Resenhas IME-USP 2002, Vol. 5, No. 4, 279 - 292.

Units in irregular elementary abelian group rings

Klaus Hoechsmann

Abstract: If p is a regular prime and A an elementary abelian p-group, every unit in the integral group ring of A is a product of units coming from cyclic subgroups of A. If p is irregular, there is always a shortfall described by a finite abelian p-group. The shape of the latter depends on a conjecture about global versus local cyclotomic units which has been verified for $p < 10,000$.

Key words: Units, group rings, irregular primes, cyclotomic units.

1. Introduction

If somebody asked how an otherwise sane person could expend so much time and energy on the arithmetic of finite group rings, and (yawn!) commutative ones at that, the answer would have to be: by sheer stubbornness. In this paper, we shall revisit the initial context — elementary abelian p-groups, where the tale to be told is relatively simple. It started in late '83, when Sudarshan — on a short leave from the Alberta snow — proposed that we try to find an explicit formula for the units in the group ring $\mathbb{Z}A$ of an abelian group $A = \langle x, y \rangle$ with $x^p = y^p = 1$, where p is an odd prime — for starters, take $p = 5$.

A simple question, good fun for a week-end. Such an A (a plane over $\mathbb{F}_p$) has exactly $p + 1$ cyclic subgroups of order p, and if *their* units are known (which is certainly true for $p = 5$) it should be just a matter of fitting them together. Sudarshan reached into his back of tricks [Se] and filled me in on basic facts, such as Higman's result (the only torsion units are $\pm A$) and the canonical split:

$$U\mathbb{Z}A = \pm A \times U_1^+\mathbb{Z}A\,, \tag{1.1}$$

where the subscript 1 means the coefficient sum ("augmentation") being $= 1$, and the superscript $+$ means staying fixed under the involution coming from $z \mapsto z^{-1}$ ($z \in A$). Therefore $U_1^+\mathbb{Z}A$ was a torsion free abelian group ("lattice") whose rank was known — via Dirichlet and Wedderburn — to equal $(p+1)(p-3)/2$; i.e. $= 6$ for $p = 5$.

Sudarshan was not teasing me: he really did want to know a basis for $U_1^+\mathbb{Z}A$. He knew that $U_1^+\mathbb{Z}C$ for the cyclic group $C = \langle z \rangle$ of order 5 was generated by the single unit $w(z) = z - 1 + z^{-1}$, and therefore had a natural candidate for the desired basis, namely $\{\, w(z_i) \mid 0 \le i \le 5\}$, where $\langle z_i \rangle = C_i$ ranges over the non-trivial cyclic subgroups of A. Thus, the problem was to prove the bijectivity

Partially supported by the Pacific Institute for the Mathematical Sciences.

Mathematics Subject Classification : 20-06, 16-06, 11R18.

of the map

$$\alpha : \prod_{C \subseteq A} U_1^+ \mathbb{Z}C \longrightarrow U_1^+ \mathbb{Z}A\,, \tag{1.2}$$

where C runs over the non-trivial cyclic subgroups of A, and the product is direct. By counting ranks, we concluded that surjectivity — i.e., trivial cokernel — was sufficient. We quickly brought in the complementary map, a slightly modified Wedderburn, namely

$$\beta : U_1^+ \mathbb{Z}A \longrightarrow \prod_{K} U_1^+ \mathbb{Z}K\,, \tag{1.3}$$

where K runs over the cyclic *factor* groups of A. Source and target of the composite $\gamma = \beta \circ \alpha$ are obviously isomorphic, and can be made identical by means of a non-degenerate pairing on A. Hence γ can be represented by a 6-by-6 matrix, whose determinant would tell us the size of the cokernel of γ. We laboured to get the matrix right and finally computed the determinant, which turned out to be 125. In the next case, $p = 7$, the components $U_1^+ \mathbb{Z}C$ would be lattices of rank 2, and the entries of the matrix representing γ would have to endomorphism of these lattices. We tried to make some headway — in vain: no clear idea about γ, much less about α. That was the week-end's work.

This narrative will soon have to move into a higher gear, but before it does, let us review the very simple make-up of $U_1 \mathbb{Z}C$ for C of order p. The isomorphism $\mathbb{Q}C \xrightarrow{\sim} \mathbb{Q} \times \mathbb{Q}[\zeta]$, where ζ is a non-trivial pth root of unity, clearly takes $\mathbb{Z}C$ into $\mathbb{Z} \times \mathbb{Z}[\zeta]$, but *not onto* it. To come from $\mathbb{Z}C$, a pair $(a) \times (c_0 + c_1\zeta + \cdots + c_{p-1}\zeta^{p-1})$ must be $\mathbb{F}_p$-compatible, that is, $\sum_i c_i$ (which is defined only modulo p) must agree with a in $\mathbb{F}_p$. This condition is also sufficient: since $1 + \zeta + \cdots + \zeta^{p-1} = 0$, the coefficient sum can be modified by any multiple of p without changing $c_0 + c_1\zeta + \cdots + c_{p-1}\zeta^{p-1}$. In other words, $\mathbb{Z}C$ is the fibre-product (in the obvious sense) of $\mathbb{Z}$ and $\mathbb{Z}[\zeta]$ over $\mathbb{F}_p$. Units inherit this property: if each component of an element in a fibre-product has an inverse, so does the element itself. In particular, $U_1 \mathbb{Z}C$ can be seen as the kernel of the map $U\mathbb{Z}[\zeta] \longrightarrow \mathbb{F}_p^\times$ given by the coefficient sum. Since our main interest is in "real units", we shall restate this more formally for them:

$$1 \longrightarrow U_1^+ \mathbb{Z}C \longrightarrow U^+ \mathbb{Z}[\zeta] \longrightarrow \mathbb{F}_p^\times \longrightarrow 1 \tag{1.4}$$

is a short exact sequence. This is no great adjustment, as the transition from $U_1 \mathbb{Z}C$ to $U_1^+ \mathbb{Z}C$ is just the projection onto the second factor in (1.1); i.e., modification by elements of C. We shall soon relate it another short exact sequence, namely

$$1 \longrightarrow \Delta^2 \mathbb{Z}G \longrightarrow \Delta \mathbb{Z}G \xrightarrow{e} G \longrightarrow 1\,, \tag{1.5}$$

where $G = \mathrm{Aut}(C) = \mathbb{F}_p^\times$. For any finite G, the ideal $\Delta\mathbb{Z}G$ is the kernel of the augmentation map $\mathbb{Z}G \longrightarrow \mathbb{Z}$, and in the abelian case, $e : \sum a_\sigma(\sigma - 1) \mapsto \prod \sigma^{a_\sigma}$ defines a homomorphism from $\Delta\mathbb{Z}G$ (additive) onto G, a kind of poor man's exponential map, whose kernel is the square of $\Delta\mathbb{Z}G$.

