Unit Bases in Small Cyclic Group Rings.

by

KLAUS HOECHSMANN

Department of Mathematics, University of British Columbia,
Vancouver, B.C., V6T 1Y4, Canada.

ABSTRACT:

Extending an idea of Bass, one can construct a large torsion-free group $\mathcal{Y}(A)$ of units in the integral group ring $\mathbb{Z}A$ of any finite abelian group A. This group of *constructible* units is "good" in two ways: it easily allows the selection of explicit sets of independent generators (bases), and it is typically of low (often trivial) index in the the full unit group of $\mathbb{Z}A$. The present paper deals with cases where $\mathcal{Y}(A)$ does not suffice to describe the full unit group, but where it is nevertheless possible to produce bases of the latter by using constructible units together with *co-induced* ones.

AMS Subject Classifications: 11T22, 20C05.

This work was supported by an operating grant from NSERC (Canada) and by the hospitality of SFB 343 at the University of Bielefeld (Germany).

1. Variations on a theme of Bass.

Any finite group $\mathcal{G}$ is the union of finite cyclic groups C, and most methods of constructing units in the integral group ring $\mathbb{Z}\mathcal{G}$ start from known subgroups of finite index in the unit groups $\mathcal{U}\mathbb{Z}C$ of the latter. As mentioned in the talks of Jespers and Sehgal, the standard generators of these, for $C =< x >$ and $|C| = n$, are the *Bass cyclic units*

$$u_m(x, a) = \left(1 + x + \cdots + x^{a-1}\right)^m + \frac{1 - a^m}{n} \left(1 + x + \cdots + x^{n-1}\right), \tag{1.1}$$

where m is a fixed multiple of Euler's $\phi(n)$ and a a variable integer prime to n. To interpret this formula, let us write $s_\nu(x) = 1 + x + \cdots + x^{\nu-1}$ for any positive integer ν. For any n-th root $\zeta \neq 1$ of unity, $s_a(\zeta)$ is the cyclotomic unit $(\zeta^a - 1)/(\zeta - 1)$, and $u_m(\zeta, a)$ is its m-th power since $s_n(\zeta)$ vanishes. The second term in $u_m(x, a)$ is rigged to yield $u_m(1, a) = 1$. The idea is to turn $s_a(x)$ into a unit by taking a power which reduces $s_a(1) = a$ to 1 modulo n.

A less radical way of cancelling $s_a(1)$ is by division modulo n: take b such that $ab \equiv 1 \pmod{n}$, and consider

$$v(x, b, c) = s_a(x^b)\, s_b(x^c) + \frac{1 - ab}{n}\, s_n(x)\,, \tag{1.2}$$

where c is another integer prime to n. Why use x^b and x^c instead of just x, and why omit the parameter a on the left hand side? The reason is that $s_a(x^b)$ is a kind of inverse to $s_b(x)$, because $s_a(x^b)s_b(x) = s_{ab}(x)$ equals 1 modulo $s_n(x)$. Hence $v(x, b, c)$ is characterized by the equation

$$v(x, b, c)\, s_b(x) = s_b(x^c)\,, \tag{1.3}$$

which is readily verified by substituting all possible n-th roots of unity (including 1) for x. An analogous characterization of the original Bass units would involve

$$u_m(x, a)\, (x - 1)^m = (x^a - 1)^m \tag{1.4}$$

as well as $u_m(1, a) = 1$. Multiplying both sides of (1.3) by $(x - 1)(x^c - 1)$ yields the relation $(x^b - 1)(x^c - 1) \equiv (x - 1)(x^{bc} - 1)$ modulo the group generated by the $v(x, b, c)$ — whence by an easy induction $(x^c - 1)^\mu \equiv (x - 1)^{\mu-1}(x^{c^\mu} - 1)$ modulo the same group. For $\mu = m$, this leads to $(x^c - 1)^m \equiv (x - 1)^m$ and, via (1.4), the observation that *$u_m(x, a)$ is contained in the group generated by the $v(x, b, c)$.*

The index of this inclusion is rather large, however, and grows at a more than exponential rate. Modulo the *trivial* units $\pm x^k$, it is a modest 2×10^3 for $n = 11$ but a stately 2×10^{96} for $n = 101$, yet in both cases the $v(x, b, c)$ generate the whole unit group $\mathcal{U}\mathbb{Z}C$ — again up to trivial units — cf. [H2, Section 3]. To stop trivial units once and for all from cluttering this narrative, let us glue them to the generators — changing every $v(x,b,c)$ to

$$w(x,b,c) = x^{(c-1)(1-b)/2} v(x,b,c)\,. \tag{1.5}$$

The new unit is *symmetric* in the sense that $w(x^{-1},b,c) = w(x,b,c)$, because (1.3) can be rewritten with $v(x,b,c)$ replaced by $w(x,b,c)$ and $s_b(x)$ by $t_b(x) = x^{(1-b)/2}s_b(x)$. The latter is defined even when $(b-1)/2$ is not integral — as then n is odd and $x^{1/2}$ equals $x^{(n+1)/2}$. It clearly satisfies $t_b(x^{-1}) = t_b(x)$.

It is important to keep in mind that $w(x,b,c)$ formally depends on n and should by rights be denoted $w_n(x,b,c)$. However, the substitutionn $x \mapsto z$ transforming $w(x,b,c)$ into $w(x',b,c)$ makes sense for any x' (anywhere) whose order n' divides n. In fact, if $b' \equiv b$ and $c' \equiv c$ modulo n', we have $w_n(x,b,c) = w_{n'}(x',b',c')$. This is why the n does not need to show up in the notation.

The group $\mathcal{W}(C)$ generated by the $w(x,b,c)$ contains no trivial units: it is *torsion-free.* In fact, it is explicitly isomorphic to the square of the augmentation ideal in the group ring $\mathbb{Z}H_n$, where H_n is the group obtained from $G_n = (\mathbb{Z}/n\mathbb{Z})^\times$ by working modulo $\{\pm 1\}$ — cf. [H2, Section 2]. The isomorphism, which is compatible with the action of H_n, associates $w(x,b,c)$ with the element $(\tau_b - 1)(\tau_c - 1) \in \mathbb{Z}H_n$, where $\tau_c \in H_n$ comes from $c \in \mathbb{Z}$ in the obvious way. If H_n is cyclic — for instance, if n is a prime power — this means that $\mathcal{W}(C)$ is generated by the H_n-orbit $\{w(x^\sigma,b,c) \mid \sigma \in H_n\}$ for fixed b and c, as long as τ_b and τ_c are (not necessarily distinct) generators of H_n. The product over the whole orbit equals 1, but that is the only relation: omit any element, and you have a basis of $\mathcal{W}(C)$.

The $\mathcal{W}(C)$ are well-behaved not only individually but also collectively. On the category of finite cyclic groups, $\mathcal{W}$ is a functor which preserves epimorphisms as well as monomorphisms. If A is a finite abelian group, $\mathcal{U}\mathbb{Z}A$ contains one $\mathcal{W}(C)$ for every cyclic subgroup $C \subseteq A$, but results of Bass (for cyclic A) and Bass-Milnor (for any abelian A) guarantee that the product $\mathcal{Y}(A)$ of all these $\mathcal{W}(C)$ is *direct*. We shall call $\mathcal{Y}(A)$ the group of *constructible* units in $\mathbb{Z}A$. This is not the place to give fuller explanations or even more general statements of these facts — the reader who wishes to pursue them will find pointers in [Ba], [H2], [H6], or [Se] — but the following theorem will serve as a reference for our purposes.

