi(\bar{b})$. Since m is the least divisor of n with the above property, then by definition it is the conductor of χ. ∎

Let p be an odd number, r a positive integer, g an integer such that $\bar{g} = g \bmod p^r$ is a generator of $(\mathbb{Z}/p^r\mathbb{Z})^*$, and $\chi : (\mathbb{Z}/p^r\mathbb{Z})^* \to \mathbb{C}^*$ a Dirichlet character. Given that there are exactly n characters over an Abelian group of order n, there are $(p-1)p^{r-1}$ Dirichlet characters χ defined over $(\mathbb{Z}/p^r\mathbb{Z})^*$, and each character is completely determined by its image in $\bar{g}$ [7]. On the other hand, $1 = \chi(\bar{I}) = \chi(\bar{g}^{(p-1)p^{r-1}}) = \chi(\bar{g})^{(p-1)p^{r-1}}$, that is, $\chi(\bar{g})$ is a $(p-1)p^{r-1}$th root of unity [3]. With this, given a character χ defined modulo p^r, there is an integer i where $0 \leqslant i < (p-1)p^{r-1}$ such that $\chi(\bar{g}) = \zeta^i_{(p-1)p^{r-1}}$. Considering the number of characters and the possibilities for the integer i, we can conclude that all Dirichlet characters defined modulo p^r are of the form $\chi_i(\bar{g}) = \zeta^i_{(p-1)p^{r-1}}$, $i = 0, \ldots, (p-1)p^{r-1}-1$.

LEMMA 3.3. *With the above notation, let i be an integer such that $0 \leqslant i < (p-1)p^{r-1}$. Then $p^j = (i, p^r)$ if and only if the conductor f_{χ_i} of χ_i is p^{r-j}.*

Proof. For $i=0$, the result is straightforward. Suppose then that $i \neq 0$ and $p^j = (i,p^r)$. So, $i = p^j t$ for some positive integer t. Let $\mathscr{H} = \{\bar{g}^a \in (\mathbb{Z}/p^r\mathbb{Z})^*; g^a \equiv 1 \pmod{p^{r-j}}\}$. From Lemma 3.2, χ_i can then be defined modulo p^{r-j} if and only if $\chi_i(x) = 1, \forall x \in \mathscr{H}$. By Lemma 3.1, $\mathscr{H} = \langle \bar{g}^{(p-1)p^{r-j-1}} \rangle$, and because $\chi_i(\bar{g}^a) = \zeta^{ai}_{(p-1)p^{r-1}}$, one has $\chi_i(\bar{g}^{(p-1)p^{r-j-1}}) = 1$. For the converse, suppose χ_i can be defined modulo p^{r-j}. Then $\chi_i(x) = 1, \forall x \in \mathscr{H}$, and, in particular, $\chi_i(\bar{g}^{(p-1)p^{r-j-1}}) = 1$. Since $\chi_i(\bar{g}^{(p-1)p^{r-j-1}}) = \zeta^{i(p-1)p^{r-j-1}}_{(p-1)p^{r-1}}$, there is an integer t such that $i(p-1)p^{r-j-1} = (p-1)p^{r-1}t$, which implies that $i = p^j t$. In summary, $i = p^j t$ if and only if χ_i can be defined modulo p^{r-j}, which is equivalent to saying that the conductor of χ_i is p^{r-j} if p^j is the greatest power of p which divides i, that is, $p^j = (i, p^r)$. ∎

Given an integer n and the field $L = \mathbb{Q}(\zeta_n)$, L is a Galois extension of the field of rational numbers, with the Galois group isomorphic to $(\mathbb{Z}/n\mathbb{Z})^*$. From the Fundamental Theorem of Galois Theory [5], it follows that there exists a one-to-one correspondence between the subgroups of $(\mathbb{Z}/n\mathbb{Z})^*$ and the subfields of L. The isomorphism between the Galois group and $(\mathbb{Z}/n\mathbb{Z})^*$ is determined by associating the automorphism σ_i of L (taking ζ_n in ζ_n^i) to each integer i in $(\mathbb{Z}/n\mathbb{Z})^*$. Then we can define a character χ acting on the automorphisms of L, where $\chi(\sigma_i)$ means $\chi(i)$.