We map (1.5) into (1.4) in two steps: $\Delta\mathbb{Z}G \longrightarrow U\mathbb{Z}[\zeta] \longrightarrow U^+\mathbb{Z}[\zeta]$, the second being the projection onto the second factor in $\langle\zeta\rangle \times U^+\mathbb{Z}[\zeta]$, the analogue of (1.1), while the first associates to every generator $(\sigma - 1)$ of $\Delta\mathbb{Z}G$ the unit $(\zeta - 1)^{\sigma-1} = (\zeta^\sigma - 1)/(\zeta - 1)$. Altogether we have a G-homomorphism $u^+ : \Delta\mathbb{Z}G \longrightarrow U^+\mathbb{Z}[\zeta]$ whose image $U^\oplus\mathbb{Z}[\zeta]$ is known as the group of *real cyclotomic* units.

To see that this yields a morphism of exact sequences, note that $u^+(\sigma - 1) = \zeta^a(1 + \zeta + \cdots + \zeta^{c-1})$ with a suitable a, and with c such that $\sigma : \zeta \mapsto \zeta^c$. Its image in $\mathbb{F}_p^\times$ is therefore c, the same as $e(\sigma - 1) = \sigma$ in light disguise. In other words, u^+ is compatible with the natural identifcation $G \longrightarrow \mathbb{F}_p^\times$. It follows that the only real cyclotomic units which can be lifted to $U\mathbb{Z}C$ are those coming from $\Delta^2\mathbb{Z}G$. Since $\Delta^2\mathbb{Z}G$ is generated by products $(\sigma_b - 1)(\sigma_c - 1)$, corresponding to automorphisms $z \mapsto z^b$ and $z \mapsto z^c$, the image group $U_1^\oplus\mathbb{Z}C$ is generated by elements of the form

$$w(b, c, z) = z^a \frac{1 + z^c + \cdots + z^{c(b-1)}}{1 + z + \cdots + z^{b-1}}, \tag{1.6}$$

again with a suitably (but uniquely) chosen. If $b = 2$ and $k = (c - 1)/2 = -a$, this comes out as the symmetric alternating sum of c terms $z^{-k} - z^{-k+1} + \cdots - z^{k-1} + z^k = w(2, c, z)$.

By one of the miraculous theorems of number theory, the index of $U^\oplus\mathbb{Z}[\zeta]$ in $U^+\mathbb{Z}[\zeta]$ is the class number h_p^+ of the real quadratic field $\mathbb{Q}[\zeta + \zeta^{-1}]$. Though difficult to compute, it seems to be $= 1$ in many cases (cf. [Wa; p. 420]). However, its very finiteness is comforting: it ensures that $U^\oplus\mathbb{Z}[\zeta]$ has the full rank of $U^+\mathbb{Z}[\zeta]$, namely $(p - 3)/2$, and ditto for $U^\oplus\mathbb{Z}C$ and $U^+\mathbb{Z}C$ (which are separated by the same index). Since G acts on $U^+\mathbb{Z}[\zeta]$ via $H = \mathbb{F}_p^\times/\{\pm 1\}$, we can tighten up the map from (1.5) to (1.4) to a pair of surjections

$$\Delta\mathbb{Z}H \longrightarrow U^\oplus\mathbb{Z}[\zeta] \quad \text{and} \quad \Delta^2\mathbb{Z}H \longrightarrow U_1^\oplus\mathbb{Z}C\,, \tag{1.7}$$

which, for reasons of equal rank, are *isomorphisms*. In fact, the cyclotomic units are the only easily computable ones, and luckily their index h_p^+ in $U_1^+\mathbb{Z}C$ seems to be always prime to p. This conjecture is attributed to Kummer or to Vandiver by different people and is being verified for ever larger primes p. Cyclotomic units can be defined for any A as forming the pre-image of their cousins under β. The reader of these pages has the choice of either believing in Vandiver (at least for the prime in question) or reading $U^\oplus$ wherever we write U^+. Leaving that question open is one of the reasons for the outlandish notation involving Φ, et al. The second reason is a notational clarity which also emphasises the purely functorial nature of some of our arguments.

Now back to the narrative. After several months of sporadic communication (e-mail was yet in its infancy) we knew that the index of $\gamma = \beta \circ \alpha$ — cf. (1.2) and (1.3) above — was p^N, with $4\,N = n\,(p - 3)\,(1 + p + \cdots + p^n)$, where $n + 1$ was the minimal number of generators of A. A proof of this can be gleaned from those

of Lemma 1 and Corollary 1 of Section 2 below, but let no one believe that we were working on that simple proof the whole time: our various initial attempts were very convoluted. Since β is injective, the cokernel of α (whose triviality we were hoping for) is included in that of γ, and hence a finite p-group. Hence we could involve the p-adic numbers without affecting it. This was done as indicated in Lemma 2 and its Corollary. Getting back from $\mathbb{Z}_p$ to $\mathbb{Z}$ can be done (strange as it may seem) by reducing both to $\mathbb{F}_p$: a non-trivial cokernel of α would still show up for $\alpha \otimes \mathbb{F}_p$; but over a field injective is also surjective, hence all is well modulo a little proviso:

$$(U_1^+ \mathbb{Z}C)^p \longrightarrow U_1^+ \mathbb{Z}C \longrightarrow U_1^+ \mathbb{F}_p C \tag{1.8}$$

must be *exact*. As we all know, this is characteristic of *regular* primes ("Kummer's Lemma"), and so we [HS] had the desired bijectivity of α in the regular case.