Theorem 1.1: *Let A be a finite abelian group of exponent n, and suppose that H_n is cyclic. If $H_n =< \tau_b >=< \tau_c >$ (with b and c not necessarily distinct), then $\mathcal{Y}(A)$ is generated by the set $\{w(z,b,c) \mid z \in A\}$; a basis of $\mathcal{Y}(A)$ is obtained by dropping one element from each H_n-orbit of this set.*

The advantage of admitting two different generators of H_n is the extra freedom to choose convenient generating units. For instance, if $H_n =< \tau_2 >=< \tau_c >$, with c odd, we get the *alternating* units $w(x,2,3) = x^{-1} - 1 + x, \quad w(x,2,5) = x^{-2} - x^{-1} + 1 - x + x^2$, etc. These work for many primes, such as 5, 7, 11, 13, 19, 23, 29, 37, … and their powers and triples (but not for 17, 31, 41, …), as well as for certain other composites such as 35, 55, 77, 143, …

To describe where $\mathcal{Y}(A)$ stands in the hierarchy of unit groups, we shall now review some of these — continuing with a finite abelian A and omitting the $\mathbb{Z}$ from the notation wherever we risk no confusion. Since units come in pairs $\pm u$, we can restrict our attention to the group $\mathcal{U}_1(A)$ of units whose coefficient sum ("augmentation") is $+1$. We have already seen that every $\mathcal{W}(C)$, and hence $\mathcal{Y}(A)$, lies in the *symmetric* part $\mathcal{U}_1^+(A)$ of $\mathcal{U}_1(A)$ — but this also includes the subgroup $A_2 \subseteq A$ generated by elements of order 2 (if any). To avoid even those trivial units, we invoke Lemma 2.6 of [CWS], which gives direct decompositions

$$\begin{aligned} \mathcal{U}_1(A) &= A \times \mathcal{U}_*(A) \\ \mathcal{U}_1^+(A) &= A_2 \times \mathcal{U}_*(A)\,, \end{aligned} \tag{1.6}$$

where $\mathcal{U}_*(A)$ *is* torsion-free. It is the kernel of the map $\mathcal{U}_1(A) \to A$ by $\sum c_z\, z \;\mapsto\; \prod z^{c_z}$, which — miraculously — is a homomorphism. We shall sometimes write $\mathcal{U}_*^+(A)$ to stress the fact that $\mathcal{U}_*(A) \subseteq \mathcal{U}_1^+(A)$ automatically. Luckily $\mathcal{Y}(A) \subseteq \mathcal{U}_*(A)$ without any further adjustment — cf. [H2, Proposition 2.3]. Most importantly, the inclusion has *finite index.*

The most serious draw-back of $\mathcal{Y}(A)$ is that it consists entirely of circular units. If $\zeta \neq 1$ is an n-th root of unity, we have

$$v(\zeta, b, c) = \frac{(\zeta^{bc} - 1)/(\zeta^c - 1)}{(\zeta^b - 1)/(\zeta - 1)}\,, \tag{1.7}$$

and $w(\zeta, b, c)$ is the same multiplied by some power of ζ. Any unit in $\mathbb{Z}[\zeta]$ composed by products and quotients from elements like $(\zeta^\mu - 1)$ and ζ^ν is called *cyclotomic*, and any unit in $\mathbb{Z}A$ having cyclotomic images under all non-trivial characters of A is called *circular.* The situation, then, is as follows:

$$\mathcal{Y}(A) \;\subseteq\; \mathcal{U}_*^\oplus(A) \;\subseteq\; \mathcal{U}_*(A)\,, \tag{1.8}$$

where $\mathcal{U}_*^\oplus(A)$ denotes the circular units in $\mathcal{U}_*(A)$. The index $\big[\mathcal{U}_*(A) : \mathcal{Y}(A)\big]$ is finite, the top part $\big[\mathcal{U}_*(A) : \mathcal{U}_*^\oplus(A)\big]$ depending on ideal class numbers h_μ^+ which are notoriously hard to compute — cf. [Wa, p.420]. If one wanted a basis for $\mathcal{U}_*(A)$ in any particular case, one could presumably begin with a basis of $\mathcal{Y}(A)$ and extend it by laborious numerical procedures. For many A of small exponent, however, $\mathcal{U}_*(A)$ fortunately equals $\mathcal{U}_*^\oplus(A)$, and here things look a lot brighter. They are brightest for groups of prime order.

Theorem 1.2: *If C has prime order p, then $\mathcal{U}_*^\oplus(C)$ equals $\mathcal{W}(C)$, and its index in $\mathcal{U}_*(C)$ is the class number h_p^+.*

In particular, $h_p^+ = 1$ implies $\mathcal{U}_*(C) = \mathcal{W}(C)$. According to [Wa, p.421], this happens for about three quarters of the primes less than ten thousand, in particular for every $p < 163$.

For $\mathcal{U}_*(C)$ to be non-trivial, p must be at least 5 — so that $\mathcal{U}_*(C) = \mathcal{U}_1^+(C)$ and $\mathcal{U}_*^\oplus(C) = \mathcal{U}_1^\oplus(C)$. The theorem then flows from two sources. The first is the obvious pull-back of ring homomorphisms

$$\begin{tikzcd} \mathbb{Z}C \arrow[r] \arrow[d] & \mathbb{Z}[\zeta] \arrow[d] \\ \mathbb{Z} \arrow[r] & \mathbb{F}_p\,, \end{tikzcd} \tag{1.9}$$

which gives rise to exact sequences of unit groups $1 \to \mathcal{U}_1^?(C) \to \mathcal{U}^?(\zeta) \to \mathcal{U}\mathbb{F}_p \to 1$, where the question mark can stand for $\oplus$ or $+$ or nothing at all. This is enough to conclude that $\big[\mathcal{U}_1^+(C) : \mathcal{U}_1^\oplus(C)\big] = \big[\mathcal{U}^+(\zeta) : \mathcal{U}^\oplus(\zeta)\big]$, which equals h_p^+ by a classical result of number theory (cf. [Wa, Theorem 8.2]).

The second source of the theorem is the fact that $\mathcal{U}_1^\oplus(C)$ and $\mathcal{W}(C)$ have the same image in $\mathcal{U}(\zeta)$. This is fairly easy to see for $|C| = p$, but since it is also true (and more difficult) for higher powers, we state it formally for later reference. It is presented in [H6] as Proposition 3.3 but goes back to Theorem 1.3 of [HR].

Lemma 1.3: *If C is cyclic of prime power order, and χ is an injection of C into the multiplicative group of a field, $\mathcal{U}_1^\oplus(C)$ and $C_2 \times \mathcal{W}(C)$ have the same image under χ.*

For $|C| = p > 3$, the equality $\mathcal{U}_1^\oplus(C) = \mathcal{W}(C)$ now follows from the aforementioned exactness of the sequence $1 \to \mathcal{U}_1^\oplus(C) \to \mathcal{U}^\oplus(\zeta) \to \mathcal{U}\mathbb{F}_p \to 1$.

