ILLINOIS JOURNAL OF MATHEMATICS
Volume 40, Number 2, Summer 1996

ON A CONDUCTOR DISCRIMINANT FORMULA OF MCCULLOH

BART DE SMIT

1. Introduction

For certain finite rings E, McCulloh has indicated a canonical construction of an order $T(E)$ in a Galois algebra $T_{\mathbb{Q}}(E)$ over $\mathbb{Q}$, whose Galois group is the unit group E^* of E. In the case that $E = \mathbb{Z}/n\mathbb{Z}$ for some non-negative integer n, the Galois algebra is the nth cyclotomic field and $T(E)$ is its ring of integers. McCulloh has used these orders to generalize Stickelberger relations [3], [4]. The construction of $T(E)$, which is explained in Section 2, works for all self-dual or quasi-Frobenius rings E.

The conductor discriminant formula for cyclotomic fields [5, Theorem 3.11] expresses the discriminant of a cyclotomic ring of integers as a product of conductors. A generalization of this formula to certain orders $T(E)$ was used by McCulloh to prove Stickelberger type formulas for the minus-part of the class group of $T(E)$; see the remark after Theorem 3 in [3]. In a talk in Durham in 1994 McCulloh posed the question of whether the following generalization holds for all commutative self-dual finite rings E:

$$\Delta_{T(E)/\mathbb{Z}} = \prod_{\chi \in \mathrm{Hom}(E^*, \mathbb{C}^*)} \mathcal{N}(\mathfrak{f}_\chi). \tag{1.1}$$

The conductor $\mathfrak{f}_\chi$ is the largest E-ideal $\mathfrak{a}$ for which χ factors through $(E/\mathfrak{a})^*$, and the norm $\mathcal{N}(\mathfrak{a})$ of an E-ideal $\mathfrak{a}$ is its index as an additive subgroup of E (or, more precisely, the $\mathbb{Z}$-ideal generated by this index). The main result of this note is the following.

THEOREM 1.2. *Let E be a self-dual finite commutative ring. The conductor product $\prod_\chi \mathcal{N}(\mathfrak{f}_\chi)$ with χ ranging over the homomorphisms $E^* \to \mathbb{C}^*$, is a divisor of $\Delta_{T(E)/\mathbb{Z}}$. We have $\Delta_{T(E)/\mathbb{Z}} = \prod_\chi \mathcal{N}(\mathfrak{f}_\chi)$ if and only if E is a principal ideal ring.*

The proof is given in Section 3, together with an explicit formula for $\Delta_{T(E)/\mathbb{Z}}$. The easiest example where (1.1) fails is $E = \mathbb{F}_2[V_4]$, the group ring over the field of two elements of the abelian group of type (2, 2). In this case, the left hand side is 2^{24}, and the right hand side is 2^{22}.

In Section 4 we show that one can often change the ring structure of E to that of a principal ideal ring without changing the order $T(E)$.

Received December 6, 1994.
1991 Mathematics Subject Classification. Primary 11R33; Secondary 11S45, 11T99.

For non-commutative self-dual rings E, McCulloh has suggested comparing the discriminant $\Delta_{T(E)/\mathbb{Z}}$ with the conductor product $\prod_\chi \mathcal{N}(\mathfrak{f}_\chi)^{\chi(1)}$. Here the product is taken over the irreducible complex characters χ of E^*. The conductor of χ is the largest two-sided E-ideal $\mathfrak{a}$ for which the representation $E^* \to \mathrm{GL}_{\chi(1)}(\mathbb{C})$ associated to χ factors through $(E/\mathfrak{a})^*$. This notion of conductor can be found in Lamprecht [2, §3.2]. At present it is not even known if one inequality holds in this generality.

