Can. J. Math. Vol. **47** (1), 1995 pp. 113–131

UNITS IN INTEGRAL GROUP RINGS FOR ORDER pq

KLAUS HOECHSMANN

ABSTRACT. For any finite abelian group A, let $\Omega(A)$ denote the group of units in the integral group ring which are mapped to cyclotomic units by every character of A. It always contains a subgroup $Y(A)$, of finite index, for which a basis can be systematically exhibited. For A of order pq, where p and q are odd primes, we derive estimates for the index $[\Omega(A) : Y(A)]$. In particular, we obtain conditions for its triviality.

0. **Introduction and summary.** For any finite abelian group A, let $\Delta(A)$ denote the kernel of the "augmentation" map $\mathbb{Z}A \longrightarrow \mathbb{Z}$ induced on the integral group ring $\mathbb{Z}A$ by the trivial character, and define $U_i(A)$ to be the group of invertible elements in the multiplicative semi-group $1+\Delta^i(A)$. Obviously the unit group $U(A)$ of $\mathbb{Z}A$ equals $U_0(A) = \pm U_1(A)$. Moreover, by a theorem of Higman [3] and a lemma of Cliff-Sehgal-Weiss [2], $U_1(A)$ turns out to be the direct product of the finite group A by the torsion-free group $U_2(A)$. The aim of the present paper is to study ways of generating large subgroups of $U_2(A)$ in the case where A has order pq, the product of two odd primes. Apart from the work of Kervaire-Murty [6], which briefly considers units by way of constructing ideal classes in $\mathbb{Z}A$ for $|A| = 15$, there seems to be as yet no literature dealing with this problem.

It is not hard to obtain subgroups of finite index in $U(A)$ for any A. The classical recipe, due to Bass [1], has the disadvantage of producing unpleasantly large indices. These are considerably reduced in a more recent procedure [4], which functorially associates with every A a well-built, explicit, and often improper group $Y(A) \subseteq U_2(A)$ of *constructible* units. However, it too is inevitably contained in the group $\Omega(A)$ of *circular* units, *i.e.*, those mapped to cyclotomic units (*cf.* [7]) by every character of A, since these are the only standard ingredients available from number fields. If ν is the exponent of A, the size of $U_2(A)/\Omega(A)$ depends, of course, on the class number h_ν^+ of the ring of real algebraic integers in the ν-th cyclotomic field. As long as the Euler number $\phi(\nu)$ is ≤ 72, we are assured (*cf.* [7], page 352) that $\Omega(A) = U_2(A)$.

Thus the only presently tractable part of the problem is the study of $\Omega(A)/Y(A)$. For p-groups A, it is in fairly satisfactory shape: this quotient is trivial if and only if p is regular or $|A| = p$; otherwise its size equals that of a certain canonical group of ideal classes (*cf.* [5]). The next most complicated case is $|A| = pq$. For $q = 2$, it was treated in [4]—with results quite similar to those which pertain to $q = 3$ in the pages that follow.

Every $u \in U_2(A)$ is *symmetric*; that is $u = u^\star$, where $\star$ denotes the involution induced on $\mathbb{Z}A$ by the map $a \longmapsto a^{-1}$ on A. If $|A|$ is odd, $U_2(A)$ actually coincides with the group

Received by the editors April 14, 1993.
AMS subject classification: 20C05, 11T22.

$U_1^+(A)$ of symmetric units in $U_1(A)$. This makes it relatively easy to describe $Y(A)$, which is always the direct product of certain canonical unit-groups $W(C)$ associated to every cyclic subgroup $C \subseteq A$. Each $W(C)$ is explicitly isomorphic to $\Delta^2(H_C)$, where $H_C = G_C/\langle\star\rangle$ and $G_C = \mathrm{Aut}(C)$. It is obtained as follows. If $x \in C$ is a generator and $\alpha \in \Delta^2(G_C)$ is written as $\alpha = \beta - \gamma$, with β and γ in $\mathbb{N}G_C$ (*i.e.*, with positive coefficients), there is a unique element $w_\alpha(x) \in U_1^+(C)$ such that the equation

$$(*) \qquad (x - x^{-1})^\beta = w_\alpha(x)(x - x^{-1})^\gamma$$

holds in $\mathbb{Z}A$. (N.B. The unit defined here would show up as $w_\alpha(x^2)$ in the notation of [4], but this is unimportant in view of the oddness of $|C|$.) Moreover, $w_\alpha(x)$ depends only on the image of α in $\Delta^2(H_C)$, and $\alpha \longmapsto w_\alpha(x)$ yields an *injection*

$$(\dagger) \qquad w(x)\colon \Delta^2(H_C) \longrightarrow U_1^+(C)$$

of H_C-modules. The image $W(C)$ of $w(x)$ is, of course, independent of the choice of generator x.

Henceforth let $|A| = pq$ be the product of two distinct odd primes. The central object of our attention will be the map

$$(\ddagger) \qquad \Xi\colon \frac{\Omega(A|p)}{Y(A|p)} \times \frac{\Omega(A|q)}{Y(A|q)} \longrightarrow \frac{\Omega(A)}{Y(A)},$$

where $\Omega(A|p)$ and $Y(A|p)$ denote circular and constructible units mapped to 1 by all characters except those of order p. We shall see, among other things, that this map is bijective whenever $(p-1)/2$ is relatively prime to $(q-1)/2$.

Our first theorem treats the constituent factors on the left of $(\ddagger)$ by relating $\Omega(A|p)$ and $Y(A|p)$, for instance, to the much more manageable group $A^q = A_p$.

THEOREM 0.1. *Any surjection $A \longrightarrow A_p$ induces isomorphisms of $\Omega(A|p)$ and $Y(A|p)$, respectively, with*

$$\ker[W(A_p) \longrightarrow U\mathbb{F}_q A_p] \quad \textit{and} \quad \mathrm{im}[\Delta^2(G_p) \cap (q - \tau_q)\Delta(G_p) \xrightarrow{w(z)} W(A_p)],$$

where $G_p = \mathrm{Aut}(A_p)$ for $A_p = \langle z\rangle$, and τ_q is the automorphism $z \longmapsto z^q$.

Since $W(A_p) \simeq \Delta^2(H_p)$ is easy to handle, this theorem (despite its wild appearance) reduces the computation of $\Omega(A|p)/Y(A|p)$ to the determination of the kernel induced by $\mathbb{Z} \longrightarrow \mathbb{F}_q$. It will be proved in Section 4, after various preliminaries in Sections 1 to 3.

The rest of our results refer to certain numerical invariants. The easiest of these is the greatest common divisor m of $h_p = (p-1)/2$ and $h_q = (q-1)/2$. Another fairly easy one is the greatest common divisor m'' of the indices $[H_p : \langle\tau_q\rangle]$ and $[H_q : \langle\tau_p\rangle]$, which is (of course) a divisor of m. For fixed q, it can be shown that $H_p = \langle\tau_q\rangle$ for about 56% of the primes p (this amounts to one-and a-half times the density of 37.4% conjectured by Artin for the p having q as primitive root). Hence m'' is rarely non-trivial.

https://doi.org/10.4153/CJM-1995-006-4 Published online by Cambridge University Press

THEOREM 0.2. *The kernel of the map Ξ is cyclic of order m''.*

The proof of this fact will occupy Section 5.

To compute the size of the two factors occurring on the left of (‡), we need more delicate invariants. If ζ_p is a primitive p-th root of unity, put $\theta_p = \zeta_p + \zeta_p^{-1}$ and consider the group $\Omega(\zeta_p)$ of cyclotomic units in the ring $\mathbb{Z}[\theta_p]$, as well as its subgroup $Y(\zeta_p)$, which is the image of $\Omega(A_p) = Y(A_p) = W(A_p)$ under the character $z \mapsto \zeta_p$. Now pass to the finite ring $\mathbb{F}_q[\theta_p] = \mathrm{im}_q\, \mathbb{Z}[\theta_p]$, obtained from $\mathbb{Z}[\theta_p]$ by reduction modulo q, and look at the unit groups

$$\acute{U}\mathbb{F}_q[\theta_p] \supseteq \mathrm{im}_q\, \acute{\Omega}(\zeta_p) \supseteq \mathrm{im}_q\, Y(\zeta_p),$$

where the acute accent means restriction to elements with trivial H_p-norm (this norm maps $\Omega(\zeta_p)$ onto $\{\pm 1\}$ and $U\mathbb{F}_q[\theta_p]$ onto $\mathbb{F}_q^\times$). We shall require the indices of this filtration, namely

$$d_q(\zeta_p) = [\acute{U}\mathbb{F}_q[\theta_p] : \mathrm{im}_q\, \acute{\Omega}(\zeta_p)] \quad \text{and} \quad e_q(\zeta_p) = [\mathrm{im}_q\, \acute{\Omega}(\zeta_p) : \mathrm{im}_q\, Y(\zeta_p)].$$

The first of these is the more important one and will be referred to as the *defect* modulo q of ζ_p. Although it tends to be trivial (at least for small p and q) its behaviour seems completely erratic. Section 6 will establish the following result.

THEOREM 0.3. *$e_q(\zeta_p)$ divides m, and*

$$\frac{m}{e_q(\zeta_p)} \cdot [\Omega(A|p) : Y(A|p)] = d_q(\zeta_p).$$

In Section 7, we finally estimate the size of the cokernel $L(\xi)/Y(\xi)$ of Ξ. Here $x \mapsto \xi$ denotes a character of maximal order on A, whereas $L(\xi)$, $Y(\xi)$ denote the images of $\Omega(A)$, $Y(A)$ under this character, and the letter L stands for "liftable". $L(\xi)$ is almost always smaller than the group $\Omega(\xi)$ of all cyclotomic units in $\mathbb{Z}[\xi]$. Our result is as follows.