Much more is known about $\mathcal{Y}(A)$ for finite abelian p-groups, for instance, that it is always of p-power index in $\mathcal{U}_*^\oplus(A)$, and actually equal to it whenever p is a *regular* prime. Such matters occupy a large part of [H6]. The following pages are dedicated to the study of units in $\mathbb{Z}A$ which are *not* constructible. We shall, however, need the following analogue of the lemma above. It is a special case of Theorem 0.4 stated in the Introduction and proved in Section 7 of [H4].

Lemma 1.4: *If A is cyclic of order pq, where p and q are primes with $(p-1, q-1) \leq 2$, and if χ is an injection of A into the multiplicative group of a field, then $\mathcal{U}_1^\oplus(A)$ and $A_2 \times \mathcal{Y}(A)$ have the same image under χ.*

The main focus of this paper will be the construction of *bases* for $\mathcal{U}_*^\oplus(A)$ in situations where this cannot be done with $\mathcal{Y}(A)$ alone.

Example: If $A =< y, z >$ with $y^2 = z^{37} = 1$, the index of $\mathcal{Y}(A)$ in $\mathcal{U}_*^\oplus(A) = \mathcal{U}_*(A)$ is known to be 3 — cf. [H2, p. 22]. Consider the group ring element

$$e(y,z) = 1 + (1+y)\big(7\,T_{18}(z) - 5\,T_{18}(z^2) - 36\big)\,, \tag{1.10}$$

where T_{18} denotes the trace over the group of order 18 in $\mathrm{Aut}(A^2)$. This is clearly symmetric. In fact it is a unit — with inverse $e(y, z^2)$ — but not a constructible one.

Since $\mathcal{W}(A_2)$ is trivial, we have $\mathcal{Y}(A) = \mathcal{W}(A^2) \times \mathcal{W}(A)$. If we wish to work with the convenient alternating unit $w(z, 2, 5) = z^{-2} - z^{-1} + 1 - z + z^2$ in $\mathcal{W}(A^2)$, we shall have to go with $w(yz,39,5) \in \mathcal{W}(A)$ in order to have a generator of $\mathcal{Y}(A)$ in the sense of Theorem 1.1. To obtain a basis of $\mathcal{U}_*(A)$ we start with a basis of $\mathcal{W}(A^2)$ and adjoin to it $e(y,z)$ as well as the H_{74}-orbit of $w(yz,39,5)$ diminished by $w(yz^9,39,5)$ and $w(yz^{18},39,5)$.

The workings of this will be explained in Section 4 below. Similar tricks can be performed on groups of order p^2. They all involve "co-induced" units in abelian group rings which are "small" in a special sense.

2. Co-induced units.

Let A be a finite abelian group of exponent n, and suppose that H_n is cyclic. We shall say that A is *small* if its order equals the product pq of two — *not necessarily distinct* — prime numbers. Since the case $|A| = 4$ is trivial, let us agree that p is always odd. This definition covers three very different types of A: cyclic and elementary abelian groups of order p^2 as well as certain cyclic groups of composite order pq. We are mainly interested in the cyclic cases, but allow elementary groups to stay in the game for most of this section.

The cyclicity of H_n is, of course, automatic for $n = p^2$. Apart from its role in the premise of Theorem 1.1, it has the function — for $p \neq q$ — of enforcing the condition $(p-1, q-1) \leq 2$, which was met in Lemma 1.4 and will be encountered again in Section 4. In fact, if $J \subseteq H_n$ is the image of the subgroup generated by $(-1,1)$ and $(1,-1)$ in $G_n = G_p \times G_q$, we have $H_n/J \simeq H_p \times H_q$, and hence the cyclicity of H_n implies that $|H|_p$ is relatively prime to $|H|_q$. The converse also holds, but will be left as an exercise..

For a small group A, then, consider a subgroup $K =< y >$ of order q, and the epimorphism $\varepsilon : A \to C = A/K$. The map (also denoted ε) thereby induced on the group ring $\mathbb{Z}A$ has a natural complement, that is, a ring homomorphism $\varepsilon' : \mathbb{Z}A \to R_\varepsilon$ such that

$$\begin{tikzcd} \mathbb{Z}A \arrow[r, "\varepsilon'"] \arrow[d, "\varepsilon"'] & R_\varepsilon \arrow[d] \\ \mathbb{Z}C \arrow[r] & \mathbb{F}_q C \end{tikzcd} \tag{2.1}$$

is a pull-back, a generalization of the one shown as (1.9). If $A =< x >$ is cyclic of order p^2, take $R_\varepsilon = \mathbb{Z}[\xi]$ where ξ is a primitive p^2-th root of 1 and $\varepsilon'(x) = \xi$. If $A =< x, y >$ with $x^p = y^q = 1$, take $R_\varepsilon = \mathbb{Z}[\eta]C$ where η is a primitive q-th root of 1 and $\varepsilon'(y) = \eta$ while $\varepsilon'(x) = \varepsilon(x)$. Given ε, the complementary ε' is essentially unique: it may be thought of as mapping $\mathbb{Z}A$ into the product of all those Wedderburn components which are not reached by ε.

On the level of units, the pull-back guarantees that ε produces an *isomorphism*

$$\ker\big(\mathcal{U}_1(A) \to \mathcal{U}R_\varepsilon\big) \quad \xrightarrow{\varepsilon} \quad \ker\big(\mathcal{U}_1(C) \to \mathcal{U}_1\mathbb{F}_q C\big)\,, \tag{2.2}$$

which obviously preserves symmetry. Its inverse $\tilde{\varepsilon}$ clearly preserves circularity. For any $v \in \mathcal{U}_1(C)$ congruent 1 modulo q, we have

$$\tilde{\varepsilon}(v) = 1 + \frac{\tilde{v} - 1}{q} \left(1 + y + \cdots + y^{q-1}\right), \tag{2.3}$$

where $\tilde{v} \in \mathbb{Z}A$ is any pre-image of v (not necessarily a unit). Note that the coefficients of $\tilde{v}\,(1 + y + \cdots + y^{q-1})$ are the same as those of v made constant on cosets modulo K. In particular, $v \in \mathcal{U}_1^+(C)$ implies $\tilde{\varepsilon}(v) \in \mathcal{U}_1^+(A)$, so that $\tilde{\varepsilon}$ preserves symmetry as well. It therefore gives an isomorphism

$$\ker\big(\mathcal{W}(C) \to \mathcal{U}_1 \mathbb{F}_q C\big) \quad \xrightarrow{\tilde{\varepsilon}} \quad \ker\big(\mathcal{U}_1^{\oplus}(A) \to \mathcal{U}R_{\varepsilon}\big), \tag{2.4}$$

which will be abbreviated as $\ker_q \mathcal{W}(C) \xrightarrow{\tilde{\varepsilon}} \mathcal{X}_K(A)$. Its image will be called the group of units *co-induced* along ε.