2. Terminology

2.1. Self-dual rings. The dual $D(A)$ of a finite abelian group A is defined to be the group $\mathrm{Hom}(A, \mu_\infty)$, where μ_∞ is the group of roots of unity in a fixed algebraic closure $\overline{\mathbb{Q}}$ of $\mathbb{Q}$. Let E be a finite ring with 1 (not necessarily commutative). The dual $D(E_+)$ of the additive group E_+ of E has a right-E-module structure given by $(\varphi e)(x) = \varphi(ex)$ for all $e, x \in E$ and $\varphi \in D(E_+)$. We say that E is self-dual if $D(E_+)$ is free of rank 1 as a right-E-module. This is equivalent to saying that E is injective as a module over itself, and that E is a quasi-Frobenius ring [1, §57–58]. A finite commutative ring is self-dual if and only if it is Gorenstein.

2.2. Galois algebras. There is a (contravariant) equivalence of categories between finite separable algebras over $\mathbb{Q}$ and finite Ω-sets, where $\Omega = \mathrm{Gal}(\overline{\mathbb{Q}}/\mathbb{Q})$. Here Ω is a profinite group, and an Ω-set is understood to be a discrete set on which Ω acts continuously. Under this equivalence, an algebra $A/\mathbb{Q}$ corresponds to the Ω-set of ring homomorphisms $\mathrm{Hom}(A, \overline{\mathbb{Q}})$, and a Ω-set X corresponds to the $\mathbb{Q}$-algebra $\mathrm{Map}_\Omega(X, \overline{\mathbb{Q}})$ consisting of Ω-equivariant maps $X \to \overline{\mathbb{Q}}$.

Giving a separable algebra A the structure of a Galois algebra with Galois group G is the same as giving a right-G-action on the Ω-set X that it corresponds to, in such a way that the following two conditions are satisfied:

(i) for all $\sigma \in \Omega$, $x \in X$ and $g \in G$ we have $(\sigma x)g = \sigma(xg)$;
(ii) for all $x, y \in X$ there is a unique $g \in G$ with $xg = y$.

The first condition says that X is a (Ω, G)-space, and the second condition says that X is a principal homogeneous G-space.

2.3. Definition of the order $T(E)$. Suppose E is self-dual finite ring. The group ring $\mathbb{Q}[E_+]$ of the additive group of E is a finite separable algebra over $\mathbb{Q}$. A $\mathbb{Q}$-algebra homomorphism $\mathbb{Q}[E_+] \to \overline{\mathbb{Q}}$ is just a group homomorphism form E_+ to $\overline{\mathbb{Q}}^*$, so the Ω-set associated to $\mathbb{Q}[E_+]$ is the set $D(E_+) = \mathrm{Hom}(E_+, \mu_\infty)$, with Ω-action induced from the action on $\mu_\infty \subset \overline{\mathbb{Q}}$. Since E is self-dual, $D(E_+)$ is a free right-E-module of rank 1. Let S be the subset of $D(E_+)$ consisting of the generators of $D(E_+)$ as a right-E-module. The set S is Ω-stable, because for every $\varphi \in D(E_+)$ and $\sigma \in \Omega$ we have $\sigma\varphi = a\varphi$ for some $a \in \mathbb{Z}$ coprime to the characteristic of E. We now define the algebra $T_{\mathbb{Q}}(E)$ to be $\mathrm{Map}_{\Omega}(S, \overline{\mathbb{Q}})$. We have canonical surjective ring homomorphisms

$$\mathbb{Q}[E_+] \xrightarrow{\sim} \mathrm{Map}_{\Omega}(D(E_+), \overline{\mathbb{Q}}) \xrightarrow{\mathrm{res}} \mathrm{Map}_{\Omega}(S, \overline{\mathbb{Q}}) = T_{\mathbb{Q}}(E).$$

Since S is the set of generators of a free right-E-module of rank 1, it has a right-action of the group E^*, making it into a principal homogeneous E^*-space. This action also respects the left action of Ω on S, so that $T_{\mathbb{Q}}(E)$ is a Galois algebra over $\mathbb{Q}$ with Galois group E^*.

The order $T(E)$ is defined to be the projection in $T_{\mathbb{Q}}(E)$ of $\mathbb{Z}[E_+]$, or, equivalently, as the $\mathbb{Z}$-algebra generated by the image of E_+ in $T_{\mathbb{Q}}(E)$. It is an order in a product of a number of copies of $\mathbb{Q}(\zeta_n)$, where n is the characteristic of E. The $\mathbb{Z}$-rank of $T(E)$ is $\#E^*$.

