Canad. Math. Bull.Vol. **36** (1), 1993 pp. 103–107

DISCRIMINANTS OF METACYCLIC FIELDS

DANIEL C. MAYER

ABSTRACT. Some formulas for multiplicities of pure cubic discriminants are generalized to the case of a pure field of arbitrary odd prime degree.

Introduction. By a *metacyclic* field we understand the normal field of a pure field $\mathbb{Q}(\sqrt[p]{D})$ of odd prime degree p, which is generated by the unique real solution of a *pure* equation $X^p - D = 0$ $(D \in \mathbb{Z})$ and is a non-Galois algebraic number field with $p-1$ complex isomorphic fields all of whose arithmetical invariants coincide, in particular their discriminants.

However, there are also examples of non-isomorphic pure fields which share a common discriminant, and it is the purpose of the present note to determine the exact number of all non-isomorphic pure fields with a foregiven discriminant, which is called the *multiplicity* of that discriminant. Making use of a theorem on the connection between the discriminant and the radicand D by W. E. H. Berwick [1], we generalize the formulas for multiplicities of pure cubic discriminants, which were given in a recent paper [2], to the case of a pure field of arbitrary odd prime degree.

1. **Radicands and conductors.** Let p be an odd rational prime, $q_1, \ldots, q_s$ pairwise distinct primes (with $s \geq 1$ and p may be among them), $D = q_1^{e_1} \cdots q_s^{e_s}$ a p-th power free radicand with integer exponents $1 \leq e_i \leq p-1$ $(i = 1, \ldots, s)$, and $L = \mathbb{Q}(\sqrt[p]{D})$ the pure field of degree p with radicand D.

Then the normal field N of L is the compositum $\mathbb{Q}(\zeta, \sqrt[p]{D})$ of the cyclotomic field $k = \mathbb{Q}(\zeta)$ of p-th roots of unity ζ with L. N is a metacyclic field of degree $p(p-1)$ whose Galois group $\mathrm{Gal}(N/\mathbb{Q})$ is the semidirect product of two cyclic groups $C(p) \rtimes C(p-1)$.

W. E. H. Berwick [1] has proved the following relationship between the radicand D of a pure field $L = \mathbb{Q}(\sqrt[p]{D})$ and the conductor f of the corresponding cyclic relative extension N/k of degree p.

THEOREM 1. *If $R = q_1 \cdots q_s$ denotes the square free product of all prime divisors of the radicand D of the pure field $L = \mathbb{Q}(\sqrt[p]{D})$, then the associated conductor f satisfies the relation*

$$f^{p-1} = \begin{cases} p^2 R^{p-1} & \text{if } D^{p-1} \not\equiv 1 \pmod{p^2} \quad \textit{(field of the 1st kind)}, \\ R^{p-1} & \text{if } D^{p-1} \equiv 1 \pmod{p^2} \quad \textit{(field of the 2nd kind)}. \end{cases}$$

Research supported by the Austrian Science Foundation, Project Nr. J0497-PHY.
Received by the editors August 14, 1991; revised November 26, 1991.
AMS subject classification: Primary: 11R20.
Key words and phrases: metacyclic fields, discriminants, pure fields of prime degree.

Consequently, since

$$d_L = d_k \cdot f^{p-1},$$
$$d_N = d_k^p \cdot f^{(p-1)^2}, \text{ and}$$
$$d_k = (-1)^{\frac{p-1}{2}} p^{p-2},$$

the discriminants of L and N are given by

$$d_L = (-1)^{\frac{p-1}{2}} \cdot \begin{cases} p^p R^{p-1} & \text{if } D^{p-1} \not\equiv 1 (\operatorname{mod} p^2), \\ p^{p-2} R^{p-1} & \text{if } D^{p-1} \equiv 1 (\operatorname{mod} p^2), \end{cases}$$
$$d_N = (-1)^{\frac{p-1}{2}} \cdot \begin{cases} p^{p^2-2} R^{(p-1)^2} & \text{if } D^{p-1} \not\equiv 1 (\operatorname{mod} p^2), \\ p^{(p-2)p} R^{(p-1)^2} & \text{if } D^{p-1} \equiv 1 (\operatorname{mod} p^2). \end{cases}$$

2. **Multiplicities of metacyclic discriminants.** We call the number $m(f)$ of pure fields $L = \mathbb{Q}(\sqrt[p]{D})$ sharing the same associated conductor f (and thus also the same discriminant d_L) the *multiplicity* of f. With the aid of Berwick's result and the technique of [2], we obtain the complete solution of the multiplicity problem for discriminants of pure fields of odd prime degree.