Our next move is to shift from torsion-free $\mathbb{Z}$-modules to finite ones. Since the endomorphism of $\mathbb{Z}C$ defined by $\tau_q : v(z) \mapsto v(z^q)$ has the same effect modulo q as taking the q-th power, $\ker_q \mathcal{W}(C)$ always contains the group

$$\mathcal{W}(C)^{q-\tau_q} = \{w(z)^q w(z^q)^{-1} \mid w(z) \in \mathcal{W}(C)\}. \tag{2.5}$$

On the other hand, every element of $\mathcal{W}(C)$ has finite order modulo this group: after finitely many applications of τ_q it either comes back to itself (if $q \neq p$) or becomes trivial (if $q = p$) — and each of these applications amounts to taking a q-th power. We shall give an explicit formula to see that $\tilde{\varepsilon}$ maps this group into $\mathcal{Y}(A)$.

Proposition 2.1: *For $A \xrightarrow{\varepsilon} C$ as above, suppose that A is cyclic. Then, for every $w \in \mathcal{W}(A)$ and $z = \varepsilon(x) \in C$, we have*

$$\tilde{\varepsilon}\left(w(z^q)^{-1} w(z)^q\right) = w(x^q)^{-1} \cdot \prod_{i=0}^{q-1} w(xy^i)\,. \tag{2.6}$$

Proof: Applying ε to the right hand side yields $w(z^q)^{-1}w(z)^q$ as it should. What happens under ε', depends on a very basic fact: if X is an indeterminate and $\eta \neq 1$ a q-th root of unity, the product over $i = 0, \ldots, q-1$ of the linear polynomials $(1 - \eta^i X)$ equals $(1 - X^q)$. In view of the formulas (1.3) and (1.5) for $w(x, b, c)$, this implies

$$\prod_{i=0}^{q-1} s_b(x\eta^i) = s_b(x^q) \quad \text{and} \quad \prod_{i=0}^{q-1} w(x\eta^i, b, c) = w(x^q, b, c)\,, \tag{2.7}$$

for any x of finite order n and b, c prime to qn. When $A =< x, y >$ with $\varepsilon'(y) = \eta$ and $\varepsilon'(x) = x$, this says exactly that ε' kills the right hand side of (2.6). When $A =< x >$

and $\varepsilon'(x) = \xi$ has order p^2, it still shows the same thing, because ξ may be substituted for x in (2.7). □

Remark: The (xy^i) on the right hand side of the formula (2.6) is a red herring: the product simply extends over all $w(t)$ such that $\varepsilon(t) = z$. For $q = p$, the formula is simplified by the fact that $w(z^q)^{-1} = 1$. Its proof works verbatim for small *elementary abelian* A, but the statement must be modified because $\mathcal{W}(A)$ makes no sense. Instead, $w(z) \in \mathcal{W}(C)$ applies directly to all xy^i. The disappearance of the $w(x^q)^{-1}$ on the right makes the formula even simpler in that case.

For any small abelian A, we now have the desired conversion of $\tilde{\varepsilon}$ to a map between finite groups:

$$\ker_q \mathcal{W}(C)/\mathcal{W}(C)^{q-\tau_q} \quad \xrightarrow{\tilde{\varepsilon}} \quad \mathcal{U}_1^{\oplus}(A)/\mathcal{Y}(A)\,. \tag{2.8}$$

Our next theorem says that these maps, as K varies over all proper subgroups of A, are collectively surjective in the sense that their images generate $\mathcal{U}_1^{\oplus}(A)/\mathcal{Y}(A)$. It is an amalgam of results which originally appeared in [H3] and [H5].

Theorem 2.2: *If A is a small abelian group, $\mathcal{U}_1^{\oplus}(A)$ is generated by constructible and co-induced units, i.e., by $\mathcal{Y}(A)$ and $\mathcal{X}_K(A)$ for all proper subgroups $K \subseteq A$.*

We distinguish three cases. For A cyclic of order p^2, this is another application of Lemma 1.3, according to which $\mathcal{W}(A)$ and $\mathcal{U}_1^{\oplus}(A)$ have the same ε'-image in $\mathcal{U}(\xi)$. A given $u \in \mathcal{U}_1^{\oplus}(A)$ can thus be modified by a $w \in \mathcal{W}(A)$ to make uw^{-1} lie in the kernel of ε' hence in the image of $\tilde{\varepsilon}$. We therefore have $\mathcal{U}_*^{\oplus}(A) = \mathcal{W}(A)\mathcal{X}_K(A)$. Of course, there is only one K in this case, namely A^p.

For A cyclic of order pq with $p \neq q$, the role of K could be played by either A^p or A^q. By tensoring the pull-back (1.9) with $\mathbb{Z}[\eta]$, the ring $\mathcal{R}_\varepsilon = \mathbb{Z}[\eta]C$ appearing as the target of ε' is seen to be the fibre-product of $\mathbb{Z}[\eta]$ with $\mathbb{Z}[\eta,\zeta]$ over $\mathbb{F}_p[\eta]$. Combined with the pull-back (2.1), this yields the double fibre-product

$$\begin{tikzcd} \mathcal{U}_*^{\oplus}(A) \arrow[r] \arrow[d] & \mathcal{U}^{\oplus}(\eta,\zeta) \arrow[d] \\ \mathcal{W}(\eta)\times\mathcal{W}(\zeta) \arrow[r] & \mathcal{U}^{+}\mathbb{F}_p[\eta]\times\mathcal{U}^{+}\mathbb{F}_q[\zeta]\,, \end{tikzcd} \qquad (2.9)$$

whose last line is isomorphic to $\mathcal{W}(A^p)\times\mathcal{W}(A^q) \longrightarrow \mathcal{U}_1^{+}\mathbb{F}_pA^p \times \mathcal{U}_1^{+}\mathbb{F}_qA^q$ since A^p and A^q are of prime order. Proceeding as above, we now get $\mathcal{U}_*^{\oplus}(A) = \mathcal{Y}(A)\mathcal{X}_{A^p}\mathcal{X}_{A^q}$ via Lemma 1.4 — remembering that its hypothesis is satified on account of "smallness". For details the reader is referred to [H4, p. 118] or [H6, p.192]. The group $\mathcal{X}_{A^p}$ coincides precisely with what was denoted by $\Omega(A|p)$ in [H4], and the present theorem is equivalent to the surjectivity of the map Ξ shown *ibidem*. These identifications are quite straightforward.

For elementary abelian A, the proof of the theorem runs differently. It uses the composite

$$\prod_{i=0}^{p}\mathcal{W}(K_i) \xrightarrow{\alpha} \mathcal{U}_1^{\oplus}(A) \xrightarrow{\beta} \prod_{j=0}^{p}\mathcal{W}(C_j)\,, \tag{2.10}$$

where K_i and C_j run over all proper subgroups and factor-groups, respectively, finds via determinants that its cokernel is a finite p-group — cf. [HSW] — and then compares (2.10) with its counterpart over the p-adic integers $\mathbb{Z}_p$. Using logarithms, it can be shown that the p-adic counterpart of α is always an isomorphism, and this suffices to prove $\mathcal{U}_1^{\oplus}(A) = \mathcal{Y}(A)$ for *regular* p — cf. [HS]. For the more interesting irregular case, this has to be combined with an idea to be explained presently. We shall be able to finish this outline at the end of the next section.