3. Proof of the theorem

In this section we prove Theorem (1.2) and we give an explicit formula for the discriminant of $T(E)$ in terms of the structure of E.

Let E be a self-dual finite commutative ring. Since E is Artinian, it is a product of local rings. We first show that we can reduce to the case that E is local. Suppose that E is a product of two finite commutative rings: $E = E_1 \times E_2$. Then E_1 and E_2 are self-dual. Moreover, we have $T(E) = T(E_1) \otimes_{\mathbb{Z}} T(E_2)$, so that $\Delta_{T(E)/\mathbb{Z}} = \Delta^{r_2}_{T(E_1)/\mathbb{Z}} \Delta^{r_1}_{T(E_2)/\mathbb{Z}}$, where $r_i = \#E_i^*$. Writing $C(E)$ for the conductor product of E, one checks easily that $C(E) = C(E_1)^{r_2} C(E_2)^{r_1}$. Also, E is a principal ideal ring if and only if both E_1 and E_2 are. Thus, the theorem follows for E if we know it for E_1 and E_2.

We may now assume that E is local. Fix a Jordan-Hölder filtration of E as an E-module:

$$(*) \qquad 0 = E_k \subset E_{k-1} \subset \cdots \subset E_1 \subset E_0 = E.$$

This means that each E_i is an ideal in E and that the quotients E_i/E_{i+1} are simple E-modules. But the only simple E-module (up to isomorphism) is the residue field $k(E)$ of E, so we have $\#E_i = q^{k-i}$, where $q = \#k(E)$. The discriminant of $T(E)$ is given by the following lemma. Again, the cyclotomic case is well known [5, Prop. 2.1].

LEMMA 3.1. *If E is a finite local commutative self-dual ring with residue field of cardinality q, then $\#E = q^k$ with $k \in \mathbb{Z}$, and*

$$\Delta_{T(E)/\mathbb{Z}} = q^{(kq-k-1)q^{k-1}}.$$

Proof. Since E is self-dual, E has a unique minimal non-zero ideal H, and the order of H is q. A character $\varphi \in D(E_+)$ is a generator of $D(E_+)$ as an E-module if and only if $\varphi(H) \neq 1$. To see this, note that the sub-E-module of $D(E_+)$ generated by

φ is exactly the set of those $\psi \in D(E_+)$ that vanish on the largest E-ideal contained in the kernel of φ. Therefore, the characters of E_+ which are not E-module generators of $D(E_+)$ are exactly the characters of E_+/H, and it follows that the canonical map $\mathbb{Q}[E_+] \longrightarrow \mathbb{Q}[E_+/H] \times T_{\mathbb{Q}}(E)$ is an isomorphism of $\mathbb{Q}$-algebras.

Under this isomorphism, $\mathbb{Z}[E_+]$ is mapped to a subalgebra of $\mathbb{Z}[E_+/H] \times T(E)$, whose index we denote by i. We want to compute this index. The group ring $\mathbb{Z}[E_+]$ surjects to $T(E)$, and the kernel is the set of H-invariants $\mathbb{Z}[E_+]^H$, where we let H act on E_+ by translation. Thus, we have a commutative diagram with exact rows:

$$\begin{array}{ccccccccc}
0 & \longrightarrow & \mathbb{Z}[E_+]^H & \longrightarrow & \mathbb{Z}[E_+] & \longrightarrow & T(E) & \longrightarrow & 0 \\
 & & \downarrow & & \downarrow & & \| & & \\
0 & \longrightarrow & \mathbb{Z}[E_+/H] & \longrightarrow & \mathbb{Z}[E_+/H] \times T(E) & \longrightarrow & T(E) & \longrightarrow & 0.
\end{array}$$

Note that $\mathbb{Z}[E_+]^H$ is generated by formal H-coset sums of E. Since such a coset-sum is mapped to q times the coset element in $\mathbb{Z}[E_+/H]$, and $\mathbb{Z}[E_+/H]$ has $\mathbb{Z}$-rank q^{k-1}, it follows that the cokernel of the leftmost vertical map has cardinality $q^{q^{k-1}}$. By the snake lemma it follows that $i = q^{q^{k-1}}$.