THEOREM 0.4. *The group $L(\xi) \subset \Omega(\xi)$ of liftable circular units has a natural filtration*

$$L(\xi) \supseteq L^\circ(\xi) \supseteq L^*(\xi) \supseteq Y(\xi),$$

with the following quotients:

(i) $L(\xi)/L^\circ(\xi)$ is a cyclic group whose order divides m''.

(ii) $L^\circ(\xi)/L^*(\xi)$ is the product of at most two cycles whose orders divide $e_q(\zeta_p)$ and $e_p(\zeta_q)$, respectively.

(iii) $L^*(\xi)/Y(\xi)$ is the product of two cycles whose orders divide $m/e_p(\zeta_q)$ and $m/e_q(\zeta_p)$, respectively.

Further details about the composition of $\Omega(A)/Y(A)$ can be gathered from the actual proofs of these theorems. At this point, however, we shall gloss over these technicalities in favour of a simple, manageable conclusion. In fact, Theorem 0.2 yields the identity

$$m''[\Omega(A) : Y(A)] = [\Omega(A|p) : Y(A|p)] \cdot [\Omega(A|q) : Y(A|q)] \cdot [L(\xi) : Y(\xi)],$$

which together with Theorems 0.3 and 0.4 implies the following.

https://doi.org/10.4153/CJM-1995-006-4 Published online by Cambridge University Press

COROLLARY 0.5. *$[\Omega(A) : Y(A)]$ is a divisor of $d_q(\zeta_p)d_p(\zeta_q)\cdot e_q(\zeta_p)e_p(\zeta_q)$, and actually equals $d_q(\zeta_p)d_p(\zeta_q)$ when $m = 1$.*

If $q = 3$, for instance, we always have $[\Omega(A) : Y(A)] = d_3(\zeta_p)$. This number turns out to be 1 for all $5 \leq p \leq 101$, except for $p = 61$, where it is a multiple of 44, and for $p = 97$, where it equals 73. Thus $\Omega(A)/Y(A)$ is a cyclic group of order 73 when $|A| = 291$. It would be interesting to see a generator.

In general, the computation of $d_q(\zeta_p)$ is not entirely routine, especially when $\mathbb{F}_q[\theta_p]$ is not a field. We have carried it out sytematically only for $(p-1)(q-1) \leq 72$. These cases are particularly interesting, since for them $\Omega(A) = U_1^+(A)$, and therefore the triviality of $[\Omega(A) : Y(A)]$ gives an explicit handle on the group of all units.

In this range, there are only 3 instances—namely $|A| = 65$, 85, and 91—for which this index is not trivial. In each of these, we have $m'' = 1$, and all defects are trivial—except for $d_7(\zeta_{13})$ which equals 3. As if to compensate, $e_7(\zeta_{13}) = 1$, whereas $e_q(\zeta_p) = m$ in each of the other five cases. Altogether then, $\Omega(A)/Y(A)$ is at most of exponent m and order m^2 for these three exceptional groups.* Details about such calculations, and about the problem of exhibiting generators for $\Omega(A)/Y(A)$, will be published separately.

1. **The set-up.** Let A be a cyclic group of order n with $n = pq$, the product of two odd primes, and with generator $x = yz$, where y is of order q and z is of order p. The four characters $\psi_i : x \longmapsto \zeta_i$, where $i = n, q, p, 1$ and ζ_i is a primitive i-th root of unity, then identify the group ring $\mathbb{Z}A$ as a subring of the maximal order

$$\mathcal{M}(A) = \mathbb{Z}[\xi] \oplus \mathbb{Z}[\eta] \oplus \mathbb{Z}[\zeta] \oplus \mathbb{Z}, \tag{1}$$

where we have set $\xi = \zeta_n$, $\eta = \zeta_q$, and $\zeta = \zeta_p$, with $\xi = \eta\zeta$, in order to simplfy the appearance of formulas. Problem: find criteria for a given quadruple of components on the right of (1) to lift to an element of $\mathbb{Z}A$. Since $\psi_n : \mathbb{Z}A \longrightarrow \mathbb{Z}[\xi]$ is surjective, we might as well start with a pre-image $\tilde{u}(x) \in \mathbb{Z}A$ of that component and endeavour to find a triple v, w, a in the remaining ones so that $\tilde{u}(\xi)$, v, w, a fit together to form the image of an element $u(x) \in \mathbb{Z}A$.

NOTATION. Let $s_i \in \mathbb{Z}A$ denote the sum over all elements of the subgroup $A_{n/i} \subseteq A$ of index i. For $v \in \mathbb{Z}[\eta]$, let $v(1) \in \mathbb{F}_q$ be the "augmentation", and analogously define $w(1)$ for $w \in \mathbb{Z}[\zeta]$.

LEMMA 1.1. *Given $u \in \mathbb{Z}[\xi]$, $v \in \mathbb{Z}[\eta]$, $w \in \mathbb{Z}[\zeta]$, and $a \in \mathbb{Z}$, pick a $\tilde{u}(x) \in \mathbb{Z}A$ such that $\tilde{u}(\xi) = u$. Then there exists a pre-image $u(x) \in \mathbb{Z}A$ for the quadruple u, v, w, a if and only if*

$$\begin{aligned} v &\equiv \tilde{u}(\eta) \pmod{p}, \quad & w &\equiv \tilde{u}(\zeta) \pmod{q}, \\ a &\equiv v(1) \pmod{q}, \quad & a &\equiv w(1) \pmod{p}. \end{aligned} \tag{2}$$

* In the meantime, R. Ferguson has shown that the order is $\leq m$ in these cases.

The desired pre-imge is then given by

$$u(x) = \tilde{u}(x) + \tilde{v}(x)s_q + \tilde{w}(x)s_p + hs_1, \tag{3}$$

where $\tilde{v}(x)$ *and* $\tilde{w}(x)$ *are chosen in* $\mathbb{Z}A$ *so that* $p\tilde{v}(\eta) = v - \tilde{u}(\eta)$ *and* $q\tilde{w}(\zeta) = w - \tilde{u}(\zeta)$, *respectively, and* $h \in \mathbb{Z}$ *is adjusted suitably.*

PROOF. Since ψ_n annihilates s_i for $i \neq n$, it is clear that any element of the form (3) gives the correct image $\tilde{u}(\xi)$ under that map. Therefore we only need to worry about the other three.

If the first part of condition (2) is satisfied, we can divide $v - \tilde{u}(\eta)$ by p and let $\tilde{v}(x)$ be any ψ_q pre-image of the result. Since ψ_q kills s_p and s_1 while mapping s_q to p, we get the correct result v under $x \longmapsto \eta$. Similarly, the second part of (2) allows us to choose $\tilde{w}(x)$ so as to make (3) yield the result w under $x \longmapsto \zeta$. With h as yet undetermined, we now have

$$u(1) = \tilde{u}(1) + \tilde{v}(1)p + \tilde{w}(1)q + hn. \tag{4}$$

Read modulo q, this gives $u(1) \equiv \tilde{u}(1) + \tilde{v}(1)p \equiv a$, because $p\tilde{v}(1) \equiv v(1) - \tilde{u}(1)$ and $v(1) \equiv a \pmod{q}$. Similarly $u(1) \equiv a \pmod{p}$ and hence $u(1) \equiv a \pmod{n}$, for any h whatsoever. For a suitable choice of the latter, we therefore get $u(1) = a$.

Conversely suppose that $u(x) \in \mathbb{Z}A$ is given such that $u(\xi) = \tilde{u}(\xi)$, and define $v = u(\eta)$, $w = u(\zeta)$, and $a = u(1)$. Then $u(x) - \tilde{u}(x) = \Phi_n(x)f(x)$ is a multiple of the n-th cyclotomic polynomial (or rather its image in $\mathbb{Z}A$). Since the polynomials Φ_p and Φ_q are relatively prime, we can write $f(x)$ as a $\mathbb{Z}A$-linear combination of $\Phi_p(x)$ and $\Phi_q(x)$. This makes

$$u(x) = \tilde{u}(x) + \Phi_n(x)[k(x)\Phi_p(x) + l(x)\Phi_q(x)] = \tilde{u}(x) + k(x)s_q + l(x)s_p, \tag{5}$$

since $\Phi_n(x)\Phi_p(x) = \Phi_p(x^q) = s_q$ *etc*. Clearly, $v = \tilde{u}(\eta) + k(\eta)p$, and $w = \tilde{u}(\zeta) + l(\zeta)q$, which gives the first line of (2). To get the second, note that $u(1) \equiv v(1) \pmod{q}$ and $u(1) \equiv w(1) \pmod{p}$. ∎

The term hs_1 does not appear in this calculation because $u(1) = a$ is given. Thus $k(x)s_q$ and $l(x)s_p$ are not *arbitrary* lifts of $v - \tilde{u}(\eta)$ and $w - \tilde{u}(\zeta)$, but special ones.

REMARK. For everyday use, we summarize the gist of Lemma 1.1 by the pull-back

$$\begin{array}{ccc} \mathbb{Z}A & \longrightarrow & \mathbb{Z}[\xi] \\ \downarrow & & \downarrow \\ \mathbb{Z}A_q \times_1 \mathbb{Z}A_p & \longrightarrow & \mathbb{F}_p[\eta] \times \mathbb{F}_q[\zeta] \end{array} \tag{6}$$

where $\times_1$ denotes the fibre-product over the augmentation maps. The vertical arrow on the right symbolizes the product $\mathrm{red}_P \times \mathrm{red}_Q$, where $\mathrm{red}_Q\colon \mathbb{Z}[\xi] \longrightarrow \mathbb{F}_q[\zeta]$ is the reduction modulo the ideal $Q = (\eta - 1)\mathbb{Z}[\xi]$, and red_P is its counterpart for $P = (\zeta - 1)\mathbb{Z}[\xi]$. For

https://doi.org/10.4153/CJM-1995-006-4 Published online by Cambridge University Press

reference, this diagram will be labelled PB0. It could just as easily be derived from the asymmetric pair of pull-backs

$$(7)\qquad \begin{array}{ccc} \mathbb{Z}A & \longrightarrow & \mathbb{Z}[\eta]A_p \\ \downarrow & & \downarrow \\ \mathbb{Z}A_p & \longrightarrow & \mathbb{F}_q A_p \end{array} \quad \text{and} \quad \begin{array}{ccc} \mathbb{Z}[\eta]A_p & \longrightarrow & \mathbb{Z}[\xi] \\ \downarrow & & \downarrow \\ \mathbb{Z}[\eta] & \longrightarrow & \mathbb{F}_p[\eta], \end{array}$$

which are to be found in [6] (Section 7). When we have occasion to refer to them, these will be called PB1 and PB2, respectively. Like the lemma, all these diagrams reduce the lifting problem to questions about the finite semi-simple rings $\mathbb{F}_p[\eta]$ and $\mathbb{F}_q[\zeta]$.