Was regularity necessary or just a by-product of this proof? It turned out to be necessary. In [H2] the $\mathbb{F}_p$-dimension of $\operatorname{coker}(\alpha) \otimes \mathbb{F}_p$ — the number of cycles in a direct decomposition — is shown to lie between $(1 + p + \cdots + p^n)\,\delta_p$ and $(1 + p + \cdots + p^{n-1})\,\delta_p$, where $n+1$ is again the "rank" of A, and δ_p is a number known as the *irregularity index* of p. Actually, an exact but less attractive count involving binomial coefficients is given. Using methods of Fröhlich [Fr], the paper also relates the size of $\operatorname{coker}(\alpha)$ to that of a certain group of projective ideal classes.

All this and more — in particular, about more general A — is summarized in [H3]. The present paper will restrict its attention to elementary abelian groups, where life is easier and results more abundant. It will give evidence to suggest that $\operatorname{coker}(\alpha)$ is itself elementary, in other words: $\operatorname{coker}(\alpha) = \operatorname{coker}(\alpha) \otimes \mathbb{F}_p$.

2. Preliminaries.

Let F be a field of q elements, $\mathcal{V}$ the category of finite dimensional vector-spaces over F. Consider a functor $\Phi : \mathcal{V} \to \mathcal{L}$, where $\mathcal{L}$ is the category of lattices, i.e., of finitely generated torsion-free $\mathbb{Z}$-modules. Note that every object V of $\mathcal{V}$ is acted on by $G = \operatorname{Aut}(F) = F^\times$, and so is every $\Phi(V)$. We shall *assume that the absolutely irreducible characters of* $\Phi(F)$ *come in non-trivial reciprocal pairs.*

Let V be an $(n+1)$-dimensional F-space, L and H the sets of its subspaces of dimensions 1 and n, respectively. Consider a family of maps $a_l : F \to V$, $(l \in L)$ such that $\operatorname{im}(a_l) = l$ and another family $b_h : V \to F$, $(h \in H)$ such that $\ker(b_h) = h$. Composing $\alpha = \prod_{l \in L} \Phi(a_l)$ with $\beta = \prod_{h \in H} \Phi(b_h)$, we then obtain a map

$$\prod_{l \in L} \Phi(F) \to \Phi(V) \to \prod_{h \in H} \Phi(F)\,. \tag{2.1}$$

Using any non-degenerate bilinear form φ on V, we get a bijection $H \to L$ which allows us to identify the source of α with the target of β and to regard $\gamma = \beta \circ \alpha$ as an endomorphism of $\Lambda = \prod_{l \in L} \Phi(F)$. G acts diagonally on this product.

To represent γ by a matrix, let Q be the set of $x \in V$ such that $x = a_l(1)$ for some $l \in L$, and let R be the set of $y \in V$ such that $\varphi(-, y) = b_h$ for some $h \in H$. For the sake of tidiness, let us make $R = Q$ by adjusting each y by a suitable factor $c \in F$; i.e. replace the map b_h by cb_h. On the index set $Q \times Q$, we then get a matrix $\mathcal{M}$ whose (x, y)-entry is $\varphi(x, y)$ interpreted as an *endomorphism of* $\Phi(F)$, either null or some element of G. Let m be the cardinality of Q.

Lemma 1. *With V, φ, Q as above, let μ be a non-trivial homomorphism $G \longrightarrow R^\times$ where R is an integral domain with $(q-1) \in R^\times$. On the index set $Q \times Q$ consider the matrix $\mathcal{M}_\mu$ whose (x, y)-entry equals $\mu\big(\varphi(x, y)\big)$. Then, if $\nu = \mu^{-1}$, we have $\mathcal{M}_\mu \mathcal{M}_\nu^t = q^n I_m$, where superscript t means matrix-transpose.*

Proof. We must show that, for $x, y \in Q$,

$$(*) \qquad S(x, y) = \sum_{z \in Q} \mu\big(\varphi(x, z)\big)\, \mu^{-1}\big(\varphi(y, z)\big) = q^n \delta(x, y)\,,$$

where the δ is Kronecker's. To prove this identity, consider the wider sum

$$T(x, y) = \sum_{v \in V} \mu\big(\varphi(x, v)\big)\, \mu^{-1}\big(\varphi(y, v)\big) = (q-1) S(x, y)\,,$$

the latter equality being due to the fact that each summand of $T(x, y)$ is left fixed by the change $x \mapsto cx$ with $c \in F^\times$.

(1) Writing $v = (u, a)$ with $u \in U = (x)^\perp$ and $a = \varphi(x, v)$, we get

$$T(x, x) = \sum_{u \in U} \sum_{a \in F^\times} \mu(a)\, \mu^{-1}(a) = q^n (q-1)\,.$$

(2) For $x \neq y$, writing $v = (u, a, b)$ with $u \in U = (x, y)^\perp$, $a = \varphi(x, v)$ while $b = \varphi(y, v)$, we get

$$T(x, y) = \sum_{u \in U} \sum_{a, b \in F^\times} \mu(a)\, \mu^{-1}(b) = q^{n-1} \sum_{a \in F^\times} \mu(a) \sum_{b \in F^\times} \mu^{-1}(b) = 0\,,$$

since μ is non-trivial.

Corollary 1. *The cokernel of γ has order q^N for suitable N. In particular, γ is injective.*

Proof. Since γ is an endomorphism of the free $\mathbb{Z}$-module $X = \prod \Phi(F)$, the order of its cokernel equals $|\det(\gamma)|$. Extending scalars to $R = \mathbb{C}$, we turn X into a direct sum of m-dimensional $\mathbb{C}$-spaces W_μ on each of which G acts via the appropriate character μ. By our assumption, characters occur in reciprocal pairs (μ, ν), for which the Lemma yields $|\det \mathcal{M}_\mu| \cdot |\det \mathcal{M}_\nu| = q^{nm}$, and $|\det(\gamma)|$ is a product of these.