THEOREM 2. *Let $f = p^e \cdot q_1 \cdots q_t > 1$ be the conductor associated with a pure field $L = \mathbb{Q}(\sqrt[p]{D})$ of odd prime degree p, i.e., $e \in \{0, \frac{2}{p-1}, \frac{p+1}{p-1}\}$, $t \geq 0$, and the q_i are pairwise distinct rational primes different from p, for $i = 1, \ldots, t$. Put*

$$u = \#\{1 \leq i \leq t \mid q_i^{p-1} \equiv 1 (\operatorname{mod} p^2)\},$$
$$v = \#\{1 \leq i \leq t \mid q_i^{p-1} \not\equiv 1 (\operatorname{mod} p^2)\}.$$

Then the multiplicity $m(f)$ of the discriminant $d_L = (-1)^{\frac{p-1}{2}} p^{p-2} \cdot f^{p-1}$ can be expressed by the formulas

$$m(f) = \begin{cases} (p-1)^t & \text{if } e = \frac{p+1}{p-1}, \text{ i.e., } p \mid D, \\ (p-1)^u \cdot X_v & \text{if } e = \frac{2}{p-1}, \text{ i.e., } D^{p-1} \not\equiv 1 (\operatorname{mod} p^2),\ p \nmid D, \\ (p-1)^u \cdot X_{v-1} & \text{if } e = 0, \text{ i.e., } D^{p-1} \equiv 1 (\operatorname{mod} p^2), \end{cases}$$

where $X_j = \frac{1}{p}\big((p-1)^j - (-1)^j\big)$ for all $j \geq -1$.

Moreover, the multiplicities of conductors with p-exponents $e = 0, \frac{2}{p-1}$ satisfy the equation

$$m(q_1 \cdots q_t) + m(p^{\frac{2}{p-1}} \cdot q_1 \cdots q_t) = (p-1)^{t-1}.$$

EXAMPLE. As an illustration, let us take $p = 5$. In this case, the sequence $(X_j)_{j \geq -1}$ is given by $(\frac{1}{4}, 0, 1, 3, 13, 51, \ldots)$, and the sequence of rational primes q satisfying $q^4 \equiv 1 (\operatorname{mod} 25)$ (or, equivalently, $q \equiv \pm 1, \pm 7 (\operatorname{mod} 25)$) starts with $7, 43, 101, 107, \ldots$.

Theorem 2 tells us that examples of pure quintic discriminants $d_L = d_k \cdot f^4$ of multiplicity 3 can be constructed by taking conductors f with $u = 0$ and $v = 2$, such that $e = \frac{1}{2}$, *i.e.*, such that $D^4 \not\equiv 1 (\mathrm{mod}\, 25)$ and $5 \not| D$.

We obtain the first occurrence of three non-isomorphic pure quintic fields $L = \mathbb{Q}(\sqrt[5]{D})$ sharing a common discriminant by selecting the two smallest possible conductor prime factors distinct from 5 and not belonging to the sequence $(7, 43, \ldots)$, that is, $q_1 = 2$, $q_2 = 3$, and $f = 5^{\frac{1}{2}} \cdot 2 \cdot 3$. The discriminant is therefore $d_L = +125 \cdot (25 \cdot 16 \cdot 81) = 4\,050\,000$.

The technique in the subsequent proof of Theorem 2 will show how to get the normalized radicands D of the corresponding pure quintic fields by raising various power products of 2 and 3 to successive powers and reducing the exponents modulo 5:

$$\begin{array}{cccc} 2 \cdot 3, & 2^2 \cdot 3^2, & 2^3 \cdot 3^3, & 2^4 \cdot 3^4; \\ 2^2 \cdot 3, & 2^4 \cdot 3^2, & 2 \cdot 3^3, & 2^3 \cdot 3^4; \\ 2^3 \cdot 3, & 2 \cdot 3^2, & 2^4 \cdot 3^3, & 2^2 \cdot 3^4; \\ 2^4 \cdot 3, & 2^3 \cdot 3^2, & 2^2 \cdot 3^3, & 2 \cdot 3^4. \end{array}$$