Remark: Although it does not directly affect the arguments of the next two sections, it is worth noting that the maps (2.8) are individually injective — for it shows that the co-induced units so obtained are not constructible, they are "exotic". For A cyclic of order p^2, this is again fairly easy to see. One has to write $\mathcal{Y}(A) = \mathcal{W}(A)\mathcal{W}(A)^{\tau_p - s}$, where s is the trace over the p-subgroup of H_{p^2}, and check that the second factor goes to $\mathcal{W}(C)^p$ under ε. For $|A| = pq \neq p^2$, the story is more subtle, and again depends on the condition $(p-1, q-1) \leq 2$ — cf. [H4, Proposition 4.2 and Scholium 4.3]. The elementary abelian case is dealt with in [H3, Section 4].

3. Kummer units.

We now specialize the scenario of the preceding section to the cases where $q = p$, and note that everything is compatible with the action of $G = (\mathbb{Z}/p\mathbb{Z})^\times$, which is part of the automorphism group of C, A, K and all derived structures. On any $\mathbb{F}_p$-space $\mathcal{S}$, this action is semi-simple and yields a direct decomposition into characteristic subspaces $\mathcal{S}_d$ (the corresponding characters χ^d being powers of the natural identification $\chi : G \to \mathbb{F}_p^\times$), and every G-map $f : \mathcal{S} \to \mathcal{S}'$ of such spaces decomposes into "slices" $f_d : \mathcal{S}_d \to \mathcal{S}'_d$. The trivial character is χ^{p-1}.

If G acts via $H = G/\{\pm 1\}$, only *even* characters are involved, that is, $d = 2k$ with $1 \leq k \leq h$, where $h = (p-1)/2$. This is clearly the case for the coefficient reduction map

$$\lambda : \mathcal{W}(C)/\mathcal{W}(C)^p \longrightarrow \acute{\mathcal{U}}_1^+ \mathbb{F}_p\, C\,, \tag{3.1}$$

derived from the bottom horizontal arrow in the pull-back diagram (2.1). Its kernel is the source $\ker_p \mathcal{W}(C)/\mathcal{W}(C)^p$ of the important map (2.8) which targets non-constructible co-induced units. The acute accent on the right hand side of (3.1) means restriction to units of H-norm 1, allowed by the obvious analogous property for elements of $\mathcal{W}(C)$. We shall see that the two sides of (3.1) are isomorphic *a priori*, although λ itself is *not* always an isomorphism.

Indeed, $\mathcal{W}(C)/\mathcal{W}(C)^p$ being isomorphic to the square of the augmentation ideal in $\mathbb{F}_p H$, it is not hard to see that it involves each non-trivial character of H, i.e., every non-trivial even character of G, exactly once. In other words, there are $h-1 = (p-3)/2$ slices λ_{2k} with $k = 1, \ldots, h-1$, each mapping a 1-dimensional $\mathbb{F}_p$-space into $\mathcal{U}_1^+ \mathbb{F}_p\, C$.

On the other hand, the natural logarithm defines an isomorphism of the multiplicative group $\mathcal{U}_1 \mathbb{F}_p\, C = 1 + (z-1)\mathbb{F}_p\, C$ with the additive group $(z-1)\mathbb{F}_p\, C$. Since $(z^a - 1)^d \equiv a^d (z-1)^d$ modulo $(z-1)^{d+1}\mathbb{F}_p\, C$, the power filtration of the ideal $(z-1)\mathbb{F}_p\, C$

is a Jordan-Hölder series in which each character χ^d occurs exactly once. It follows that $\acute{\mathcal{U}}_1^+ \mathbb{F}_p C$ involves exactly the same χ^d as $\mathcal{W}(C)/\mathcal{W}(C)^p$. *Hence each λ_d is either zero or bijective.*

Lemma 3.1: *λ_d is zero if and only if p divides the Bernoulli number $B_d \in \mathbb{Z}_p$.*

This result is implicit in Kummer's 1847 paper [Ku] — for a modern rendition, cf. [BS, V. 5] or [H6, Section 7]. It will not be needed for the present argument, but it explains how the triviality or injectivity of λ_d can be decided. Moreover, it partially accounts for our wavering between G and H: although it is applied to the latter (i.e., symmetric units), its genesis is in the world of the former, and hence so is its statement (involving $d = 2k$ instead of k itself). In fact, the injectivity of λ is equivalent to p being prime to h_p^-, and this often fails even with $h_p^+ = 1$.

Definition. We shall say that the prime p is *irregular at d* if λ_d is zero. An element of $\ker_p \mathcal{W}(C)$ not in $\mathcal{W}(C)^p$ will be called a *Kummer unit at d.*

The first seven primes concerned are p =37, 59, 67, 101, 103, 131, 149; they are irregular at d =32, 44, 58, 68, 24, 22, 130, respectively. The eighth irregular prime $p = 157$ has two bad degrees, namely $d_1 = 62$ and $d_2 = 110$. The first prime which is irregular at three degrees is $p = 491$, with $d_1 = 292$, $d_2 = 336$, $d_3 = 338$. These values come from [Wa, p. 410].

Proposition 3.2: *Suppose that p is irregular at $d = 2k$ and that $\{w(z^a) \mid a \in \mathbb{Z}\}$ spans $\mathcal{W}(C)$. Then, for $\theta = \sum_a n_a \cdot \tau_a \in \mathbb{Z}H$ with $a = 1, \ldots, h$, the unit*

$$w(z)^\theta = \prod_{a=1}^{h} w(z^a)^{n_a} \tag{3.2}$$

is a Kummer unit at d whenever $n_a a^d$ yields a constant $t \not\equiv 0$ in $\mathbb{F}_p$.

Proof. The minimal idempotent $e_d =$

$$-\sum_{\sigma \in G} \chi^d(\sigma^{-1}) \cdot \sigma = -\sum_{a=1}^{p-1} a^{-d} \cdot \tau_a \tag{3.3}$$

in $\mathbb{F}_p G$ projects any $\mathbb{F}_p G$-module $\mathcal{S}$ onto its d-th slice $\mathcal{S}_d = e_d \mathcal{S}$. The same is true for any $\mathbb{F}_p^\times$-multiple of e_d such as $\bar{\theta} =$

$$\sum_{a=1}^{h} \bar{n}_a \cdot \tau_a = -\frac{t}{2}\, e_d\,, \tag{3.4}$$

where "bar" indicates coefficient reduction modulo p. It follows that the class of $w(z)^\theta$ generates the d-th slice of $\mathcal{W}(C)/\mathcal{W}(C)^p$. □

Proposition 3.3: *Suppose that p is irregular at exactly $d_1, \ldots, d_r$ and that A is cyclic of order p^2. Then, if $\{v_1, \ldots, v_{h-1}\}$ is a basis of $\mathcal{W}(A^p)$ such that v_i is a Kummer unit* *at d_i for $i \le r$, a basis of $\mathcal{U}_1^{\oplus}(A)$ is obtained by extending a basis of $\mathcal{W}(A)$ by the sets $\{\tilde{\varepsilon}(v_1), \ldots, \tilde{\varepsilon}(v_r)\}$ and $\{v_{r+1}, \ldots, v_{h-1}\}$.*