When we apply any of the functors U_1, U_1^+, or Ω to the rings shown in (6), we still get a pull-back (now with a *direct* product in the lower left), which we continue to label PB0. We are especially interested in the Ω-version

$$(8)\qquad \begin{array}{ccc} \Omega(A) & \longrightarrow & \Omega(\xi) \\ \downarrow & & \downarrow \\ W(A_q) \times W(A_p) & \longrightarrow & U\mathbb{F}_p[\eta] \times U\mathbb{F}_q[\zeta], \end{array}$$

whose lower left hand corner reflects the important fact that $\Omega(A_p) = Y(A_p) = W(A_p)$.

It also shows, for instance, that the kernel $\Omega(A|p,q)$ of the map $\Omega(A) \longrightarrow \Omega(\xi)$ is the direct product $\Omega(A|p) \times \Omega(A|q)$. The notation $(A|\cdots)$ is supposed to recall which characters of A are permitted to be non-trivial on the units in question. Putting $L(\xi) = \mathrm{im}[\Omega(A) \longrightarrow \Omega(\xi)]$, where L stands for "liftable", we obtain the short exact sequence

$$(9)\qquad 1 \longrightarrow \Omega(A|p) \times \Omega(A|q) \longrightarrow \Omega(A) \longrightarrow L(\xi) \longrightarrow 1.$$

Unfortunately, the functor Y does not preserve the pull-back property. So, when we restrict the map $x \longmapsto \xi$ to the constructible units $Y(A)$, the kernel $Y(A|p,q)$ does not in general split as conveniently. However, it obviously contains the product $Y(A|p)Y(A|q)$, which is direct because $\Omega(A|p)$ does not intersect $\Omega(A|q)$. Hence we wind up with the exact sequence

$$(10)\qquad 1 \longrightarrow \frac{Y(A|p,q)}{Y(A|p)Y(A|q)} \longrightarrow \frac{\Omega(A|p)}{Y(A|p)} \times \frac{\Omega(A|q)}{Y(A|q)} \longrightarrow \frac{\Omega(A)}{Y(A)} \longrightarrow \frac{L(\xi)}{Y(\xi)} \longrightarrow 1.$$

Our aim is to study $\Omega(A)/Y(A)$ by analysing the other terms of this sequence.

2. **Cyclotomic units.** We continue with the abbreviations $\zeta_q = \eta$, $\zeta_p = \zeta$, and $\zeta_n = \eta\zeta = \xi$. If G_ν denotes the automorphism group of a cyclic group of order ν, we have $G_n = G_q \times G_p$. Finally, we put $\vartheta(x) = x^{-1} - x$ for any x such that $x^n = 1$.

LEMMA 2.1. *The group $\Omega(\xi)$ of real cyclotomic units in $\mathbb{Z}[\xi]$ is given by*

$$(11)\qquad \Omega(\xi) = \vartheta(\xi)^{\Delta G_n + 2Z} \cdot \vartheta(\eta)^{\Delta G_q} \cdot \vartheta(\zeta)^{\Delta G_p}.$$

PROOF. First we recall that $(1-\xi)$ is a unit in $\mathbb{Z}[\xi]$, since its G_n-norm equals $\Phi_n(1) = 1$. Hence the first factor on the right of (11) is indeed a group of units.

https://doi.org/10.4153/CJM-1995-006-4 Published online by Cambridge University Press

Applying complex conjugation, we see that $\overline{\vartheta}(\xi) = -\vartheta(\xi)$ implies $\vartheta(\xi)^2$ is real, and so, of course, is any $\vartheta(\xi)^{\sigma-1}$ with $\sigma \in G_n$, *etc.*. Modulo the group on the right hand side of (11), every $u \in \Omega(\xi)$ is therefore of the form $u = \xi^i \cdot \vartheta(\xi)^j \cdot \vartheta(\eta)^k \cdot \vartheta(\zeta)^l$ with non-negative integers i, k, l, and $j = 0, 1$. Since the ring $\mathbb{Z}[\xi]/(\eta - 1)\mathbb{Z}[\xi] \simeq \mathbb{F}_q[\zeta]$ is non-zero, $\vartheta(\eta)$ is a non-unit, and k must be 0. Likewise $l = 0$. For $u = \xi^i\vartheta(\xi)^j$, however, we have $\overline{u} = (-1)^j\xi^{-i}\vartheta(\xi)^j$, so that $u = \overline{u}$ entails $\xi^{2i} = (-1)^j$, an impossibility unless $j = 0$. Finally, no $\xi^i \neq 1$ is real, by oddness of n. ∎

We shall also have to deal with the subgroups

$$\Omega^\circ(\xi) = \vartheta(\xi)^{\Delta G_n}\vartheta(\eta)^{\Delta G_q}\vartheta(\zeta)^{\Delta G_p}, \quad Y(\xi) = \vartheta(\xi)^{\Delta^2 G_n}\vartheta(\eta)^{\Delta^2 G_q}\vartheta(\zeta)^{\Delta^2 G_p} \tag{12}$$

of $\Omega(\xi)$. By the description of $Y(A) = W(A) \times W(A^p) \times W(A^q)$ given in the Introduction, $Y(\xi)$ is exactly the ψ_n-image of $Y(A)$. The main difficulty in analysing the cokernel of the homomorphism Ξ lies in the fact that the ψ_n-image of $\Omega(A)$ is more elusive.

Remember that m is the greatest common divisor of $(p-1)/2$ and $(q-1)/2$.

LEMMA 2.2. *The group $\Omega(\xi)/\Omega^\circ(\xi)$ is cyclic of order dividing m.*

PROOF. This depends heavily on the basic norm relations, norms taken with respect to G_p and to G_q, which connect $\vartheta(\xi)$ with the cyclotomic units in $\mathbb{Z}[\eta]$ and $\mathbb{Z}[\zeta]$. For instance, if i runs from 1 to $q-1$, we clearly have $\prod_i(1 - \eta^i\zeta) = \Phi_q(\zeta)$, which just says that

$$(1 - \xi)^{\Sigma(G_q)} = (1 - \zeta)^{\tau_q - 1}, \tag{13}$$

where $\Sigma(G_q) \in \mathbb{Z}G_n$ denotes the sum over the subgroup $G_q \times 1$, and $\tau_q \in G_p$ is the automorphism $\zeta \mapsto \zeta^q$. Applying this to ξ^2 and multiplying both sides by ζ^{1-q}, we obtain the desired relation

$$\vartheta(\xi)^{\Sigma(G_q)} = \vartheta(\zeta)^{\tau_q - 1}. \tag{14}$$

Since $\Sigma(G_q) \equiv q - 1$ modulo ΔG_q, we also conclude that $\vartheta(\xi)^{q-1} \in \vartheta(\xi)^{\Delta G_q}\vartheta(\zeta)^{\Delta G_p}$, which, together with its G_p-analogue, shows that $\vartheta(\xi)^{2m} \in \Omega^\circ(\xi)$. This proves our claim, since $\Omega(\xi)/\Omega^\circ(\xi)$ is obviously generated by the class of $\vartheta(\xi)^2$. ∎

REMARK. Another important subgroup of $\Omega(\xi)$ is defined as $\Omega^*(\xi) = \vartheta(\xi)^{\Delta G_n}Y(\xi)$. The proof of Lemma 2.2 also shows that $\Omega^*(\xi)/Y(\xi)$ has an exponent dividing $2m$, and it is easily seen to have at most two generators.

Indeed, for any group G we have an obvious group epimorphism $G \longrightarrow \Delta(G)/\Delta^2(G)$, by $\sigma \mapsto (\sigma - 1)$. In this way, we get a surjection

$$V\colon G_n \times G_q \times G_p \longrightarrow \Omega^*(\xi)\Omega(\eta)\Omega(\zeta)/Y(\xi) = \Omega^\circ(\xi)/Y(\xi), \tag{15}$$

where $\Omega(\zeta) = \vartheta(\zeta)^{\Delta G_p}$, *etc.* Since G_n has two generators, so does $V(G_n) = \Omega^*(\xi)/Y(\xi)$. The other two components, $V(G_q)$ and $V(G_p)$, are cyclic but may have orders as large

https://doi.org/10.4153/CJM-1995-006-4 Published online by Cambridge University Press

as $(q-1)/2$ and $(p-1)/2$, respectively (remember: these units are *real*). For future reference, we note that V is explicitly given by

$$V(\varphi,\rho,\sigma) = \vartheta(\xi)^{\varphi-1}\vartheta(\eta)^{\rho-1}\vartheta(\zeta)^{\sigma-1}Y(\xi). \tag{16}$$

Our analysis of the cokernel of Ξ will use the filtration

$$\Omega(\xi) \supseteq \Omega^{\circ}(\xi) \supseteq \Omega^{*}(\xi) \supseteq Y(\xi). \tag{17}$$

In this section, we have obtained some estimates of the sizes of its "slices": the first and last have exponents dividing m or $2m$, and at most one or two generators, respectively. The potentially biggest is the middle one, $\Omega^{\circ}(\xi)/\Omega^{*}(\xi)$, with two generators whose orders are not bounded by $2m$ *a priori*.