With the above notation, if K is the subfield of L fixed by H, we say that the character χ is associated to K if $\chi(\sigma) = 1$ for all σ in H. As an example, if $K = L$, the subgroup H that fixes K is the identity σ_1 of L. It is easy to see that $\chi(\sigma_1) = 1$ for all χ defined modulo n, and therefore all the characters are associated to L. Also, if K is the field of rational numbers, then the only character associated to K is the trivial one.

THEOREM 3.1 (Washington [7]). *Let n be a positive integer, $L = \mathbb{Q}(\zeta_n)$, H a subgroup of the group of the automorphisms of L, and K the subfield of L fixed by H. Then the discriminant of the field K is, up to sign, the product of the conductors of the characters defined modulo n which are associated to K.*

4. MAIN RESULT

Let p be an odd prime number, r a positive integer, and $L = \mathbb{Q}(\zeta_{p^r})$. Because L is a Galois extension of the rationals whose Galois group is isomorphic to $(\mathbb{Z}/p^r\mathbb{Z})^*$, a cyclic group, there is a one-to-one correspondence between the subfields of L and the divisors of $(p-1)p^{r-1}$, the degree of L. In the next theorem, we calculate the discriminant of any subfield K of L as a function of p and its degree only. Since the degree of K is a divisor of $(p-1)p^{r-1}$, we write $[K:\mathbb{Q}] = up^j$, where u is a divisor of $p-1$, and $j \leqslant r-1$.

THEOREM 4.1. *Let K be a subfield of $\mathbb{Q}(\zeta_{p^r})$ with $[K:\mathbb{Q}] = up^j$ where p does not divide u. Then* $\mathrm{Disc}(K) = p^{u((j+2)p^j - \frac{p^{j+1}-1}{p-1})-1}$.

Proof. Observe that $G = \mathrm{Gal}(\mathbb{Q}(\zeta_{p^r})/\mathbb{Q})$ is a cyclic group of order $(p-1)p^{r-1}$. Let $g \in \mathbb{Z}$ be such that its class $\bar{g}$ is a generator of $(\mathbb{Z}/p^r\mathbb{Z})^*$. So if $[K:\mathbb{Q}] = up^j$, then the subgroup H of G that fixes K is cyclic of order $(p-1)p^{r-j-1}/u$. If σ_a is a generator of H, we conclude that a character χ defined modulo p^r is associated to K if and only if $\chi(\sigma_a) = 1$. Since the order of a modulo p^r is equal to the order of H, that is, $(p-1)p^{r-j-1}/u$, we can assume $a \equiv g^d \pmod{p^r}$ with $d = up^j$ without loss of generality. Therefore, given a character χ_i defined modulo p^r, $\chi_i(\bar{a}) = 1$, namely, χ_i is associated to K if and only if $di \equiv 0 \pmod{(p-1)p^{r-1}}$ or, equivalently, if and only if

TABLE I

Number of χ_i Associated to K Having Conductor f_{χ_i}

ℓ	Number of χ_i	$f_{\chi_i} = p^{j+1-\ell}$
0	$up^{j-1}(p-1)$	p^{j+1}
1	$up^{j-2}(p-1)$	p^j
$\vdots$	$\vdots$	$\vdots$
$j-1$	$up^0(p-1)$	p^2
j	$u-1$	p

$i = (p-1)p^{r-1}t/d,\ t = 0, \ldots, d-1$ (recall that $\chi_i(\bar{g}) = \zeta^i_{(p-1)p^{r-1}}$; thus $\chi_i(\bar{a}) = \zeta^{di}_{(p-1)p^{r-1}}$). Since $d = up^j$, $\chi_i(\bar{a}) = 1$ if and only if $i = \frac{p-1}{u}p^{r-j-1}t$ where $t = 0, \ldots, up^j - 1$.

If $t = 0$, then $i = 0$; according to Lemma 3.3, $f_{\chi_i} = 1$. If $t \neq 0$, let $t = p^\ell t_k$, where ℓ is an integer in $[0, j]$, and $(t_k, p) = 1$. Note that for each $\ell \in [0, j-1]$, there are $up^{j-\ell-1}(p-1)$ elements t_k in these conditions. From Lemma 3.3, the conductors of the corresponding χ_i are all equal to $p^{j+1-\ell}$. If $\ell = j$, there are $u-1$ elements t_k with $(t_k, p) = 1$, and the conductors of the corresponding χ_i are all equal to p. Table I summarizes these results. The first column displays each possible value for ℓ; the second, the number of (nontrivial) characters χ_i for which $i = \frac{p-1}{u}p^{r-j-1+\ell}t_k$ and $(t_k, p) = 1$; the third column lists the common conductor of these characters χ_i. Note that except for the trivial character, all the others that are associated to K are counted in Table I.