For $F = \mathbb{F}_p$ and $R = \mathbb{Z}_p$, all characters μ are powers of Teichmüller's $\tau : G \longrightarrow \mathbb{Z}_p^\times$, which coincides modulo p with the identification $G = \mathbb{F}_p^\times$. If $\mu = \tau^d$ we shall write $\mathcal{M}_d$ instead of $\mathcal{M}_\mu$. The reciprocal character then is $\tau^{d'}$, where $d + d' = p - 1$. Now let $\overline{\mathcal{M}}_d = \mathcal{M}_d \otimes \mathbb{F}_p$ denote $\mathcal{M}_d$ with entries read modulo p.

Lemma 2: *The rank of $\overline{\mathcal{M}}_d$ equals the binomial coefficient $C(n+d, n)$.*

Proof: Using any basis of V over $\mathbb{F}_p$, the elements of V are identified with $(n+1)$-tuples $x = (x_0, x_1, \ldots, x_n)$, and the bilinear form φ might as well be the old "dot product"

$$\varphi(x, y) = \sum_{k=0}^{n} x_k y_k, \qquad \text{whence} \qquad \overline{\mathcal{M}}_d(x, y) = \sum_{k=0}^{n} (x_k y_k)^d .$$

As in Lemma 1, the index set of this square matrix is Q — a set of "projective points" — but again, the rank does not change if we expand it to all of $\mathbb{F}_p^{n+1}$: we are only adjoining multiples of rows and columns which are already there. Thus we obtain a $p^{n+1} \times p^{n+1}$ matrix, each of whose rows, now labelled $c = (c_0, c_1, \ldots, c_n)$, consists of all possible evaluations $\mathbb{F}_p^{n+1} \longrightarrow \mathbb{F}_p$ of the d-form

$$g_c(T) = \Big(\sum_{k=0}^{n} c_k T_k \Big)^d ,$$

where $T = (T_0, T_1, \ldots, T_n)$. Now, since $\mathbb{F}_p$ has more than d elements, any polynomial of degree $\leq d$ is characterised by its evaluations (as is easily proved by induction on n with inhomogeneous polynomials). Hence the desired rank equals the dimension of the space of d-forms generated by the $g_c(T)$, thus at most that of the space of *all* d-forms; i.e., the number of monomials of degree d in $(n+1)$ indeterminates, in other words, the number of $j = (j_0, \ldots, j_n)$ with $j_0 + \cdots + j_n = d$. This number, call it $h(n, d)$, obviously equals $h(n-1, d) + h(n, d-1)$, whence by an easy induction $h(n, d) = C(n+d, n)$.

Now consider a new matrix, with rows labelled by $c = (c_0, c_1, \ldots, c_n) \in \mathbb{F}_p^{n+1}$, and columns by the $j = (j_0, \ldots, j_n)$ just described, which at (c, j) has the entry $c_0^{j_0} c_1^{j_1} \cdots c_n^{j_n}$. Every column represents all evaluations of the d-form $T_0^{j_0} T_1^{j_1} \cdots T_n^{j_n}$. As these are linearly independent, so are the $C(n+d, n)$ columns of the new matrix. Since

$$g_c(T) = \sum_j c_0^{j_0} c_1^{j_1} \cdots c_n^{j_n} \cdot C(d, j) T^j ,$$

where $C(d, j) = (d!/j_0! \cdots j_n!)$ and $T^j = T_0^{j_0} T_1^{j_1} \cdots T_n^{j_n}$, the space spanned by the $g_c(T)$ has the maximal dimension $C(n+d, n)$, as was to be shown.

Corollary 2. *If $\{p^{r_i} \mid i = 1, \ldots, m\}$, with $r_1 \geq \cdots \geq r_m$, are the elementary divisors of $\mathcal{M}_d$ in $\mathbb{Z}_p$, we have $r_1 = n$ and $r_m = 0$. The first strict inequality is $n > r_{i+1}$ for $i = C(d'+n, n)$, and the last one is $r_j > 0$ for $m - j = C(d+n, n)$.*

Proof. By Lemma 2, the rank of $\mathcal{M}_d \otimes \mathbb{F}_p$ is $C(d+n, n)$. This makes the last $C(d+n, n)$ elementary divisors equal to 1, whence the last assertion of this

corollary. By linear algebra, there exist $L, R \in \mathrm{GL}_m(\mathbb{Z}_p)$ such that $L\mathcal{M}_d R = \Delta_d$ is diagonal with the p^{r_i} as non-zero entries. By Lemma 1, this implies $p^n \Delta_d^{-1} = R^{-1}\mathcal{M}_{d'}^t L^{-1} = \Delta_{d'}$. Hence, the elementary divisors of $\mathcal{M}_{d'}$ are $p^{n-r_m} \geq \cdots \geq p^{n-r_1}$, whence the first assertion.

At this point, the multiplicative language — writing A instead of $\mathcal{V}$, and thinking ab instead of $v + w$ — becomes more natural. We now consider two functors which associate with every elementary abelian p-group A a suitable $\mathbb{Z}_p$-lattice: $\Phi_p(A) = U_1^+ \mathbb{Z}_p A$ and $\Psi_p(A) = \Delta^+ \mathbb{Z}_p A$. In each case, the target object is complete under the $\mathbb{Z}_p$-topology. From [HS], we obtain the next lemma.

Lemma 3. *There is a natural isomorphism* $\log : U_1^+ \mathbb{Z}_p A \longrightarrow \Delta^+ \mathbb{Z}_p A$ *defined by the usual power series for* $\log(1+\delta)$ *with* $\delta \in \Delta^+ \mathbb{Z}_p A$.