3. **Three abstract lemmas.** If $G \subseteq H$ is a subgroup of a (finite) abelian group, let $\Sigma(G) \in \mathbb{Z}H$ stand for the sum over the elements of G. Consider a product of subgroups $H = F \cdot G$ which is not necessarily direct, and let $\mathcal{M}$ and $\mathcal{N}$ denote the ideals generated in $\mathbb{Z}H$ by $\Sigma(F)$ and $\Sigma(G)$, respectively. Let f and g denote the respective group orders.

LEMMA 3.1. *$\mathbb{Z}H/(\mathcal{M}+\mathcal{N})$ is torsion-free over $\mathbb{Z}$.*

PROOF. We shall exhibit a linearly independent set of $d = |H| - [H:F] - [H:G] + 1$ generators for the $\mathbb{Z}$-module $\mathbb{Z}H/(\mathcal{M}+\mathcal{N})$. Starting with the obvious set H, we reduce it to $H - S - T$ by replacing certain $\tau \in H$ by sums over the cosets τF or τG via the relations

$$\tau \equiv -\sum_{1 \neq \rho \in F} \tau\rho \pmod{\mathcal{M}} \quad \text{and} \quad \tau \equiv -\sum_{1 \neq \sigma \in G} \tau\sigma \pmod{\mathcal{N}}. \tag{18}$$

Choosing a complete system $S \subset G$ of coset representatives modulo F, we obtain a reduced set of generators $H - S$ by means of the first of these relations. Since the discarded set S lies entirely in a single G-coset (namely the neutral one), we are free to choose one element τ from each of the $[H:G]-1$ non-neutral G-cosets and replace it by a similar sum using the second relation. We have thus discarded a total of $[H:F]+[H:G]-1$ generators, proving that the rank of $\mathbb{Z}H/(\mathcal{M}+\mathcal{N})$ is at most d.

If there were a linear relation between the remaining generators, it would show up in the complex vector space $\mathbb{C}H/(\mathbb{C}\mathcal{M}+\mathbb{C}\mathcal{N})$, giving it a dimension less than d. But

$$\frac{1}{g}\Sigma(G) = \sum_{\chi(G)=1} e_{\chi}, \tag{19}$$

where χ runs over all characters of $\mathbb{C}H$, and e_{χ} stands for the corresponding minimal idempotents. The sum on the right of (19) has $[H:F]$ terms. Since we have a similar result for F, and since only the trivial character trivializes both F and G, the dimension of $\mathbb{C}\mathcal{M}+\mathbb{C}\mathcal{N}$ equals exactly $[H:F]+[H:G]-1$. ∎

LEMMA 3.2. *Let $\mathcal{M}_0$ and $\mathcal{N}_0$ denote the intersections of $\Delta(H)$ with $\mathcal{M}$ and $\mathcal{N}$, respectively. Then the torsion group of $\Delta(H)/(\mathcal{M}_0 + \mathcal{N}_0)$ is cyclic of order m, the greatest common divisor of $[H : F]$ and $[H : G]$. It is generated by the class of*

$$\delta_0 = \frac{[H : F]}{m}\Sigma(F) - \frac{[H : G]}{m}\Sigma(G). \tag{20}$$

PROOF. We first show that $m\delta_0 \in \mathcal{M}_0 + \mathcal{N}_0$. This results from the fact that $\Sigma(H)$ can be expressed eiher as $\alpha\Sigma(F)$ or as $\beta\Sigma(G)$, where α and β are sums in $\mathbb{Z}H$ over systems of representatives modulo F and G, respectively. If we write $\alpha = [H : F] - \delta$ and $\beta = [H : G] - \varepsilon$, the equality $\alpha\Sigma(F) = \beta\Sigma(G)$ takes the form

$$[H : F]\Sigma(F) - [H : G]\Sigma(G) = \delta\Sigma(F) - \varepsilon\Sigma(G), \tag{21}$$

which puts $m\delta_0$ where we want it, since both δ and ε are in $\Delta(H)$.

Conversely, let $\delta_1 \in \Delta(H)$ with $k\delta_1 \in \mathcal{M}_0 + \mathcal{N}_0$. Modulo this ideal, every element of $\mathcal{M} + \mathcal{N}$ is obviously congruent to something in $\Sigma(F)\mathbb{Z} + \Sigma(G)\mathbb{Z}$. Since $\delta_1 \in \mathcal{M} + \mathcal{N}$, by the preceding lemma, we may therefore assume that

$$\delta_1 = n_F\Sigma(F) - n_G\Sigma(G) \quad \text{and} \quad k\delta_1 = \delta_F\Sigma(F) - \delta_G\Sigma(G), \tag{22}$$

with $n_F, n_G \in \mathbb{Z}$ and $\delta_F, \delta_G \in \Delta(H)$. Taken together, these equations yield

$$(kn_F - \delta_F)\Sigma(F) = (kn_G - \delta_G)\Sigma(G). \tag{23}$$

Left fixed by both F and G, this element must be a multiple of $\Sigma(H)$, hence $= l\Sigma(H)$ for some $l \in \mathbb{Z}$. Comparing augmentations in the equality $(kn_G - \delta_G)\Sigma(G) = l\Sigma(H)$, we get $kn_G = l[H : G]$, and analogously $kn_F = l[H : F]$, whence finally

$$\delta_1 = \frac{lm}{k}\delta_0. \tag{24}$$

To show that the rational factor lm/k is actually integral, we must suppose that $\delta_0 \neq 0$, in particular, that $F \neq G$. We might as well assume that some $\sigma \in G$ is not in F. Now, δ_0 is of the form $a\Sigma(F) + b\Sigma(G)$ with a relatively prime to b. In the expression $r\delta_0$, with $r \in \mathbb{Q}$, the coefficient of the neutral element of H then is $ra + rb$, while the coefficient of σ is just rb. For both of these to be integral, it is clearly necessary that $r \in \mathbb{Z}$.

The only thing that remains to be proved is that, if the torsion factor $k > 0$ is chosen minimal, then $k|m$. Since k divides lm, it suffices to show $(k, l) = 1$. In fact, any common divisor t of k and l would lead to a reduced torsion-formula $(k/t)\delta_1 = \delta'_F\Sigma(F) - \delta'_G\Sigma(G)$, where $t\delta'_F\Sigma(F) = \delta_F\Sigma(F)$ and $t\delta'_G\Sigma(G) = \delta_G\Sigma(G)$, as we shall now see.

For the existence of δ'_G, remember that

$$\delta_G\Sigma(G) = kn_G + l\Sigma(H), \tag{25}$$

so that t does divide $\gamma = \delta_G\Sigma(G)$. Since γ is G-invariant, its coefficients (with respect to the natural basis H of $\mathbb{Z}H$) are constant on cosets of G. Having chosen a system R

of representatives of H mod G, we can therefore write $\gamma = \theta_R \Sigma(G)$, where the natural coefficients of θ_R are 0 outside of R and equal to those of γ otherwise. Clearly, t divides γ if and only if it divides θ_R, *i.e.*, if and only if $\theta_R = t\delta'_G$. ∎

We conclude this section with a closer look at the nature of $\mathcal{M}_0$ and $\mathcal{N}_0$. Clearly, any element in $\mathcal{M}_0 \cap \mathcal{N}_0$ is left fixed by both F and G, hence by H. Therefore $\mathcal{M}_0 \cap \mathcal{N}_0 \subseteq \Sigma(H)\mathbb{Z} \cap \Delta(H) = 0$, and the sum $\mathcal{M}_0 + \mathcal{N}_0 = \mathcal{M}_0 \oplus \mathcal{N}_0$ is direct.

As far as the individual summands are concerned, we note that $\mathcal{N}_0 = \Sigma(G)\Delta(H)$ also equals

$$\mathrm{Fix}_G \Delta(H) = \Sigma(G)\Delta(F), \tag{26}$$

the latter because of the identity $(\rho\sigma - 1) = (\rho - 1)(\sigma - 1) + (\rho - 1) + (\sigma - 1)$, with $\rho \in F$ and $\sigma \in G$, the former because $\mathbb{Z}H$ is free over $\mathbb{Z}G$. Of course, we also have the analogous facts for $\mathcal{M}_0$. Our third lemma relates these items to $\Delta^2(H)$.

LEMMA 3.3. *(i)* $(\mathcal{M}_0 \oplus \mathcal{N}_0) \cap \Delta^2(H) = \mathcal{M}_0 \cap \Delta^2(H) \oplus \mathcal{N}_0 \cap \Delta^2(H)$
(ii) $\varepsilon \in \Delta(G)$, $\Sigma(F)\varepsilon \in \Delta^2(H) \Longrightarrow (f, g)\varepsilon \in \Delta^2(G)$.

PROOF. Let $\varepsilon\Sigma(F) \in \mathcal{M}_0$ and $\delta\Sigma(G) \in \mathcal{N}_0$, with $\delta \in \Delta(F)$ and $\varepsilon \in \Delta(G)$. Since $\Sigma(F)\varepsilon \equiv f\varepsilon \big(\mathrm{mod}\, \Delta^2(H)\big)$, the first statement says that $f\varepsilon + g\delta$ lies in $\Delta^2(H)$ only if each summand does. Let the standard isomorphism $\Delta(H)/\Delta^2(H) \xrightarrow{\sim} H$ be denoted by $\alpha \mapsto [\alpha]$. Then $[\varepsilon]^f[\delta]^g = 1$ implies that $[\varepsilon]^f = [-\delta]^g$ lies in $G^f \cap F^g$. But this intersection is trivial, as is easily seen by considering primary components.