The discriminant of the group ring $\mathbb{Z}[A]$ of an abelian group A of order n is n^n, so one finishes the proof by noting that

$$\Delta_{T(E)/\mathbb{Z}} = \frac{\Delta_{\mathbb{Z}[E_+]/\mathbb{Z}}}{i^2 \Delta_{\mathbb{Z}[E_+/H]/\mathbb{Z}}} = \frac{q^{kq^k}}{q^{2q^{k-1}} q^{(k-1)q^{k-1}}} = q^{(kq-k-1)q^{k-1}}. \qquad \square$$

We return to the proof of the theorem. The ring E is still local. For each i with $1 \leq i \leq k$ the quotient ring E/E_i is a local ring of order q^i. The units of E/E_i are exactly the elements not contained in its maximal ideal, so $(E/E_i)^*$ has order $s_i = q^i - q^{i-1}$. Putting $s_0 = 1$ this also holds for $i = 0$. For each character $\chi : E^* \to \mu_\infty$ let $\mathfrak{f}_\chi^*$ be the largest E-ideal E_i in our filtration $(*)$ for which χ factors over $(E/E_i)^*$. This depends on the choice of the Jordan-Hölder filtration $(*)$. For each i with $0 \leq i \leq k$ it is clear that exactly s_i characters of E^* factor over $(E/E_i)^*$. This implies that the number of characters χ of E^* with $\mathfrak{f}_\chi^* = E_i$ is $s_i - s_{i-1}$ if $i \neq 0$. It follows that

$$\prod_{\chi \in D(E^*)} \mathcal{N}(\mathfrak{f}_\chi^*) = \prod_{i=1}^{k} \mathcal{N}(E_i)^{s_i - s_{i-1}}.$$

Since $\mathcal{N}(E_i) = q\mathcal{N}(E_{i-1})$ for $i \neq 0$ this is equal to

$$q^{-s_0}(q^k)^{s_k} \prod_{i=1}^{k-1} q^{-s_i} = q^{-1+k(q^k-q^{k-1})-(q^{k-1}-1)} = q^{(kq-k-1)q^{k-1}} = \Delta_{T(E)/\mathbb{Z}}.$$

This means that the conductor discriminant formula holds for the conductors $\mathfrak{f}^*$ rather than for $\mathfrak{f}$. The first statement of the theorem now follows from the observation that $\mathfrak{f}_\chi$ divides $\mathfrak{f}_\chi^*$.

If the ideals of E are linearly ordered by inclusion then every ideal of E occurs in $(*)$, and we have $\mathfrak{f}_\chi^* = \mathfrak{f}_\chi$. Conversely, if $\mathfrak{f}_\chi^* = \mathfrak{f}_\chi$ for all characters χ of E^*, then the ideals of E are linearly ordered. To see this, let I be an ideal of E and choose i maximal under the condition that $E_i \supset I$. We may assume that $I \neq E$ so that $i \geq 1$. For every character χ of E^* that vanishes on $1 + I$, the assumption that $\mathfrak{f}_\chi^* = \mathfrak{f}_\chi$ implies that it also vanishes on $1 + E_i$. By duality of finite abelian groups it follows that $1 + E_i = 1 + I$ and therefore $I = E$.

It remains to show that a finite local ring E is a principal ideal ring if and only if its ideals are ordered linearly by inclusion. To see "only if" note that every ideal is of the form $x^i E$ for $i \geq 0$ if the maximal ideal of E is generated by x. To prove "if" suppose that $x, y \in E$. If the ideals are ordered linearly, then $xE \subset yE$ or $yE \subset xE$, so the ideal (x, y) is equal to (x) or to (y). But then any non-empty set of generators of an E-ideal can be thinned out to a set of 1 element; i.e., E is a principal ideal ring. This completes the proof of (1.2). $\square$

4. Changing the ring structure

If one is only interested in the structure of the order $T(E)$, then one can sometimes change the ring structure of E to that of a principal ideal ring, without changing the isomorphism class of $T(E)$. In our example $E = \mathbb{F}_2[V_4]$, where the conductor discriminant formula fails to hold, one may say that we just picked the wrong ring structure on E_+, because the group ring $E' = \mathbb{F}_2[C_4]$ of the cyclic group of order 4, is a principal ideal ring for which $T(E)$ and $T(E')$ are isomorphic. A more general construction is given in the next proposition.