Note: Without the superscript + in the definitions of Φ_p and Ψ_p the lemma is false. (For $a, b \in A$ not in the same cyclic subgroup, the equation $\log(ab) = \log(a) + \log(b)$ is clearly impossible.)

The trick is to prove this lemma first for $A = C$ of order p. Since $\Delta^+ \mathbb{Z}_p C$ is generated by terms like $(1-x) + (1-x^{-1}) = -x^{-1}(1-x)^2$, it lies in $\left(\Delta \mathbb{Z}_p C\right)^2$. This makes the exp-series converge (the log-series is no problem) and the exp-log mechanism function in the usual manner. That leads to the two vertical isomorphisms in the following diagram

$$\begin{array}{ccccc} \prod_C U_1^+ \mathbb{Z}_p C & \xrightarrow{\alpha_p} & U_1^+ \mathbb{Z}_p A & \xrightarrow{\beta_p} & \prod_K U_1^+ \mathbb{Z}_p K \\ \simeq \downarrow & & \downarrow & & \simeq \downarrow \\ \prod_C \Delta^+ \mathbb{Z}_p C & \longrightarrow & \Delta^+ \mathbb{Z}_p A & \longrightarrow & \prod_K \Delta^+ \mathbb{Z}_p K\,, \end{array} \tag{2.2}$$

in which C and K run over all cyclic subgroups and factor-groups, respectively. The injectivity of the middle vertical arrow now follows from that of the upper right β_p, which is a form of the Wedderburn decomposition. Surjectivity follows from the fact that the lower left arrow is bijective, since different $C's$ intersect only in the neutral element. The following is a by-product.

Corollary 3: *The natural map* $\alpha_p : \prod_C U_1^+ \mathbb{Z}_p C \longrightarrow U_1^+ \mathbb{Z}_p A$ *is bijective.*

Our third and last lemma concerns the subring $\prod'_C \mathbb{Z}C$ of $\prod_C \mathbb{Z}C$ consisting of those m-tuples in which all components have the same augmentation.

Lemma 4: *The following diagram is a pull-back of rings,*

$$\begin{array}{ccc} \mathbb{Z}A & \xrightarrow{\beta} & \prod'_K \mathbb{Z}K \\ \downarrow & & \downarrow \\ \mathbb{Z}_p A & \xrightarrow{\beta_p} & \prod_K \mathbb{Z}_p K\,. \end{array} \tag{2.3}$$

Proof: Any $f = \sum_{a \in A} f(a)\, a \in \mathbb{Q}A$, where A is any finite abelian group, can be reconstructed from its Wedderburn components $\chi(f)$ by the usual trick,

$$|A|\, f(a) = \sum_{\chi} \mathrm{Tr}_\chi\left[\chi(a^{-1})\, \chi(f)\right], \tag{2.4}$$

of equating two evaluations of the regular character on

$$a^{-1}f = f(a)\cdot 1 + \sum_{x\neq 1} f(ax)x.$$

Now let A be elementary abelian of order p^{n+1}. Apart from the trivial character χ_0, there are $m = (1+p+\cdots+p^n)$ characters χ, each factoring over a cyclic group $K_\chi = A/\ker(\chi)$. For $f \in \mathbb{Q}A$, and some fixed $\chi \neq \chi_0$, let g denote the image of f in $\mathbb{Q}K_\chi$. Since χ and χ_0 are the only rational characters on K_χ, the formula yields

$$p\,g(c) = \chi_0(f) + \mathrm{Tr}_\chi\left[\chi(c^{-1})\,\chi(f)\right], \tag{2.5}$$

for every $c \in K_\chi$, which is, of course, the image $a_\chi \in K_\chi$ for some $a \in A$. Substituting this result into the formula (2.4), we get

$$|A|\,f(a) = \chi_0(f) + \sum_{\chi\neq\chi_0}\left[pf_\chi(a_\chi) - \chi_0(f)\right],$$

where we have written f_χ instead of g. Grouping together the terms $\chi_0(f)$ and dividing by p, we finally have

$$p^n f(a) = -(1+p+\cdots+p^{n-1})\,\chi_0(f) + \sum_{\chi\neq\chi_0} f_\chi(a_\chi), \tag{2.6}$$

for any $f \in \mathbb{Q}A$. Remember that, given a set $\{f_\chi \in \mathbb{Z}K_\chi\}$ of cyclic group-ring elements with a *common augmentation*, the Wedderburn isomorphism ensures the existence of a unique $f \in \mathbb{Q}A$ such that $\beta(f) = \{f_\chi\} \in \prod'\mathbb{Z}K_\chi$, the product running over $\chi \neq \chi_0$. This f will be in $\mathbb{Z}A$ if and only if the right hand side of (2.6) is always in $p^n\mathbb{Z}$. Equation (2.6) shows this to be the case, if f is known to be in $\mathbb{Z}_pA$. This proves the lemma.

If $f_\chi \in U_1\mathbb{Z}K_\chi$ for each χ, the resulting $f \in \mathbb{Z}A$ will also be in $U_1\mathbb{Z}A$ since it is invertible in the maximal order of $\mathbb{Q}A$ (cf. [RS, Proposition 3]). We conclude

Corollary 4: *The following diagram is a pull-back*

$$\begin{array}{ccc} U_1\mathbb{Z}A & \xrightarrow{\beta} & \prod_K U_1\mathbb{Z}K \\ \downarrow & & \downarrow \\ U_1\mathbb{Z}_pA & \xrightarrow{\beta_p} & \prod_K U_1\mathbb{Z}_pK\,. \end{array}$$

3. The Main Results.

With A, C, K having the same meanings as in Section 2, consider the following diagram of $\mathbb{Z}_pG$-modules:

$$\begin{array}{ccccc} \prod_C \hat{\Phi}C & \xrightarrow{\alpha} & \hat{\Phi}A & \xrightarrow{\beta} & \prod_K \hat{\Phi}K \\ \downarrow\lambda & & \downarrow\lambda & & \downarrow\lambda \\ \prod_C \Phi_pC & \xrightarrow{\alpha_p} & \Phi_pA & \xrightarrow{\beta_p} & \prod_K \Phi_pK\,, \end{array} \tag{3.1}$$

where Φ_pA stands for $U_1^+\mathbb{Z}_pA$, while ΦA could denote either $U_1^+\mathbb{Z}A$ or $U_1^{\oplus}\mathbb{Z}A$. Originally, ΦA is a $\mathbb{Z}$-lattice, but the "hat" over it means $\otimes\mathbb{Z}_p$ or equivalently — since the λ are inclusions induced by $\mathbb{Z} \hookrightarrow \mathbb{Z}_p$ — the topological closure in Φ_pA. In fact, all arrows represent injections, the upper horizontal ones by Corollary 1, for instance. We could invoke Wedderburn for the injectivity of β_p and point to the bijectivity of α_p obtained in Corollary 3.