By the same reasoning, $\Sigma(F)\varepsilon \in \Delta^2(H)$ is equivalent to $f\varepsilon \in \Delta^2(G)$. Since $(f, g) = af + bg$ for suitable $a, b \in \mathbb{Z}$, and since $g\varepsilon \in \Delta^2(G)$ anyway, this proves the lemma. ∎

In the next section, we shall only require this simple lemma. The more substantial Lemma 3.2 will be deployed after that.

4. **Constructible units.** We now return to our customary setting. Thus $n = q \cdot p$ is odd, $G_n = \mathrm{Aut}(A) = G_q \times G_p$, and $H_n = G_n/\langle\star\rangle$. Since the involution $\star$ does not lie in either of the subgroups $G_q \times 1$ and $1 \times G_p$ of G_n, these groups have faithful images $\tilde{G}_q$ and $\tilde{G}_p$ in H_n, and

$$H_n = \tilde{G}_q \cdot \tilde{G}_p \quad \text{with} \quad \tilde{G}_q \cap \tilde{G}_p = J, \tag{27}$$

where J is generated by $(-1, 1) \equiv (1, -1) \pmod{\star}$. We let $\tilde{G}_q$, $\tilde{G}_p$, and H_n play the respective roles of F, G, and H in the preceding paragraph.

To decongest the *notation*, we shall use the following conventions:

- The two cyclic automorphism groups are mainly referred to by their generators: ρ for $\tilde{G}_q$ and σ for $\tilde{G}_p$.
- If $\delta \in \Delta(H_n)$ and $\lambda \in \mathbb{Z}H_n$ are such that $\lambda\delta \in \Delta^2(H_n)$, we "abusively" write $w_\delta(x)^\lambda = w_{\lambda\delta}(x)$, even if $\delta \notin \Delta^2(H_n)$.
- We usually allow the same letter (say, δ) to stand at the same time for an element of $\Delta(H_n)$ and its canonical image in $\Delta(H_p)$ or $\Delta(H_q)$.

https://doi.org/10.4153/CJM-1995-006-4 Published online by Cambridge University Press

For instance, the basic G_q-norm relation (14) appears as

$$w_\delta(\xi)^{\Sigma(\rho)} w_\delta(\zeta)^{1-\tau_q} = 1. \tag{28}$$

The purpose of this section is to deal with the group $\Omega(A|p)$ of circular units trivialized by the characters ψ_n, ψ_q, and ψ_1, especially with the subgroup $Y(A|p)$ of constructible units.

PROPOSITION 4.1. *Every element of $Y(A|p)$ has the form*

$$u(x) = w_\delta(x)^{\Sigma(\rho)} w_\delta(x^q)^{\tau_q^{-1}-1}, \tag{29}$$

with $\delta \in \Delta(\tilde{G}_p)$ and $\alpha = \Sigma(\rho)\delta \in \Delta^2(H_n)$.

PROOF. If $u(x) = w_\alpha(x) w_\beta(x^p) w_\gamma(x^q) \in Y(A)$ has both $u(\xi) = 1$ and $u(\eta) = 1$, it is ρ-invariant. Since $Y(A)$ is a direct product, each of the constituent factors of $u(x)$ is itself ρ-invariant. In particular, $\beta = 0$ because multiplication by $(\rho - 1)$ is injective in $\Delta^2(H_q)$. Hence $u(x) = w_\alpha(x) w_\gamma(x^q)$. Moreover, the ρ-invariance of α means that $\alpha = \Sigma(\rho)\delta$ by equation (26). Now the norm relation (28) says $u(\xi) = w_\delta(\zeta)^{\tau_q - 1} w_\gamma(\zeta^q)$, which equals 1 if and only if $w_\gamma(\zeta)^{\tau_q} = w_\delta(\zeta)^{1-\tau_q}$, as was to be shown. ∎

Our next task is to work out a proof of Theorem 0.1, *i.e.*, a description of the finite group $\Omega(A|p)/Y(A|p)$ in terms of A_p. We note that PB1 guarantees an isomorphism

$$\Omega(A|p) \xrightarrow{\sim} \ker_q W(A_p) \tag{30}$$

given by $x \mapsto z$. Here and elsewhere $\ker_q X$ stands for the kernel of the map, induced on a unit group X, by the reduction of coefficients $\mathbb{Z} \longrightarrow \mathbb{F}_q$. We must find out where the isomorphism (30) takes $Y(A|p)$. The answer to that question involves the greatest common divisor m of $h_q = |H_p|$ and $h_p = |H_q|$.

PROPOSITION 4.2. *The substitution $x \mapsto z$ maps $Y(A|p)$ bijectively onto the group*

$$\hat{W}(A_p)^{q-\tau_q} = \{w_\varepsilon(z)^{q-\tau_q} \mid \varepsilon \in \Delta(H_p), m\varepsilon \in \Delta^2(H_p)\}. \tag{31}$$

PROOF. We first have to translate the second part of Lemma 3.3 into the present setting. For $\delta \in \Delta(\tilde{G}_p)$, that lemma says $\Sigma(\rho)\delta \in \Delta^2(H_n)$ if and only if $2m\delta \in \Delta^2(\tilde{G}_p)$, because $2m = (q-1, p-1)$. But this is equivalent to $m\delta \in \Delta^2(H_p)$ since $\tilde{G}_p$ is cyclic.

If $u(x)$ is as in (29), we have $u(z) = w_\delta(z)^{q-1} w_\delta(z^q)^{\tau_q^{-1}-1} = w_\delta(z)^{q-\tau_q}$. By the preceding remark, $m\delta \in \Delta^2(H_p)$ because $\Sigma(\rho)\delta \in \Delta^2(H_n)$,and therefore $u(z) \in \hat{W}(A_p)^{q-\tau_q}$.

Conversely, given $w_\varepsilon(z)^{q-\tau_q}$ with $m\varepsilon \in \Delta^2(H_p)$, we take a pre-image $\delta \in \Delta(H_n)$ for ε. Again by the opening remark, it follows that $\Sigma(\rho)\delta \in \Delta^2(H_n)$, and we can write down $u(x)$ as in (29). ∎

To situate the somewhat unusual group (31) in the general scheme of things, we make the following observation.

https://doi.org/10.4153/CJM-1995-006-4 Published online by Cambridge University Press

SCHOLIUM 4.3. *The group* $\hat{W}(A_p)^{q-\tau_q}/W(A_p)^{q-\tau_q}$ *is cyclic of order* m.

PROOF. Under the standard isomorphism $W(A_p) \simeq \Delta^2(H_p)$, the group we are talking about is $(q-\tau_q)T/(q-\tau_q)\Delta^2(H_p)$, where T consists of all $\delta \in \Delta(H_p)$ which are shifted into $\Delta^2(H_p)$ via multiplication by m. Cyclicity is inherited from $T/\Delta^2(H_p)$, which is canonically identified with the subgroup of order m in H_p.

Let σ^b represent a generator of that group, and consider the corresponding element $(\tau_q - q)(\sigma^b - 1) \in (\tau_q - q)T$. If modulo $(\tau_q - q)\Delta^2(H_p)$ the latter had order k, there would be an $\alpha \in \Delta^2(H_p)$ such that $(\tau_q - q)[\alpha - k(\sigma^b - 1)] = 0$. Since q is not an eigenvalue of τ_q on $\Delta(H_p)$, this would imply $0 \equiv k(\sigma^b - 1)$ modulo $\Delta^2(H_p)$ and hence $m|k$. ∎

REMARKS. By Proposition 4.2, we see that $\Omega(A|p)/Y(A|p)$ is isomorphic (via PB1) to the factor group $\ker_q W(A_p)/\hat{W}(A_p)^{q-\tau_q}$. We shall not be able determine the structure of this group, but we *can* compute its index, at least in principle. In Section 6, we shall first find the index $[\ker_q W(A_p) : W(A_p)^{q-\tau_q}]$—without the "hat"—and then put the hat back on (*i.e.*, divide by m) using the scholium.

To establish Theorem 0.1, we note that $\hat{W}(A_p)^{q-\tau_q}$ could equivalently and perhaps more naturally be described as

$$\hat{W}(A_p)^{q-\tau_q} = \{w_\delta(z)^{q-\tau_q} \mid \delta \in \Delta(G_p), (q-\tau_q)\delta \in \Delta^2(G_p)\}, \tag{32}$$

i.e., the image of $\Delta^2(G_p) \cap (q-\tau_q)\Delta(G_p)$ under the surjection $w(z)\colon \Delta^2(G_p) \longrightarrow W(A_p)$. Indeed, for δ and ε as above, $m\varepsilon \in \Delta^2(H_p) \Leftrightarrow 2m\delta \in \Delta^2(G_p) \Leftrightarrow (q-1)\delta \in \Delta^2(G_p) \Leftrightarrow \big((q-1)+(1-\tau_q)\big)\delta \in \Delta^2(G_p)$.

5. **The kernel.** In this section we come back to the main theme of Section 3: the torsion group of $\Delta(H_n)/\big(\Sigma(\rho)\Delta(H_n) \oplus \Sigma(\sigma)\Delta(H_n)\big)$. Remember that it is cyclic of order $m = (h_q, h_p)$ and generated by the class of $\delta_0 = (h_p/m)\Sigma(\rho) - (h_q/m)\Sigma(\sigma)$.

LEMMA 5.1. *There is an* $\varepsilon_0 \in \Sigma(\rho)\Delta(H_n) \oplus \Sigma(\sigma)\Delta(H_n)$ *such that* $\delta_0 + \varepsilon_0 \in \Delta^2(H_n)$.