Proof. Since the set in question has the correct number of elements, we need only show that it generates $\mathcal{U}_1^{\oplus}(A)$. Since Theorem 2.2 says that $\mathcal{U}_1^{\oplus}(A)/\mathcal{Y}(A)$ is spanned by $\{\tilde{\varepsilon}(v_1), \ldots, \tilde{\varepsilon}(v_r)\}$, it suffices to prove that all of $\mathcal{Y}(A)$, or more precisely every v_i for $i \le r$, can be expressed in terms of this set. For a unit $\tilde{\varepsilon}\big(w(z)^\theta\big)$ co-induced from $w(z)^\theta$ as shown in (3.2), the formula (2.6) translates to

$$\tilde{\varepsilon}\big(w(z)^\theta\big)^p = \tilde{\varepsilon}\big(w(z)^p\big)^\theta \equiv w(y)^{-\theta} \pmod{\mathcal{W}(A)} \tag{3.5}$$

where $y = x^p$ with $< x >= A$ as usual. The right hand side is just the inverse of the Kummer unit $v = w(y)^\theta$ — here visibly expressed in termd of $\mathcal{W}(A)$ and $\tilde{\varepsilon}(v)$. □

Corollary 3.4: *In Proposition 3.3, suppose that $r = 1$, and that $n_b = n_c + 1$ for two specific coefficients of θ in $v_1 = w^\theta$. Then a basis of $\mathcal{U}_1^{\oplus}(A)$ is given by extending a basis of $\mathcal{W}(A)$ by the set $\{w(y^a) \mid 1 \le a \le h,\, a \ne b, c\}$ and the co-induced Kummer unit $\tilde{\varepsilon}\big(w(z)^\theta\big)$.*

Proof. Multiplying the relation (3.2) by $1 = \prod_a w(y^a)^{-n_c}$, we get the expression

$$w(z)^\theta = \prod_{a=1}^{h} w(z^a)^{n_a - n_c}\,, \tag{3.6}$$

which lacks the factor $w(z^c)$ and is linear in $w(z^b)$. This shows that $w(y)^\theta$ together with $\{w(y^a) \mid 1 \le a \le h,\, a \ne b, c\}$ generates $\mathcal{W}(K)$, as required by Proposition 3.3. □

Remark: By a suitable choice of θ, the hypothesis $n_b = n_c + 1$ can be satisfied for any pair b, c with $b^d \not\equiv c^d$ modulo p. One need only adjust the constant $t \in \mathbb{F}_p$ named in Proposition 3.2, and choose n_b, n_c between 1 and $p-1$, so that $n_b - n_c \equiv 1$ modulo p implies $n_b - n_c = 1$. This yields bases for $\mathcal{U}_*^{\oplus}(A)$ in all cases where A is cyclic of order p^2 and p is irregular at only one d, i.e. where $\mathcal{W}(C)/\mathcal{W}(C)^p$ is cyclic.

Examples.

1. Let us work this out for $p = 37$, which is irregular at $d = 32$ only. Since G is generated by τ_2 as well as by τ_5, the prescriptions of Section 1 make $w(z) = z^{-2} - z^{-1} + 1 - z + z^2$ an appropriate $\mathbb{Z}G$-generator of $\mathcal{W}(C)$. The crucial character $\chi^d : \tau_a \mapsto a^{32} = a^{-4}$ (with values in $\mathbb{F}_p^\times$) has the kernel $G_4 = \{\pm 6, \pm 1\}$. Picking the coefficients n_a of θ to be constant on cosets of G_4, we can index them by the set $I = \{1, 2, 3, 4, 5, 8, 9, 10, 15\}$ of representatives. Invariance under G_4 then forces our co-induced Kummer unit $\tilde{\varepsilon}(w^\theta)$ to look like

$$1 + (1 + y + \cdots + y^{p-1}) \sum_{i \in I} c_i\, (x^i + x^{-i} + x^{6i} + x^{-6i} - 4)\,. \tag{3.7}$$

It is computed by first evaluating $v = w(z)^\theta$ and then using the formula (2.3). Choosing n_a to be the positive residue defined by $(p-2)\,a^4 = q_a p + n_a$, we obtain the following coefficients c_i:

$$\begin{aligned} c_1 &= +1826391438413288649 & c_2 &= -1021466795253062642 \\ c_3 &= +162246643879408744 & c_4 &= +706070271863032512 \\ c_5 &= -1501545774926023726 & c_8 &= +878425477417643782 \\ c_9 &= -280909292629400144 & c_{10} &= -328201689410415248 \\ c_{15} &= +1060029695130133555 \end{aligned}$$

Since $\sigma e_d = \chi^d(\sigma)e_d$ for any $\sigma \in H$, the substitution $te_d \mapsto \chi^d(\sigma)te_d$ only permutes these coefficients. Hence there are only 4 essentially different outcomes depending to the class of t in $\mathbb{F}_p^\times$ modulo 4-th powers. The one displayed above (for $t = -2$) corresponds to e_d itself and happens to have the smallest coefficients.

Since $n_2 = 5$ and $n_4 = 6$ differ by 1, Corollary 3.4 says that a basis of $\mathcal{U}_*^\oplus(A)$ is formed by $\tilde{\varepsilon}(w^\theta)$ as shown in (3.7), together with $\{w(y^a) \mid 1 \le a \le 18,\ a \ne 5, 6\}$ and a basis of $\mathcal{W}(A)$, for instance: $\{w(x^{b+pc}) \mid 1 \le b \le 18,\ 0 \le c \le 36,\ b + pc \ne 1\}$. So much for $p = 37$.

2. For $r = 2$, say p irregular at d and d', the criterion generalizing Corollary 3.4 would be that one could adjust $\theta = \sum_a n_a \cdot \tau_a$ and $\theta' = \sum_a n'_a \cdot \tau_a$ in such a way that

$$\det \begin{bmatrix} 1 & 1 & 1 \\ n_b & n_c & n_g \\ n'_b & n'_c & n'_g \end{bmatrix} = \pm 1 \tag{3.8}$$

with suitable values $a = b, c, g$ between 1 and $h = (p - 1)/2$. A basis of $\mathcal{U}_*^\oplus(A)$ would then be given by extending a basis of $\mathcal{W}(A)$ by the set $\{w(y^a) \mid 1 \le a \le h,\ a \ne b, c, g\}$ and the co-induced Kummer units $\tilde{\varepsilon}(v)$ and $\tilde{\varepsilon}(v')$, where v and v' are obtained from θ and θ', respectively, à la (3.2).

It is not clear that this can always be done, but it seems plausible because of all the available choices. In the case $p = 157$, for instance, we have $d = 110$ and $d' = 62$. Choosing n_a and n'_a to be the smallest positive residues such that $ta^{46} = q_a p + n_a$ and $t'a^{94} = q'_a p + n'_a$, respectively, one solution of (3.8) is to put $t = 1$, $t' = 3$ and $b = 1$, $c = 16$, $g = 76$. This yields the determinant

$$\det \begin{bmatrix} 1 & 1 & 1 \\ 1 & 153 & 40 \\ 3 & 42 & 13 \end{bmatrix} = -1$$

and a basis of $\mathcal{U}_*^\oplus(A)$ built on the set $\{w(y^a) \mid 1 \le a \le h,\ a \ne 1, 16, 76\} \subseteq \mathcal{W}(K)$ as above and including two co-induced units. The coefficients of these would, however, be horrendously big.