The commutative square on the right of (3.1) is a pull-back on account of Corollary 4. Actually, the latter applies to ΦA, not $\hat{\Phi}A$. To see that it carries over, think of β_p and λ as inclusions. Then, in $\prod_K \Phi_pK$, we have

$$\Phi A = \Phi_pA \cap \prod_K \Phi K \quad \Longrightarrow \quad \hat{\Phi}A = \Phi_pA \cap \prod_K \hat{\Phi}K\,, \tag{3.2}$$

because Φ_pA is closed and open. This is just a simple generality about subsets E and F of a topological space: if E is closed and open, the closure of $E \cap F$ equals $E \cap \hat{F}$.

The object of interest in this section is the cokernel of α. Actually, it is $\hat{\alpha}$ which is shown in (3.1), but since the cokernel of the unadorned α is a finite p-group, it will not be distorted by this shift to the completions. Continuing to work in $\prod_K \Phi_pK$, we have:

$$\lambda\beta(\hat{\Phi}A) = \gamma_p\Big(\prod_C \Phi_pC\Big) \cap \prod_C \lambda(\hat{\Phi}C), \tag{3.3}$$

where the C's and K's have been identified (as usual) by means of a bilinear form on A. The cokernel of α can be computed as

$$\operatorname{coker}(\alpha) = \operatorname{im}\beta/\operatorname{im}\gamma \simeq \operatorname{im}\lambda\beta/\operatorname{im}\lambda\gamma = \operatorname{im}\lambda\beta/\operatorname{im}\gamma_p\lambda\,. \tag{3.4}$$

Using (3.3) and (3.4), we now get

$$\operatorname{coker}(\alpha) \simeq \frac{\gamma_p(X_p) \cap \lambda(\hat{X})}{\gamma_p\lambda(\hat{X})}\,, \tag{3.5}$$

where $\hat{X}$ and X_p stand for the direct products of the $\hat{\Phi}C$ and Φ_pC, respectively.

Remember that $\hat{\Phi}A$ and $\Phi_p A$ are completely reducible $\mathbb{Z}_p G$-modules, and so, of course, are $\hat{\Phi}C$ and $\Phi_p C$. In fact, each irreducible submodule of the latter two is just a rank-one $\mathbb{Z}_p$ on which G acts via one of the even powers of the Teichmüller character $\tau : G \to \mathbb{Z}_p^\times$. The restriction $\lambda_d : (\hat{\Phi}C)_d \longrightarrow (\Phi_p C)_d$ is just multiplication with some $\theta_d \in \mathbb{Z}_p$.

Going back to the context of Corollary 2, remember the dth slice $\mathcal{M}_d$ of the matrix representing γ_p seen as an endomorphism of $\prod_C \Phi_p C$, and let $\mathcal{C}(\mathcal{M}_d) \subseteq (\mathbb{Z}_p)^m$ denote the $\mathbb{Z}_p$-submodule spanned by the columns of $\mathcal{M}_d$. The dth slice of (3.5) then looks like

$$\operatorname{coker}(\alpha_d) = \frac{\mathcal{C}(\mathcal{M}_d) \cap \theta_d \cdot (\mathbb{Z}_p)^m}{\theta_d \cdot \mathcal{C}(\mathcal{M}_d)}. \tag{3.6}$$

As in Corollary 2, left and right multiplication by Gaussian matrices turns $\mathcal{M}_d$ into a diagonal matrix Δ_d, with diagonal entries $p^{r_1} \geq \ldots \geq p^{r_m}$, say. Putting $\operatorname{ord}_p(\theta_d) = t_d$ and $\mu_i = \max(r_i, t_d)$, we note that $p^{r_i}\mathbb{Z}_p \cap \theta_d \mathbb{Z}_p = p^{\mu_i}\mathbb{Z}_p$, and therefore

$$\operatorname{coker}(\alpha_d) \simeq \frac{\mathcal{C}(\Delta_d) \cap p^{t_d} \cdot \mathbb{Z}_p^m}{p^{t_d} \cdot \mathcal{C}(\Delta_d)} = \sum_{i=1}^{m} p^{\mu_i}\mathbb{Z}_p / p^{t_d + r_i}\mathbb{Z}_p \,. \tag{3.7}$$

If $r_i \geq t_d$, then $\mu_i = r_i$ and $p^{\mu_i}\mathbb{Z}_p / p^{t_d+r_i}\mathbb{Z}_p \simeq \mathbb{Z}/p^{t_d}\mathbb{Z}$. On the other hand, if $r_i < t_d$ then $\mu_i = t_d$, and $p^{\mu_i}\mathbb{Z}_p / p^{t_d+r_i}\mathbb{Z}_p \simeq \mathbb{Z}/p^{r_i}\mathbb{Z}$. We therefore have

$$\operatorname{coker}(\alpha_d) \simeq \sum_{r_i \geq t_d} \mathbb{Z}/p^{t_d}\mathbb{Z} + \sum_{r_i < t_d} \mathbb{Z}/p^{r_i}\mathbb{Z} \,. \tag{3.8}$$

If p is *regular* at d, then $t_d = 0$, this yields a trivial cokernel, as expected.