From Theorem 3.1, the discriminant of K is, up to sign, equal to the product of the conductors of the characters χ_i that are associated to K. Using this and the results in Table I, we obtain

$$\mathrm{Disc}(K) = \prod_{i;\chi_i \text{ is assoc. to } K} f_{\chi_i} = p^\alpha,$$

where α is computed as the sum of the second column entries times $\log_p$ of the third column entries. Hence,

$$\begin{aligned}
\alpha &= u(p-1)((j+1)p^{j-1} + jp^{j-2} + \cdots + 2p^0) + u - 1 \\
&= \frac{u(p-1)}{p} \sum_{i=0}^{j} (i+1)p^i - \frac{u(p-1)}{p} + u - 1 \\
&= \frac{u(p-1)}{p} \frac{d}{dp}\left(\frac{p^{j+2}-1}{p-1}\right) + \frac{u}{p} - 1 \\
&= \frac{u(p-1)}{p}\left(\frac{(j+2)p^{j+1}(p-1) - (p^{j+2}-1)}{(p-1)^2}\right) + \frac{u}{p} - 1.
\end{aligned}$$

This implies that

$$\alpha = u\left((j+2)p^j - \frac{p^{j+2}-1}{p(p-1)} + \frac{1}{p}\right) - 1,$$

and therefore,

$$\alpha = u\left((j+2)p^j - \frac{p^{j+1}-1}{p-1}\right) - 1. \quad \blacksquare$$

COROLLARY 4.1 (Washington [7]). *Given positive integers p and r with p an odd prime, the discriminant of the cyclotomic field $\mathbb{Q}(\zeta_{p^r})$ is, up to sign, equal to $p^{(p-1)((r+1)p^{r-1}-(p^r-1)/(p-1))-1}$.*

COROLLARY 4.2. *If p is an odd prime and $K \subset \mathbb{Q}(\zeta_p)$, then* $\mathrm{Disc}(K) = \pm p^{[K:\mathbb{Q}]-1}$.

Remark 4.1. Note that the main result in this paper, Theorem 4.1, was possible due to the following: Given an odd prime p, a positive integer r, and the cyclotomic field $F = \mathbb{Q}(\zeta_{p^r})$, the divisors of $\phi(p^r)$ are in a one-to-one correspondence with the subfields of F. Hence, for each $d = up^j$ where $j = 0, \ldots, r-1$, there is exactly one subfield K of $\mathbb{Q}(\zeta_{p^r})$ with degree d. In this way, the discriminant of K can be obtained as a function of its degree.

On the other hand, for more general cyclotomic extensions, say of the form $\mathbb{Q}(\zeta_n)$ where n is any positive integer, there may be two or more subfields with a given degree that have different discriminants. In other words, the extension of the results in this paper depends on determining the other properties (besides the degree) which specify a given subfield of $\mathbb{Q}(\zeta_n)$ and therefore, its discriminant.

ACKNOWLEDGMENTS

The authors sincerely thank the referee for very careful reading of the manuscript, for appreciating their work, and for pointing out several mistakes. All of the suggestions made (in particular, those to the proofs of Lemma 3.3 and Theorem 4.1) have greatly improved the readability of the paper.

REFERENCES

1. Z. I. Borevich and I. R. Shafarevich, "Number Theory," Academic Press, New York, 1966.

2. Deleted in proof.
3. J. J. Rotman, "An Introduction to the Theory of Groups," 4th ed., Springer-Verlag, New York, 1995.
4. Deleted in proof.
5. I. N. Stewart, "Galois Theory," 2nd ed., Chapman & Hall/CRC Press, London/Boca Raton, FL, 1990.
6. Deleted in proof.
7. L. C. Washington, "Introduction to Cyclotomic Fields," Springer-Verlag, New York, 1982.