The minima of the rows are 6, 12, 18, and 48. However, $D = 18 \equiv -7 (\mathrm{mod}\, 25)$ is the radicand of a single field of the second kind. Hence, the desired three pure quintic fields with the coinciding minimal discriminant 4 050 000 are

$$\mathbb{Q}(\sqrt[5]{6}), \quad \mathbb{Q}(\sqrt[5]{12}), \quad \mathbb{Q}(\sqrt[5]{48}).$$

They are all of the first kind. Here, we have $t = u + v = 2$ and the relation

$$m(6) + m(5^{\frac{1}{2}} \cdot 6) = 1 + 3 = 4 = (p-1)^{t-1}.$$

Numerous examples for higher multiplicities of discriminants of pure cubic fields, the case $p = 3$, can be found in [2].

PROOF. First observe that every field $L = \mathbb{Q}(\sqrt[p]{D})$ can be generated by $p - 1$ different radicals without rational divisors. The corresponding p-th power free radicands differ from $D, D^2, \ldots, D^{p-1}$ only by complete p-th powers and are obtained by reduction of the involved exponents modulo p. The smallest one among them will be called the *normalized* radicand of L.

The case $e = \frac{p+1}{p-1}$ is treated separately. $f = p^{\frac{p+1}{p-1}} \cdot q_1 \cdots q_t$ is equivalent to $f = p^{\frac{2}{p-1}} R$, $p | R$, and thus also to $D \equiv 0 (\mathrm{mod}\, p)$. In this case, there are $(p-1)^{t+1}$ choices for the exponent systems $1 \leq w_0, w_1, \ldots, w_t \leq p - 1$ in p-th power free radicands $D = p^{w_0} \cdot q_1^{w_1} \cdots q_t^{w_t}$ which all share the same value of $R = p \cdot q_1 \cdots q_t$. But only the $(p-1)$-st part of all systems $(w_0, \ldots, w_t)$ belongs to normalized radicands. Hence,

$$m(p^{\frac{p+1}{p-1}} \cdot q_1 \cdots q_t) = \frac{1}{p-1}(p-1)^{t+1} = (p-1)^t.$$

Now, the cases $e = \frac{2}{p-1}$ and $e = 0$ are investigated simultaneously. $f = p^{\frac{2}{p-1}} \cdot q_1 \cdots q_t$ is equivalent to $f = p^{\frac{2}{p-1}} R$, $p \not| R$, and further to $D^{p-1} \not\equiv 1 (\mathrm{mod}\, p^2)$, whereas $f = q_1 \cdots q_t$ is equivalent to $f = R$, $p \not| R$, and also to $D^{p-1} \equiv 1 (\mathrm{mod}\, p^2)$. In both cases, there are

https://doi.org/10.4153/CMB-1993-015-x Published online by Cambridge University Press

$(p-1)^t$ choices for exponents $1 \leq w_1, \ldots, w_t \leq p-1$ in p-th power free radicands $D = q_1^{w_1} \cdots q_t^{w_t}$ which all share the same value of $R = q_1 \cdots q_t$, but some of them (those with $D^{p-1} \equiv 1 (\mathrm{mod}\, p^2)$) belong to the conductor $f = R$ and the others (with $D^{p-1} \not\equiv 1 (\mathrm{mod}\, p^2)$) to the conductor $f = p^{\frac{2}{p-1}} R$. Again, only the $(p-1)$-st part of the systems $(w_1, \ldots, w_t)$ belongs to normalized radicands. (The normalized radicand and the non-normalized radicands of a given pure field are all of the same kind.) Therefore,

$$m(q_1 \cdots q_t) + m(p^{\frac{2}{p-1}} \cdot q_1 \cdots q_t) = \frac{1}{p-1}(p-1)^t = (p-1)^{t-1}.$$

To separate these two multiplicities it is convenient to fix a value $u \geq 0$ of the number of prime divisors q with $q^{p-1} \equiv 1 (\mathrm{mod}\, p^2)$ of D and to argue by induction with respect to the number $v \geq 0$ of prime divisors q with $q^{p-1} \not\equiv 1 (\mathrm{mod}\, p^2)$ of D. Then $u + v = t$, since $p \not| D$, in the present situation.

To start the induction we must consider the two values $v = 0$ and $v = 1$.