PROOF. Since expressions like $(\rho - 1) + (\rho^{-1} - 1)$ are in $\Delta^2(H_n)$, the only terms of δ_0 which might cause problems are those involving elements of order 2 in $\tilde{G}_q \cup \tilde{G}_p$. But there is just one such element ι, and it happens to be in $\tilde{G}_q \cap \tilde{G}_p$. Hence,

$$\delta_0 \equiv \frac{h_p - h_q}{m}(\iota - 1)\big(\mathrm{mod}\,\Delta^2(H_n)\big). \tag{33}$$

If the coefficient $(h_p - h_q)/m$ is even, this lies in $\Delta^2(H_n)$, and there is nothing to show. Let us suppose, therefore, that h_p/m is even and h_q/m is odd. Since h_p/m is the order of σ^{2m}, its being even means that $\iota = \sigma^{2mk}$ for some positive integer k. Since the augmentation of $\Sigma(\rho)$ equals $2h_q$, we have

$$(\sigma^k - 1)\Sigma(\rho) \equiv (\sigma^{2km} - 1)(h_q/m) \equiv (\iota - 1)\big(\mathrm{mod}\,\Delta^2(H_n)\big), \tag{34}$$

because h_q/m is odd. Putting $\varepsilon_0 = (\sigma^k - 1)\Sigma(\rho)$ does the trick. ∎

PROPOSITION 5.2. *The group* $Y(A|p,q)/\big(Y(A|p) \times Y(A|q)\big)$ *is cyclic, and its order equals the greatest common divisor* m'' *of the indices* $[H_q : \langle\tau_p\rangle]$ *and* $[H_p : \langle\tau_q\rangle]$.

PROOF. The map

$$Y(A) \longrightarrow \Delta^2(H_n) \quad \text{by } u(x) = w_\alpha(x)w_\beta(x^p)w_\gamma(x^q) \longmapsto \alpha \tag{35}$$

is injective when restricted to $Y(A|p,q)$. In fact, if we had $u(\xi) = 1$ and $\alpha = 0$, we would get an element $w_\beta(\eta^p) = w_\gamma(\zeta^q)^{-1}$ in the intersection of two essentially disjoint unit groups. In view of Proposition 4.1, this injection of $Y(A|p,q)$ into $\Delta^2(H_n)$ induces an isomorphism

$$Y(A|p) \times Y(A|q) \xrightarrow{\sim} [\Sigma(\rho)\Delta(\tilde{G}_p) \oplus \Sigma(\sigma)\Delta(\tilde{G}_q)] \cap \Delta^2(H_n), \tag{36}$$

with an assist from Lemma 3.3, which allows distributing the $\cap\Delta^2(H_n)$ over the direct sum on the right. Altogether this yields an injection

$$\frac{Y(A|p,q)}{Y(A|p) \times Y(A|q)} \longrightarrow \frac{\Delta(H_n)}{\Sigma(\rho)\Delta(\tilde{G}_p) \oplus \Sigma(\sigma)\Delta(\tilde{G}_q)}, \tag{37}$$

whose image we shall now determine. Since $Y(A|p,q) \subseteq \Omega(A|p,q) = \Omega(A|p) \times \Omega(A|q)$, the group on the left is finite. By Lemma 3.2, its image is generated by the class of $t\alpha_0$, where $t|m$ and $\alpha_0 = \delta_0 + \varepsilon_0$ as in Lemma 5.1. Our task is to find t. Writing $\alpha_0 = \alpha'\Sigma(\rho) + \alpha''\Sigma(\sigma)$, we have

$$w_{\alpha_0}(\xi) = w_{\alpha'}(\zeta)^{\tau_q - 1} w_{\alpha''}(\eta)^{\tau_p - 1}. \tag{38}$$

Therefore $t\alpha_0$ is in the image of our map if and only if there is a $\beta \in \Delta^2(H_q)$ and a $\gamma \in \Delta^2(H_p)$ such that

$$1 = w_{t\alpha'}(\zeta)^{\tau_q - 1} w_\gamma(\zeta^q) \cdot w_{t\alpha''}(\eta)^{\tau_p - 1} w_\beta(\eta^p). \tag{39}$$

Since $\Omega(\zeta) \cap \Omega(\eta) = 1$, both halves of this expression must be trivial separately, so that $t\alpha'(\tau_q - 1) + \tau_q\gamma = 0$ and $t\alpha''(\tau_p - 1) + \tau_p\beta = 0$. In other words, the conditions on t are as follows:

$$\begin{aligned} &\text{(i)} \quad t\alpha'(\tau_q^{-1} - 1) \in \Delta^2(H_p) \text{ and} \\ &\text{(ii)} \quad t\alpha''(\tau_p^{-1} - 1) \in \Delta^2(H_q). \end{aligned} \tag{40}$$

As these are completely symmetric with respect to p and q, we can concentrate on (i). Looking back at Lemma 5.1, we recall that $\alpha' = (h_p/m) + \varepsilon'$ with $\varepsilon' \in \Delta(H_n)$. Hence

$$t\alpha'(\tau_q^{-1} - 1) \in \Delta^2(H_p) \iff t(h_p/m)(\tau_q^{-1} - 1) \in \Delta^2(H_p), \tag{41}$$

which in turn is equivalent to saying that τ_q, raised to the power th_p/m, is trivial in H_p, or finally: th_p/m is a multiple of the order h_p/μ of τ_q in H_p, where $\mu = [H_p : \langle\tau_q\rangle]$.

Actually it is more convenient to reformulate this criterion in terms of the complementary divisor $d = m/t$: it must be such that $\mu/d \in \mathbb{Z}$. Bringing condition (ii) back into the picture, we therefore require that d divide both $[H_p : \langle\tau_q\rangle]$ and $[H_q : \langle\tau_p\rangle]$. That is all, since the condition $d|m$ is now redundant. By Lemma 3.2, d is the order modulo $\Sigma(\rho)\Delta(H_n) \oplus \Sigma(\sigma)\Delta(H_n)$ of the element $t\alpha_0 \in \Delta^2(H_n)$ thus obtained. ∎

In view of the exact sequence (9), this proves Theorem 0.2.

https://doi.org/10.4153/CJM-1995-006-4 Published online by Cambridge University Press

6. **Index comparisons.** In this section, we shall prove Theorem 0.3, that is, compute the order of a typical factor, say $\Omega(A|p)/Y(A|p)$, in the domain of the homomorphism Ξ. Eschewing symmetry, we can temporarily enjoy a simplified notation: $H = H_p$, h its order, $\theta = \zeta + \zeta^{-1}$, $\tau = \tau_q$ (or rather, its image in H).

Parallel to $\ker_q X$ for $X \subseteq U(A)$, we also want to consider

$$\operatorname{im}_q X = \operatorname{im}[X \longrightarrow U\mathbb{F}_q A], \tag{42}$$

and the same *mutatis mutandis* for $X \subseteq U(\xi)$. In particular, we are interested in the inclusion $\operatorname{im}_q W(A_p) \subseteq \acute{U}_1^+ \mathbb{F}_q A_p$, where the acute accent (as in $\acute{U}$ or $\acute{\Omega}$) stands for the kernel of the H_p-norm—NOT the G_p-norm this time.

LEMMA 6.1. $[\ker_q W(A_p) : W(A_p)^{\tau-q}] = [\acute{U}_1^+ \mathbb{F}_q A_p : \operatorname{im}_q W(A_p)]$

PROOF. We use the abbreviation $A_p = K$. Since $W(K)/\ker_q W(K) \simeq \operatorname{im}_q W(K)$, the statement of the lemma is equivalent to the equality

$$[W(K) : W(K)^{\tau-q}] = |\acute{U}_1^+ \mathbb{F}_q K|. \tag{43}$$

Let f be the order of $\tau \in H$, and define $g = h/f$. We shall prove the lemma by showing that each side of (43) is equal to $(q^f - 1)^g/(q-1)$.

(I). For the left side, recall that $W(K) \simeq \mathbb{Z}H/\mathcal{N}(H)$, where $\mathcal{N}(H) \in \mathbb{Z}H$ is the ideal generated by $\Sigma(H)$. Note that $\mathcal{N}(H) \simeq \mathbb{Z}$ as an H-module (with trivial H-action). Now consider the commutative square

$$\begin{array}{ccc} \mathcal{N}(H) & \longrightarrow & \mathbb{Z}H \\ {\scriptstyle 1-q}\downarrow & & \downarrow{\scriptstyle \tau-q} \\ \mathcal{N}(H) & \longrightarrow & \mathbb{Z}H \end{array} \tag{44}$$

as well as the maps

$$W(K) \xrightarrow{\tau-q} W(K) \quad \text{and} \quad \frac{\mathcal{N}(H)}{(1-q)\mathcal{N}(H)} \longrightarrow \frac{\mathbb{Z}H}{(\tau-q)\mathbb{Z}H} \tag{45}$$

induced on the horizontal and vertical cokernels of (44), respectively. By general abstract nonsense, the cokernels of these latter maps are canonically isomorphic. Once we know that the second one is injective, we shall be able to conclude that

$$[W(K) : W(K)^{\tau-q}] = \frac{[\mathbb{Z}H : (\tau-q)\mathbb{Z}H]}{q-1}. \tag{46}$$

To see the desired injectivity, suppose that $\alpha = (\tau - q)\beta$ for $\alpha \in \mathcal{N}(H)$ and $\beta \in \mathbb{Z}H$. Since q cannot be an eigenvalue of τ, the linear map $(\tau - q)$ is invertible on $\mathbb{Q}H$, and $\beta = (\tau-q)^{-1}\alpha \in \mathbb{Q}\mathcal{N}(H) \cap \mathbb{Z}H = \mathcal{N}(H)$.

It remains to identify $[\mathbb{Z}H : (\tau-q)\mathbb{Z}H]$. A *priori*, this is the determinant of the operator $(\tau-q)$ on $\mathbb{Z}H$, *i.e.*, the characteristic polynomial of τ evaluated at q. Now, this polynomial is $(X^f - 1)^g$ by the decomposition of H into g cosets with respect to the cyclic group of order f generated by τ.