PROPOSITION 4.1. *Suppose that E is a finite self-dual commutative ring and E_+ is homogeneous, i.e., free over $\mathbb{Z}/n\mathbb{Z}$ where $n = \operatorname{char} E$. Then there exists a finite commutative principal ideal ring E', an isomorphism of abelian groups $E_+ \cong E'_+$, and an isomorphism of $\mathbb{Z}$-algebras $T(E) \cong T(E')$ such that the diagram*

$$\begin{array}{ccc} E_+ & \xrightarrow{\sim} & E'_+ \\ \downarrow & & \downarrow \\ T(E) & \xrightarrow{\sim} & T(E'). \end{array}$$

is commutative.

Proof. By writing E as a product of local rings, we may assume that E is local. Let p and $q = p^f$ be the characteristic and cardinality of its residue field. The characteristic n of E is also a power of p. We let r be the rank of E_+ over $\mathbb{Z}/n\mathbb{Z}$. The p-torsion subgroup of E has size p^r and since it is an E-ideal, p^r is a power of q. This implies that r is divisible by f, and we put $e = r/f$.

Now take a finite field extension K of the field $\mathbb{Q}_p$ of p-adic numbers, for which the residue degree is f, and the ramification index is e. Denote the ring of integers of K by $\mathcal{O}_K$, and let E' be the ring $\mathcal{O}_K/n\mathcal{O}_K$. The ring E' is clearly a principal ideal ring, which also implies that it is self-dual. Both E_+ and E'_+ are free over $\mathbb{Z}/n\mathbb{Z}$ of rank r, and the minimal non-zero ideals H and H' of E and E' are both elementary abelian subgroups of order q.

It is not hard to see that there exists an isomorphism of abelian groups $E_+ \xrightarrow{\sim} E'_+$ that maps H to H'. This isomorphism induces an isomorphism $\mathbb{Z}[E_+] \xrightarrow{\sim} \mathbb{Z}[E'_+]$ of $\mathbb{Z}$-algebras. We claim that this induces an isomorphism of quotients $T(E) \xrightarrow{\sim} T(E')$. To see this, we recall from the proof of Lemma 3.1 that the kernel of the map $\mathbb{Z}[E_+] \to T(E)$ is generated by formal sums of H-cosets of E. These sums clearly map to H'-coset sums in E'. $\square$

One can do the same construction for products of homogeneous rings. For non-homogeneous local rings the statement in the proposition may fail to hold. To see this, consider the ring $\mathbb{Z}[X]/(2X, X^2+4)$, which is the only self-dual commutative ring E with additive group of type (8,2) for which the $\mathbb{Z}$-rank of $T(E)$ is 8.

REFERENCES

1. C. W. Curtis and I. Reiner, *Representation theory of finite groups and associative algebras*, Interscience, New York, 1962.
2. E. Lamprecht, *Struktur und Relationen allgemeiner Gaussscher Summen in endlichen Ringen, I*, J. Reine Angew. Math. **197** (1957), 1–26.
3. L. R. McCulloh, "Stickelberger relations in class groups and Galois module structure" in *Journées Arithmétiques* 1980, Cambridge University Press, Cambridge 1982, pp. 194–201.
4. ———, *Galois module structure of abelian extensions*, J. Reine Angew. Math. **375/376** (1987), 259–306.
5. L. C. Washington, *Introduction to cyclotomic fields*, Graduate Texts in Math. **83**, Springer-Verlag, New York, 1982.

ERASMUS UNIVERSITEIT
ROTTERDAM, THE NETHERLANDS