Theorem 1: *The following are equivalent:*

(i) *For every elementary abelian p-group, the cokernel of α_d is elementary abelian.*

(ii) *For the elementary abelian group of order p^3, the cokernel of α_d is elementary abelian.*

(iii) *The cokernel of $\lambda_d : (\hat{\Phi}C)_d \longrightarrow (\Phi_p C)_d$ has order less than p.*

Proof: Condition (iii) means that $t_d = \operatorname{ord}_p(\theta_d)$ is at most 1, and in that case, (3.8) shows that the $\operatorname{coker}(\alpha_d)$ is elementary abelian for *any* A. By Corollary 2, the first $C(d'+n, n)$ exponents r_i are equal to p^n. Thus, if $n = 2$ (i.e. A of order p^3), the cokernel would *not* be elementary abelian, *unless* these initial p^2's where cut off by t_d being less than 2.

Proposition 1: *For t_d to be less than two, it is sufficient that* $\log\big(\lambda_d w(a,b,x)\big)$ *lies outside $p^2\mathbb{Z}_p$ for some $a, b \in \mathbb{Z}$. Given $a, b \in \mathbb{Z}$, this is also necessary, unless $(a^d - 1)(b^d - 1) \in p\mathbb{Z}$.*

Proof: The first statement is clearly true for *any* $u \in U_1^+\mathbb{Z}C$: if $\log\big(\lambda_d(u)\big)$ lies outside $p^2\mathbb{Z}_p$, the ideal it generates is $p\mathbb{Z}_p$ or $\mathbb{Z}_p$.

For the second statement, recall that the $\mathbb{Z}H$-isomorphism $w : \Delta^2 H \xrightarrow{\sim} U_1^{\oplus}\mathbb{Z}C$, mentioned in the Introduction, links $(\sigma_a - 1)(\sigma_b - 1)$ to $w(a,b,x)$. If we wish to know whether the projection $\hat{\Phi}(C) \longrightarrow \hat{\Phi}(C)_d \simeq \mathbb{Z}_p$ takes $w(a,b,x)$ to a unit, we can check the image of $(\sigma_a - 1)(\sigma_b - 1)$ under the corresponding projection $\mathbb{Z}_p \otimes \Delta^2(H) \longrightarrow \mathbb{Z}_p$ — which is nothing but our ring homomorphism τ^d. Now we finish the argument by pointing out that $\big(\tau^d(a) - 1\big)\big(\tau^d(b) - 1\big)$ is congruent to $(a^d - 1)b^d - 1)$ modulo p.

4. Calculation and Conjecture.

This section will deal with the logarithm of $\lambda\big(w(2,3,x)\big) = (x^{-1} - 1 + x) = 1 + (x^{-1} - 2 + x)$. With $\delta(x) = x^{-1} - 2 + x = x^{-1}(1-x)^2$, whose conjugates $\delta(x^j)$ obviously generate $\Delta^+\mathbb{Z}C$, we therefore have $w(2,3,x) = 1 + \delta(x)$. Working in $\mathbb{Z}_p$ modulo p^2, we easily see (leaving out the fastidious λ) that

$$\log w(2,3,x) = \sum_{n=1}^{p} (-1)^{n-1}\delta(x)^n/n \tag{4.1}$$

with no further terms, because $\delta(x)^p \equiv 0$ modulo p^2. To compute the terms of this sum, we note that $x^{-n}(1-x)^{2n}$ equals

$$\sum_{i=0}^{2n} (-1)^i \binom{2n}{i} x^{i-n} = \sum_{j=1}^{n} (-1)^{n-j} \binom{2n}{n-j} \delta(x^j)\,. \tag{4.2}$$

The first of these sums extends over all of the $2n$th line of Pascal's triangle, the second one — after putting $i + j = n$ and grouping x^{-j} with $-x^j$ — catches only the part to the left of the middle term, which gets gobbled up in the process, since the result must lie in ΔC. The right hand side can be interpreted as the result of the $\mathbb{Z}_pG$-element

$$\Lambda_n = \sum_{j=1}^{n} (-1)^{n-j} \binom{2n}{n-j} \sigma_j \tag{4.3}$$

acting on $\delta(x) \in \Delta^+\mathbb{Z}_pC$, where σ_j denotes the automorphism $x \mapsto x^j$, for $1 \le j \le p-1$, and $\sigma_p = 0$ since $\delta(x^p) = 0$. Altogether we now have

$$\log w(2,3,x) = -\sum_{n=1}^{p} \frac{(-1)^n}{n} \Lambda_n \cdot \delta(x) \tag{4.4}$$

This makes sense even for $n = p$, because p divides the relevant binomial coefficients.

Now remember that $\Delta^+\mathbb{Z}_pC$ splits into rank-one pieces $(\Delta^+\mathbb{Z}_pC)_d$, with $2 \le d = 2k \le (p-1)$ corresponding to one of the characters of H, i.e., the *even* characters

of G. These are the even powers τ^{2k} of the Teichmüller character $\tau : G \longrightarrow \mathbb{Z}_p^\times$, which is the unique extension of the identification $G \longrightarrow \mathbb{F}_p^\times$. We therefore have

$$\tau^d(\Lambda_n) = \sum_{j=1}^{n}(-1)^{n-j}\binom{2n}{n-j}\tau(j)^d\,, \tag{4.5}$$

with the understanding that $\tau(p) = 0$. Since we are ultimately interested in doing this calculation modulo p^2, that is, in the ring $\mathbb{Z}_p^{(2)} = \mathbb{Z}/p^2\mathbb{Z}$, it behooves us to note that $\tau : G \longrightarrow \left(\mathbb{Z}_p^{(2)}\right)^\times$ takes the form $\sigma_j \mapsto j^p$.

Instead of directly applying this to (4.5), we first prepare the ground for an elementary lemma by writing $j^{pd} = F_d(j) + G_d(j)$, whose two components are obtained by raising $j^p = j + (j^p - j)$ to the dth power, getting

$$F_d(j) = (1-d)j^d + d\,j^{d+p-1} \qquad \text{and} \qquad G_d(j) = j^d\sum_{\nu=2}^{d}\binom{d}{\nu}\left(j^{p-1}-1\right)^\nu. \tag{4.6}$$

For the elegant proof of the following lemma, we are indebted to Joel Friedman of UBC.