In the case $v = 0$, we have $R = q_1 \cdots q_u$ with $u \geq 1$ and $D^{p-1} \equiv 1 (\mathrm{mod}\, p^2)$, whence

$$Y_{-1} := m(q_1 \cdots q_u) = (p-1)^{u-1},$$
$$Y_0 := m(p^{\frac{2}{p-1}} \cdot q_1 \cdots q_u) = 0.$$

In the case $v = 1$, we have $R = q_1 \cdots q_u \cdot q_{u+1}$ with $u \geq 0$ and certainly $D^{p-1} \not\equiv 1 (\mathrm{mod}\, p^2)$, whence

$$m(q_1 \cdots q_u \cdot q_{u+1}) = 0 = Y_0,$$
$$Y_1 := m(p^{\frac{2}{p-1}} \cdot q_1 \cdots q_u \cdot q_{u+1}) = (p-1)^u.$$

Now we carry out the induction step for an additional prime factor q_{u+v+1} with $q_{u+v+1}^{p-1} \not\equiv 1 (\mathrm{mod}\, p^2)$, assuming that the multiplicities $m(q_1 \cdots q_{u+v}) =: Y_{v-1}$ and $m(p^{\frac{2}{p-1}} \cdot q_1 \cdots q_{u+v}) =: Y_v$ are known already.

If the new prime factor q_{u+v+1} and the powers $q_{u+v+1}^2, \ldots, q_{u+v+1}^{p-1}$ (which are not $(p-1)$-st roots of unity mod p^2 either) are multiplied by a radicand D with $D^{p-1} \equiv 1 (\mathrm{mod}\, p^2)$, then there are generated $p-1$ new radicands $D' = D \cdot q_{u+v+1}^{w_{u+v+1}}$ $(1 \leq w_{u+v+1} \leq p-1)$ with $(D')^{p-1} \not\equiv 1 (\mathrm{mod}\, p^2)$. However, if they are multiplied by a radicand D with $D^{p-1} \not\equiv 1 (\mathrm{mod}\, p^2)$, then exactly one of the $p-1$ new radicands D' satisfies $(D')^{p-1} \equiv 1 (\mathrm{mod}\, p^2)$ (the one, where $q_{u+v+1}^{w_{u+v+1}}$ represents the inverse of D in the group $U(\mathbb{Z}/p^2\mathbb{Z})/\{x \mid x^{p-1} \equiv 1 (\mathrm{mod}\, p^2)\} \simeq C(p)$) and the other $p-2$ radicands satisfy $(D')^{p-1} \not\equiv 1 (\mathrm{mod}\, p^2)$. Thus,

$$m(q_1 \cdots q_{u+v+1}) = m(p^{\frac{2}{p-1}} \cdot q_1 \cdots q_{u+v}) = Y_v,$$
$$\begin{aligned} Y_{v+1} &:= m(p^{\frac{2}{p-1}} \cdot q_1 \cdots q_{u+v+1}) \\ &= (p-2) \cdot m(p^{\frac{2}{p-2}} \cdot q_1 \cdots q_{u+v}) + (p-1) \cdot m(q_1 \cdots q_{u+v}) \\ &= (p-2) \cdot Y_v + (p-1) \cdot Y_{v-1}. \end{aligned}$$

https://doi.org/10.4153/CMB-1993-015-x Published online by Cambridge University Press

Consequently, the numbers Y_j ($j \geq -1$) satisfy a binary linear recursion, $Y_{j+1} = (p-2)Y_j + (p-1)Y_{j-1}$ for $j \geq 0$, with initial values $Y_{-1} = (p-1)^{u-1}$ and $Y_0 = 0$. This recursion can be solved by diagonalization of the corresponding matrix

$$M = \begin{pmatrix} p-2 & p-1 \\ 1 & 0 \end{pmatrix}.$$

The solution obtained by this straightforward procedure is $Y_j = (p-1)^u \cdot X_j$ with $X_j := \frac{1}{p}\big((p-1)^j - (-1)^j\big)$ for all $j \geq -1$. ∎

ACKNOWLEDGEMENT. The author would like to acknowledge that the original motivation for the generalization in this paper and valuable suggestions for the proof were given by Pierre Barrucand in Paris.

REFERENCES

1. W. E. H. Berwick, *Integral bases,* Cambridge Tracts in Math. and Math. Phys. **22**, 1927.

2. D. C. Mayer, *Multiplicities of dihedral discriminants,* Math. Comp. **58**(1992), 831–847 and Supplements section S55–S58.

Department of Computer Science
University of Manitoba