(II). The second equality comes from the decomposition of q in the Dedekind ring $\mathbb{Z}[\theta]$. Its Galois group is H, its Frobenius automorphism given by $\tau:\zeta \mapsto \zeta^q$, and its degree of inertia is therefore f. Now $\mathbb{F}_q K \simeq \mathbb{F}_q \oplus \mathbb{F}_q[\zeta]$ implies $U_1^+\mathbb{F}_q K \simeq U\mathbb{F}_q[\theta]$, and hence

$$|U_1^+\mathbb{F}_q K| = (q^f - 1)^g, \tag{47}$$

because g is the number of simple components of the semi-simple ring $\mathbb{F}_q[\theta]$. To get the final result we need only recall that the Galois-norm

$$U^+\mathbb{F}_q[\zeta] = U\mathbb{F}_q[\theta] \longrightarrow \mathbb{F}_q^\times \tag{48}$$

is surjective. Indeed, this well-known fact about relative norms of finite fields clearly remains true even if $\mathbb{F}_q[\theta]$ is not a field, *i.e.* if $g \neq 1$. ∎

Remember that $U^+\mathbb{F}_q A_p \xrightarrow{\sim} U^+\mathbb{F}_q[\zeta]$ is an isomorphism and that $L(\zeta) = \Omega(\zeta)^{\Delta H}$ represents the "liftable" cyclotomic units, *i.e.* those which come from $Y(A_p) = W(A_p)$. We obviously have

$$\operatorname{im}_q L(\zeta) \subseteq \operatorname{im}_q \acute{\Omega}(\zeta) \subseteq \acute{U}^+\mathbb{F}_q[\zeta], \tag{49}$$

with the acute accent as always denoting the elements of H-norm 1. Accordingly the index $[\acute{U}_1^+\mathbb{F}_q A_p : \operatorname{im}_q W(A_p)]$ breaks up into two factors. As we shall see, one of these factors is the order of a cyclic group.

PROPOSITION 6.2. *The group* $\operatorname{im}_q \acute{\Omega}(\zeta)/\operatorname{im}_q L(\zeta)$ *is cyclic of order* $e|m$, *and*

$$(m/e)\cdot[\ker_q W(A_p) : \hat{W}(A_p)^{\tau-q}] = [\acute{U}_1^+\mathbb{F}_q[\zeta] : \operatorname{im}_q \acute{\Omega}(\zeta)]. \tag{50}$$

PROOF. If σ generates G_p, then $(\sigma - 1)$ generates $\Delta(G_p)/\Delta^2(G_p)$. Hence every element of $\Omega(\zeta)$ has the form $v_\sigma(\zeta)^{a+\delta}$ with $a \in \mathbb{Z}$ and $\delta \in \Delta H$, where $v_\sigma(\zeta) = \vartheta(\zeta)^{\sigma-1}$. Since the H-norm of $v_\sigma(\zeta)$ equals $\vartheta(\zeta)^{\star-1} = -1$, we have $v_\sigma(\zeta)^{a+\delta} \in \acute{\Omega}(\zeta)$ if and only if $a = 2b$. Therefore $\operatorname{im}_q \acute{\Omega}(\zeta)/\operatorname{im}_q L(\zeta)$ is generated by the image $\check{v}_\sigma(\zeta)^2 = \operatorname{im}_q v_\sigma(\zeta)^2$.

Now $\check{v}_\sigma(\zeta)^{p-1}$ is liftable since $(p-1) = [\Delta(G_p) : \Delta^2(G_p)]$. On the other hand, $\check{v}_\sigma(\zeta)^{q-1} = \check{v}_\sigma(\zeta)^{\tau-1}$ is liftable because the q-th power acts as the Frobenius automorphism τ over $\mathbb{F}_q$. It follows that $\check{v}_\sigma(\zeta)^{2m}$ is also liftable. This proves the first part of the proposition. The rest is obvious from items 4.3 and 6.1. ∎

REMARK. Obviously, $e = e_q(\zeta)$ as defined in the Introduction, and the right hand side of (50) represents the "defect" $d_q(\zeta)$. In view of Scholium 4.3 and the subsequent remarks, Proposition 6.2 constitutes a reformulation of Theorem 0.3.

N.B. The switching back and forth between G_p and H_p is an irritating but essential ingredient of these deliberations. For instance: whereas G_p acts on $v_\sigma(\zeta)$ via H_p, the liftability of $v_\sigma(\zeta)^{p-1}$ depends on the relation between $v_\sigma(\zeta)$ and $\vartheta(\zeta)$—and the latter does *not* regard $\star$ as trivial.

We conclude this section with a lemma which is sometimes useful, though it is specialized to the case $g = 1$.

https://doi.org/10.4153/CJM-1995-006-4 Published online by Cambridge University Press

LEMMA 6.3. *Suppose that $\mathbb{F}_q[\theta]$ is a field. Then $d_q(\zeta)$ and $m/e_q(\zeta)$ are odd.*

PROOF. It is clear from (50) that we need only prove the oddness of $d_q(\zeta)$. With $v_\sigma(\zeta)$ and $\check{v}_\sigma(\zeta)$ as in the proof of Proposition 6.2, consider the equation

$$\check{v}_\sigma(\zeta)^{1+q+\cdots+q^{h-1}} = -1, \tag{51}$$

which follows from the H-norm of $v_\sigma(\zeta)$ being -1, because the field hypothesis makes the Frobenius τ generate H.

Now, $1 + q + \cdots + q^{h-1}$ is precisely the order of $\acute{U}^+\mathbb{F}_q[\zeta]$, and $\acute{\Omega}(\zeta)$ is generated by $\check{v}_\sigma(\zeta)^2$. Evenness of the index $d_q(\zeta)$ would therefore mean that $\check{v}_\sigma(\zeta)^2$ is trivialized by the power $(1 + q + \cdots + q^{h-1})/2$, contradicting (51). ∎

7. **The cokernel.** Let $L(\xi)$ denote the ψ_n-image of $\Omega(A)$. The first lemma of this section relates $L(\xi)$ to the kernel $\ker_{P,Q}\Omega(\xi)$ of the map

$$\mathrm{red}_P \times \mathrm{red}_Q : \Omega(\xi) \longrightarrow U\mathbb{F}_p[\eta] \times U\mathbb{F}_q[\zeta] \tag{52}$$

which appears as the right vertical arrow in PB0.

LEMMA 7.1 $L(\xi) = Y(\xi) \cdot \ker_{P,Q}\Omega(\xi)$. *In other words, $u \in \Omega(\xi)$ is liftable to $\Omega(A)$ if and only if its image under* $\mathrm{red}_P \times \mathrm{red}_Q$ *lies in* $\mathrm{im}_p\, Y(\eta) \times \mathrm{im}_q\, Y(\zeta)$.

PROOF. Since the restriction

$$\mathrm{red}_P \times \mathrm{red}_Q : Y(\xi) \longrightarrow \mathrm{im}_p\, Y(\eta) \times \mathrm{im}_q\, Y(\zeta) \tag{53}$$

is obviously surjective, any $u \in \Omega(\xi)$ which maps to $\mathrm{im}_p\, Y(\eta) \times \mathrm{im}_q\, Y(\zeta)$ can be adjusted modulo $Y(\xi)$ so as to lie in $\ker_{P,Q}\Omega(\xi)$. Since PB0 is a pull-back, it is clear that any $u \in \ker_{P,Q}\Omega(\xi)$ defines a unit in $\Omega(A)$—with trivial image in $\Omega(A_q) \times \Omega(A_p)$.

Conversely, if $u \in \Omega(\xi)$ lifts to $\Omega(A)$, its $(\mathrm{red}_P \times \mathrm{red}_Q)$-image can be obtained via the natural map $\Omega(A) \longrightarrow Y(A_q) \times Y(A_p)$, hence lies in $\mathrm{im}_p\, Y(\eta) \times \mathrm{im}_q\, Y(\zeta)$. ∎

Intersecting the filtration (17) with $L(\xi)$, we obtain

$$L(\xi) \supseteq L^\circ(\xi) \supseteq L^*(\xi) \supseteq Y(\xi), \tag{54}$$

with $L^\circ(\xi) = Y(\xi)\ker_{P,Q}\Omega^\circ(\xi)$ and $L^*(\xi) = Y(\xi)\ker_{P,Q}\Omega^*(\xi)$, by the preceding lemma. As promised in Theorem 0.4., we shall successively deal with the "slices" $L(\xi)/L^\circ(\xi)$, $L^\circ(\xi)/L^*(\xi)$, and $L^*(\xi)/Y(\xi)$ of our cokernel $L(\xi)/Y(\xi)$.