This section has dealt with cyclic A of order p^2, but it can also shed some light on the elementary abelian case. To finish the discussion of Theorem 2.2, imagine the maps α and β of (2.10) taken modulo p-th powers (i.e., operating on $\mathcal{W}(C)/\mathcal{W}(C)^p$, etc.) and then restricted to d-th components. If p is regular at d, the old p-adic argument shows that $\bar{\alpha}_d$ is surjective ("bar" meaning modulo p-th powers). On the other hand, if p is irregular at d, it is easy to see that the images of co-induced Kummer units cover the entire target of $\bar{\beta}_d$. Since $\mathcal{U}_1^{\oplus}(A)/\mathcal{Y}(A)$ is known to be a finite p-group — cf. [HSW] — the theorem now follows via Nakayama's Lemma.

More precisely, the corollary of Proposition 2 in [H1] says that $\mathcal{U}_1^{\oplus}(A)/\mathcal{Y}(A)$ is an $\mathbb{F}_p$-space, which has dimension $p-d$ when p is irregular at only one d. For $p=37$, this means that it is generated by 5 of the 38 elements obtained from (3.7) by letting $< y >$ run through all proper subgroups of A. However, it is not clear how to construct a basis of $\mathcal{U}_1^{\oplus}(A)$ — which in this case equals $\mathcal{U}_1^{+}(A)$ — from this information.

4. Composite cases.

When $q \neq p$, the group $G_p = (\mathbb{Z}/p\mathbb{Z})^{\times}$ no longer acts on K, and its action on $\mathcal{U}_1 \mathbb{F}_q\, C$ is no longer a representation over $\mathbb{F}_q$ — let alone a semi-simple one. Nevertheless, we still have the coefficient reduction map

$$\lambda_q : \mathcal{W}(C)/\mathcal{W}(C)^{q-\tau_q} \longrightarrow \acute{\mathcal{U}}_1^{+} \mathbb{F}_q\, C\,, \tag{4.1}$$

whose kernel is the source of the arrow (2.8) aimed at non-constructible co-induced units. The acute accent on the right hand side again means restriction to units of H_p-norm 1, where $H_p = G_p/\{\pm 1\}$ as usual. We shall see that the two sides of (4.1) are isomorphic *a priori*, although λ_q itself is *not* always an isomorphism. This time, however, there will be no lifted idempotents to lead us to its kernel.

Proposition 4.1: *$\mathcal{W}(C)/\mathcal{W}(C)^{q-\tau_q}$ and $\acute{\mathcal{U}}_1^{+} \mathbb{F}_q\, C$ are isomorphic finite H_p-modules.*

Proof. The Chinese Remainder Theorem yields a decomposition $\mathbb{F}_q\, C \simeq \mathbb{F}_q \oplus \mathbb{F}_q[\zeta_p]$ whose second summand is a separable $\mathbb{F}_q$-algebra of dimension $p-1$, on which G_p acts as a group of automorphisms. Since its elements are characterized by having a 1 in the first summand, $\mathcal{U}_1 \mathbb{F}_q\, C$ can be identified with the multiplicative group of $\mathbb{F}_q[\zeta_p]$. In this way, $\mathcal{U}_1^{+} \mathbb{F}_q\, C$ becomes identified with the multiplicative group of the separable $\mathbb{F}_q$-algebra $\mathbb{F}_q[\zeta_p + \zeta_p^{-1}]$, which has dimension $h_p = (p-1)/2$ and is acted upon by H_p. Its simple components are extension fields $E_1, \ldots, E_g$ of $\mathbb{F}_q$, which are permuted cyclically by the action of H_p. Each multiplicative group $E_k^{\times}$ is cyclic of order $q^f - 1$, where f is the order of τ_q in H_p, and the Frobenius automorphism τ_q acts on it as the q-th power.

Any generator u of one of the cyclic groups $E_k^{\times}$ therefore becomes a $\mathbb{Z}H_p$-generator of $\mathcal{U}\, \mathbb{F}_q[\zeta_p + \zeta_p^{-1}]$ alias $\mathcal{U}_1^{+} \mathbb{F}_q\, C$. In other words, it induces a surjection

$$\mathbb{Z}H_p/(q-\tau_q)\mathbb{Z}H_p \xrightarrow{u} \mathcal{U}_1^{+} \mathbb{F}_q\, C\,, \tag{4.2}$$

which is easily seen to be an isomorphism by counting elements on both sides — using the decomposition into cosets modulo $< \tau_q >$ on the left. Via its identification with $\mathcal{U}\, \mathbb{F}_q[\zeta_p + \zeta_p^{-1}]$, this H_p-module is well known to be cohomologically trivial (cf. Hilbert's Theorem 90 and the triviality of the Brauer Group). Hence, if σ generates H_p, the element $v = u^{\sigma - 1}$ induces a surjection

$$\mathbb{Z}H_p/(q-\tau_q)\mathbb{Z}H_p \xrightarrow{v} \acute{\mathcal{U}}_1^{+} \mathbb{F}_q\, C\,, \tag{4.3}$$

whose kernel consists exactly of the H_p-norms of the module on the left. Since $\mathcal{W}(C)$ is isomorphic to $\mathbb{Z}H_p$ modulo such norms, this becomes an isomorphism between $\mathcal{W}(C)/\mathcal{W}(C)^{q-\tau_q}$ and $\acute{\mathcal{U}}_1^+\mathbb{F}_q\,C$ as advertised. $\square$

Definition: If $(q-1, p-1) \leq 2$, we shall say that p is *defective* modulo q if λ_q fails to be injective (and hence an isomorphism). The order $\left[\,\ker_q \mathcal{W}(C) : \mathcal{W}(C)^{q-\tau_q}\right]$ of the kernel will be denoted $d_q(p)$ and referred to as the *defect* of p modulo q.

Remark: In Proposition 4.1, no reference was needed to the peculiar requirement that H_n be cyclic or $(q-1, p-1)$ be ≤ 2. For p and q both odd, it turns out that the kernel of λ_q always contains a cyclic group of order (h_p, h_q) — cf. [H4, Proposition 4.2 and Scholium 4.3]. In general, λ_q would therefore not be considered abnormal unless its kernel were bigger than that — which would lead to a correspondingly more complex definition of the defect.

There are fifty-two numbers of the form $n = pq < 200$, and all have $h_n^+ = 1$ except $n = 145$ and $n = 183$. Forty of the remaining fifty give $\mathcal{Y}(A) = \mathcal{U}_*(A)$ for cyclic A of order n. Of the ten exceptions, five — namely 65, 85, 91, 133, 185 — fail to be small in our sense; the index $\left[\mathcal{U}_*(A) : \mathcal{Y}(A)\right]$ happens to equal (h_p, h_q) for all of them. The five "small" exceptions owe their imperfection to p being defective modulo q. We list them in the form $q \times p\,\big(d_q(p)\big)$: $2 \times 37\,(3)$, $2 \times 73\,(7)$, $2 \times 97\,(7)$, $11 \times 13\,(3)$, $11 \times 17\,(3)$.

Generally it is harder to find out (without assists from Kummer and Bernoulli) whether a prime p is defective modulo q than whether it is irregular. Moreover, the actual computation of the defect can be quite subtle — cf. [H5]. The values listed above are taken from [Fe, p. 67].