Lemma 5: Let $t < 2n$ be a positive, even integer. Then

$$\sum_{j=1}^{n}(-1)^j\binom{2n}{n-j}j^t = 0\,. \tag{4.7}$$

Proof: On the ring $\mathbb{Z}[X]$ of polynomials, consider the shift operator $S : f(X) \mapsto f(X-1)$ as well as the identity operator I. Since $(I-S)$ decapitates monomials, it lowers the degree of any polynomial. Therefore $(I-S)^{2n}X^t$ must vanish. Expanding $(I-S)^{2n}$ and noting that S^i maps X to $X-i$ yields the result by setting $X = n$, and $j = n - i$. In principle, the sum runs from $i = 0$ to $i = 2n$, that is, j from n to $-n$, but the even parity of t gives the same result on both sides of the middle in Pascal's $2n$th line, for instance $0 \le i < n$, i.e., $0 < j \le n$. Done.

With $\tau(j)^d = F_d(j) + G_d(j)$ substituted in (4.5), the first summand will now vanish identically by the lemma, as long as $d < 2n - (p-1)$, while the second obviously vanishes modulo p^2 for all $j < p$, and yields an intelligible result for $j = p$.

Proposition 2: *Let $s = (p-1+d)/2$. For the equivalent conditions of* Theorem 1 *to be satisfied, it is sufficient that*

$$\sum_{n=1}^{s}\frac{1}{n}\sum_{j=1}^{n}(-1)^j\binom{2n}{n-j}j^{pd} \not\equiv 0 \pmod{p^2}\,,$$

in $\mathbb{Z}_p$. This is also necessary, unless $(2^d-1)(3^d-1) \in p\mathbb{Z}$.

Proof: We shall prove $\tau^d(\Lambda_n/n)$ vanishes in $\mathbb{Z}_p^{(2)}$ for any positive $n \leq p$ and even d such that $2 < d < 2n - (p-1)$. Since $F_d(j)$ as defined in (4.6) has degree $d + (p-1)$, Lemma 5 ensures that

$$\frac{1}{n}\sum_{j=1}^{n}(-1)^{n-j}\binom{2n}{n-j}j^{pd} = \frac{1}{n}\sum_{j=1}^{n}(-1)^{n-j}\binom{2n}{n-j}G_d(j) \tag{4.8}$$

because the analogous sum with $F_d(j)$ is zero even in $\mathbb{Q}$. Now for $n < p$, the right hand side of (4.8) lies in $p^2\mathbb{Z}_p$, because this is obvioulty true for every $G_d(j)$.

The case $n = p$ is more delicate. First a minor adjustment: since $\tau^d(p) = 0$, the left hand side of (4.8) is not quite the same as $\tau^d(\Lambda_p/p)$, but the difference (namely p^{pd-1}) is irrelevant. On the right, we now have

$$\frac{1}{p}\sum_{j=1}^{p}(-1)^{1+j}\binom{2p}{p-j}\cdot j^d\sum_{\nu=2}^{d}\binom{d}{\nu}\left(j^{p-1}-1\right)^{\nu} \tag{4.9}$$

For $j \neq p$, the first of these factors is certainly in $\mathbb{Z}$, and the second vanishes modulo p^2. The obstruction to vanishing in $\mathbb{Z}_p^{(2)}$ is therefore the summand corresponding to $j = p$, to wit:

$$p^{d-1}\sum_{\nu=2}^{d}\binom{d}{\nu}(-1)^{\nu} = p^{d-1}(d-1)\,, \tag{4.10}$$

which occurs only for $d = 2$, where it takes on the value p. This finishes the proof.

The expression displayed in Proposition 2 was computed for all irregular primes $p < 10,000$ and their "bad" indices d. It always vanished modulo p (*irrégularité oblige*) but never modulo p^2. This suggests a *conjecture*, namely that

if A is an elementary abelian p-group, so is $\mathrm{coker}(\alpha)$,

and raises a question: are there secret treaties between irregular pairs (p, d), which prohibit p from dividing $(2^d - 1)(3^d - 1)$?

Acknowledgment

Most of this work was done in the pleasant environment of the Institut Girard Desargues at the Université Claude Bernard Lyon 1. The author wishes to express his sincere gratitude to its Director Olivier Mathieu for offering this hospitality, and to thank all the charming staff and colleagues who made the daily tramway trip something to look forward to.

REFERENCES

[Fr] Fröhlich, A., On the classgroup of integral grouprings of finite abelian groups. Mathematika 16 (1969), 143 - 152

[H1] Hoechsmann, K., Functors on finite vector spaces and units in abelian group rings. Can. Math. Bull. 29(1), 1986, 79 - 83

[H2] — , Units and class-groups in elementary abelian group rings. J. Pure and Appl. Alg. 47 (1987), 253 - 264

[H3] —, On the arithmetic of commutative group rings; in Group Theory, Algebra, Number Theory (Ed.: H.G. Zimmer). Walter de Gruyter, Berlin. (1996), 145 - 201

[HS] —, Sehgal, S.K., Units in regular elementary abelian group rings. Arch. d. Math. 47 (1986), 413 - 417

[HSW] —, —, Weiss, A., Cyclotomic units and the unit group of an elementary abelian group ring. Arch. d. Math. 45 (1985), 5 -

[RS] Ritter, J., Sehgal, S.K., Integral group rings of some p-groups. Can. J. Math. 32 (1982), 233 - 246

[Se] Sehgal, S.K., Topics in Group Rings. Marcel Dekker, N.Y. (1978)

[Wa] Washington, L., Introduction to Cyclotomic Fields, 2nd Ed. Springer Verlag, N.Y. (1996)

Klaus Hoechsmann
Department of Mathematics
University of BC
Canada V6T 1Z2
e-mail: hoek@math.ubc.ca
Vancouver, BC