Throughout the remainder of this section, we use the notation

$$v_a(\xi) = \vartheta(\xi^a)/\vartheta(\xi), \quad v_b(\eta) = \vartheta(\eta^b)/\vartheta(\eta), \quad v_c(\zeta) = \vartheta(\zeta^c)/\vartheta(\zeta), \tag{55}$$

if a, b, c are integers prime to n, q, p, respectively. Accordingly, the formula (16) will be rewritten as

$$V(a, b, c) = v_a(\xi)v_b(\eta)v_c(\zeta)Y(\xi). \tag{56}$$

This is multiplicative in a, b, c, and represents all elements of $\Omega^\circ(\xi)/Y(\xi)$.

https://doi.org/10.4153/CJM-1995-006-4 Published online by Cambridge University Press

PROPOSITION 7.2. *The group $L(\xi)/L^\circ(\xi)$ is cyclic, and its order divides m''.*

PROOF. That group will be generated by some $w = \vartheta(\xi)^{2t} v_a(\xi) v_b(\eta) v_c(\zeta)$ with $t|m$. By Lemma 7.1, we can insist that

$$\operatorname{red}_Q w = \vartheta(\zeta)^{2t} b v_a(\zeta) v_c(\zeta) \tag{57}$$

should equal 1 in $\mathbb{F}_q[\zeta]$. Taking the H_p-norm (which *a fortiori* must be 1), we get

$$p^t = \pm b^{h_p} \quad \textit{i.e.,}\ \tau_p^t \in H_q^{h_p}, \tag{58}$$

because p is the H_p-norm of $-\vartheta(\zeta)^2 = (1-\zeta)(1-\zeta^{-1})$. Putting $\tau_p = \rho^\nu$, where ν is the index $[H_q : \langle \tau_p \rangle]$ and ρ is a suitable generator of H_q, this says that $\rho^{\nu t} = \rho^{k h_p}$ for some integer k, *i.e.*, that $\nu t = k h_p + l h_q$. Therefore $\vartheta(\xi)^{2\nu t} \in \Omega^\circ(\xi)$ and consequently $w^\nu \in \Omega^\circ(\xi)$. Analogously $w^\mu \in \Omega^\circ(\xi)$ for the other index $\mu = [H_p : \langle \tau_q \rangle]$. ∎

REMARK. This proposition clearly covers item (i) of Theorem 0.4.

PROPOSITION 7.3. *There exists a group epimorphism*

$$[\mathbb{F}_q^\times \cap \operatorname{im}_q \Omega(\zeta)] \times [\mathbb{F}_p^\times \cap \operatorname{im}_p \Omega(\eta)] \longrightarrow L^\circ(\xi)/L^*(\xi). \tag{59}$$

PROOF. Suppose that $b \in \mathbb{F}_q^\times \cap \operatorname{im}_q \Omega(\zeta)$, say $b = \operatorname{im}_q v_d(\zeta) w$, for some $d \in \mathbb{F}_p^\times$ and $w \in Y(\zeta)$. Then, choosing $a \in \mathbb{Z}$ such that

$$a \equiv b^{-1} \pmod q \quad \text{and} \quad a \equiv d^{-1} \pmod p, \tag{60}$$

we claim that $v_a(\xi) v_b(\eta) \in L^\circ(\xi)$. Indeed,

$$\operatorname{red}_Q v_a(\xi) v_b(\eta) = \operatorname{im}_q v_a(\zeta) b = \operatorname{im}_q v_a(\zeta) v_d(\zeta) w \in \operatorname{im}_q Y(\zeta), \tag{61}$$

because $v_a(\zeta) v_d(\zeta) \equiv v_{ad}(\zeta)$ modulo $Y(\zeta)$. Likewise $\operatorname{red}_P v_a(\xi) v_b(\eta) = \operatorname{im}_p v_a(\eta) v_b(\eta)$ lies in $\operatorname{im}_p Y(\eta)$. The coset $v_a(\xi) v_b(\eta) L^*(\xi) \in L^\circ(\xi)/L^*(\xi)$ clearly depends only on b. Similarly every $c \in \mathbb{F}_p^\times \cap \operatorname{im}_p \Omega(\eta)$ also determines an element of $L^\circ(\xi)/L^*(\xi)$.

Mapping the pair (b, c) to the product of these two elements, we get a homomorphism as promised in the proposition. To see its surjectivity, let $u = v_a(\xi) v_b(\eta) v_c(\zeta)$ be an arbitrary element of $\ker_{P,Q} \Omega^\circ(\xi)$. Then $\operatorname{red}_Q u = \operatorname{im}_q v_a(\zeta) v_c(\zeta) b \in \operatorname{im}_q Y(\zeta)$ implies $b \in \mathbb{F}_q^\times \cap \operatorname{im}_q \Omega(\zeta)$, and analogously $\operatorname{red}_P u \in \operatorname{im}_p Y(\eta)$ entails $c \in \mathbb{F}_p^\times \cap \operatorname{im}_p \Omega(\eta)$. ∎

REMARK. In order to establish item (ii) of Theorem 0.4, we note first that the map $b \mapsto v_b(\zeta) L^*(\xi)$ kills $b = -1$ (because $V(-1,-1,1)$ is trivial) and hence has at most one half the order of $\mathbb{F}_q^\times \cap \operatorname{im}_q \Omega(\zeta)$. Secondly, the latter is the kernel of the endomorphism $(\sigma - 1)$ on $\operatorname{im}_q \Omega(\zeta)$, and therefore has the same order as the cokernel $\operatorname{im}_q \Omega(\zeta)/\operatorname{im}_q Y(\zeta)$, namely $2e_q(\zeta)$.

PROPOSITION 7.4. *There exists a group epimorphism*

$$G_q^{2e_p(\eta)} \times G_p^{2e_q(\zeta)} \longrightarrow L^*(\xi)/Y(\xi). \tag{62}$$

PROOF. Using the decomposition $G_n = G_q \times G_p$, we shall identify the pre-image of $L^*(\xi)/Y(\xi) \subseteq \Omega^*(\xi)/Y(\xi)$ under the surjection $V\colon G_n \longrightarrow \Omega^*(\xi)/Y(\xi)$. Writing $a = b \times c$ for $a \in G_n = G_q \times G_p$, we note that $\mathrm{red}_P \times \mathrm{red}_Q$ maps $v_a(\xi)$ to $\mathrm{im}_p\, v_b(\eta) \times \mathrm{im}_q\, v_c(\zeta)$. Therefore we must find conditions on b and c for this to lie in $\mathrm{im}_p\, Y(\eta) \times \mathrm{im}_q\, Y(\zeta)$.

If $s \in \mathbb{Z}$ denotes a generator of G_p, the definition of $e_q(\zeta)$ implies that $\nu = 2e_q(\zeta)$ is the smallest positive integer such that $\mathrm{im}_q\, v_s(\zeta)^\nu \in \mathrm{im}_q\, Y(\zeta)$. Indeed this exponent *must* be even, because the H_p-norm of $v_s(\zeta)$ is -1. Since $v_s(\zeta)^\nu \equiv v_{s^\nu}(\zeta)\big(\mathrm{mod}\, Y(\zeta)\big)$, this means that

$$\{c \in G_p \mid \mathrm{im}_q\, v_c(\zeta) \in \mathrm{im}_q\, Y(\zeta)\} = G_p^{2e_q(\zeta)}, \tag{63}$$

as was to be shown. ∎

REMARK. The preceding proposition suffices to prove item (iii) of Theorem 0.4, because the epimorphism in question is the restriction of a map whose full image $\Omega^*(\xi)/Y(\xi)$ has an exponent dividing $2m$—*cf.* the remark following Lemma 2.2.

COROLLARY 7.5. $\big(L^\circ(\xi)/Y(\xi)\big)^m$ *is the product of two cyclic groups of order* ≤ 2, *which are trivial, respectively, if* $m/e_p(\eta)$ *or* $m/e_q(\zeta)$ *are odd, respectively.*

PROOF. By the proof Proposition 7.3, $V(a,b,c) \in L^\circ(\xi)/Y(\xi)$ implies

$$V(a,b,c)^m = V(a^m, b^m, c^m) = V(\pm a^m, 1, 1), \tag{64}$$

since $\big(\mathbb{F}_q^\times \cap \mathrm{im}_q\, \Omega(\zeta)\big)^{2m} = \big(\mathbb{F}_p^\times \cap \mathrm{im}_p\, \Omega(\eta)\big)^{2m} = 1$, and thus b^m and c^m are ± 1. On the other hand, $V(\pm a^m, 1, 1) \in \big(\Omega^*(\xi)/Y(\xi)\big)^m$, because $\star \in G_n^m$ and hence $\pm a^m = d^m$ for some $d \in G_n$. Therefore

$$\big(L^\circ(\xi)/Y(\xi)\big)^m \subseteq \big(\Omega^*(\xi)/Y(\xi)\big)^m \cap \big(L^*(\xi)/Y(\xi)\big). \tag{65}$$

Letting r and s be generators of $G_q \times 1 \subset G_n$ and $1 \times G_p \subset G_n$, respectively, note that $\big(\Omega^*(\xi)/Y(\xi)\big)^m$ is a Klein 4-group generated by $v_r(\xi)^m$ and $v_s(\xi)^m$. But Proposition 7.4 says, $v_r(\xi)^m \in L^*(\xi) \Leftrightarrow 2e_p(\eta) | m$, and $v_s(\xi)^m \in L^*(\xi) \Leftrightarrow 2e_q(\zeta) | m$. ∎

RECALL. By Lemma 6.3, $m/e_q(\zeta)$ is odd whenever $\mathbb{F}_q[\theta_p]$ is a field.

ACKNOWLEDGEMENTS. The author is deeply indebted to Jürgen Ritter (Augsburg), who sustained this work with generous donations of his time, attention, and ingenuity. Thanks are due also to DFG (Germany) and NSERC (Canada) for their financial assistance, and to Augsburg University for its hospitality.

REFERENCES

1. H. Bass, *The Dirichlet unit theorem, induced characters, and Whitehead groups of finite groups*, Topology **4**(1966), 391–410.
2. G. H. Cliff, S. K. Sehgal, A. R. Weiss, *Units of integral group rings of metabelian groups*, J. Algebra **73**(1981), 167–185.
3. G. Higman, *The units of group rings*, Proc. London Math. Soc. (2) **46**(1940), 231–248.
4. K. Hoechsmann, *Constructing units in commutative group rings*, Manuscripta Math. **75**(1992), 5–23.
5. ———, *Local units and circular index in abelian p-group rings*, J. Pure Appl. Alg. **82**(1992), 253–272.
6. M. A. Kervaire and M.P. Murthy, *On the projective class group of cyclic groups of prime power order*, Coment. Math. Helv. **52**(1977), 415–452.
7. L. Washington, *Introduction to cyclotomic fields*, Springer, New York, 1982.

Department of Mathematics
University of British Columbia
Vancouver, British Columbia
V6T 1Y4