Henceforth, we shall put $A =< y, z >$ with $y^q = z^p = 1$, and take $C =< z >$. Let $v = w(z)$ be an H_p-generator of $\mathcal{W}(C)$. Given $v^\gamma \in \ker_q \mathcal{W}(C)$, we are interested in relating the co-induced unit $\tilde{\varepsilon}(v^\gamma)$ back to $\mathcal{Y}(A)$. If d is the order of v^γ modulo $\mathcal{W}(C)^{q-\tau_q}$, we have $(v^\gamma)^d = (v^\theta)^{q-\tau_q}$ for some $\theta \in \mathbb{Z}H_p$. In other words,

$$\gamma d = \mu \sum_{a=1}^{h} \tau_a \;+\; (q-\tau_q) \sum_{a=1}^{h} n_a\, \tau_a \tag{4.4}$$

for some sequence $n_1, \ldots, n_h$ of integers, where $h = h_p$. These integers (the coefficients of θ) are not unique: they can be changed by adding any constant integer k — and simultaneously subtracting $(q-1)k$ from μ. Formula (2.6) now yields

$$\tilde{\varepsilon}(v^\gamma)^d = \prod_{a=1}^{h} \tilde{\varepsilon}\big(w(z^a)^{n_a(q-\tau_q)}\big) = w(z)^{(1-\tau_q)\theta} \cdot \prod_{i=1}^{q-1} \prod_{a=1}^{h} w(z^a y^i)^{n_a}\,, \tag{4.5}$$

where $w(yz)$ is an H_n-generator of $\mathcal{W}(A)$ which specializes to $w(z)$ under $\varepsilon : A \to C$, i.e., setting $\varepsilon(y) = 1$. To see that (4.5) is legitimate, fix $w(z^a) \in \mathcal{W}(C)$ and apply (2.6) to get

$$\tilde{\varepsilon}\big(w(z^a)^{q-\tau_q}\big) = w(z^a)^{-\tau_q} \prod_{i=0}^{q-1} w(z^a y^i)\,, \tag{4.6}$$

where the product over $i = 0, \ldots, (q-1)$ is just the multiplication of all $w(t)$ with $t \in A$ such that $\varepsilon(t) = z^a$. Then throw the term for $i = 0$ in with the factor $w(z^a)^{-\tau_q}$, and finally take the product over $a = 1, \ldots, h$ with the weights n_a. We can now prove a result similar to Corollary 3.4 above.

Proposition 4.2: *Let* $\ker_q \mathcal{W}(C)/\mathcal{W}(C)^{q-\tau_q}$ *be cyclic of order* d *with generator* $w(z)^\gamma \in \mathcal{W}(C)$*. Suppose that* $n_b = n_c + 1$ *for two specific coefficients in* (4.4)*. Then a basis of* $\mathcal{X}_K(A)\mathcal{Y}(A)$ *is given by adjoining to bases of* $\mathcal{W}(A^q)$ *and* $\mathcal{W}(A^p)$ *the co-induced unit* $\tilde{\varepsilon}\big(w(z)^\gamma\big)$ *as well as the* H_n*-orbit of* $w(zy)$ *diminished by* $\{w(z^b y), w(z^c y)\}$*.*

Proof. The set $\{w(z^a y^i) \mid 1 \le a \le h,\ 1 \le i \le q-1\}$ is the full H_n-orbit of $w(zy)$. The product of its elements equals 1, and a basis of $\mathcal{W}(A)$ is obtained by omitting any one of them. According to (4.5), we can write

$$\tilde{\varepsilon}(v^\gamma)^d \equiv \prod_{i=2}^{q-1} \prod_{a=1}^{h} w(z^a y^i)^{n_a - n_c} \pmod{\mathcal{W}(A^q)}\,. \tag{4.7}$$

The $q-1$ terms with $a = c$ are missing, and those with $a = b$ appear to the first power. Any one of the latter can therefore be omitted and replaced by $\tilde{\varepsilon}(v^\gamma)$. □

The one condition which makes the computation of defects go smoothly is that $\mathbb{F}_q[\zeta_p + \zeta_p^{-1}]$ be a field, i.e., that τ_q generate H_p. Then both sides of (4.1) are cyclic of order $1 + q + \cdots + q^{f-1}$ with $f = h_p$, and one only needs to compare that with the order of $\lambda_q(w)$ for a $\mathbb{Z}H_p$-generator w of $\mathcal{W}(C)$. Furthermore, it is surprisingly easy to find a $\gamma \in \mathbb{Z}H_p$ such that $v = w^\alpha$ generates the cyclic group $\ker_q \mathcal{W}(C)/\mathcal{W}(C)^{q-\tau_q}$ and to incorporate the co-induced unit $\tilde{\varepsilon}(w^\gamma)$ into a basis of $\mathcal{X}_K(A)\mathcal{Y}(A)$.

Proposition 4.3: *Let* $w(zy)$ *be a* $\mathbb{Z}H_n$*-generator of* $\mathcal{W}(A)$ *and assume* $H_p =< \tau_q >$*. If* c *is the order of* $\lambda_q\big(w(z)\big)$ *in* $\acute{\mathcal{U}}_1^+\mathbb{F}_q C$*, a basis of* $\mathcal{X}_K(A)\mathcal{Y}(A)$ *is formed by adjoining to bases of* $\mathcal{W}(A^p)$ *and* $\mathcal{W}(A^q)$ *the* H_n*-orbit of* $w(zy)$ *augmented by* $\tilde{\varepsilon}\big(w(z)^c\big)$ *and diminished by* $\{w(z^a y), w(z^b y) \mid a = q^{f-1},\ b = q^{f-2}\}$*.*

Proof. If the defect is d, we have $cd = 1 + q + \cdots + q^{f-1}$ and

$$cd - (1 + \tau_q + \cdots + \tau_q^{f-1}) = (q - \tau_q) + \cdots + (q^{f-1} - \tau_q^{f-1}) = (q - \tau_q)\,\theta\,, \tag{4.8}$$

where $\theta = \sum_i m_i \tau_q^i$ has the form of a monic polynomial of degree $f-2$ in τ_q, in other words: $m_{f-1} = 0$ and $m_{f-2} = 1$. Now apply the previous proposition. □

Corollary 4.4: *In Propsition 4.3, let* $c_0 + c_1 q + \cdots + c_s q^s$ *be the* q*-adic representation of* c*, and consider* $\gamma = c_0 + c_1\tau_q + \cdots + c_s\tau_q^s \in \mathbb{Z}H_p$*. Then the conclusion is valid with* $\tilde{\varepsilon}\big(w(z)^c\big)$ *replaced by* $\tilde{\varepsilon}\big(w(z)^\gamma\big)$*.*

Proof. Since $d > 1$ implies $s < f-1$, this replacement modifies the preceding calculation by a ”polynomial” summand of lower degree, namely $c_1(t_q - q) + \cdots + c_s(t_q^s - q^s)$. □

Examples. Of the five “small” exceptional $n < 200$ mentioned after the definition of defect, three have τ_q generating H_p. The first of these, $n = 74$, was already displayed at the end of Section 1. Let us now look at the other two. In every case, the two defects $d_p(q)$ and $d_q(p)$ were computed previously. It so happens that in these examples only one of them — which we call $d_q(p)$ — is non-trivial. Hence $\mathcal{U}_*^{\oplus}(A) = \mathcal{X}_k(A)\mathcal{Y}(A)$, and bases are obtained by a straightforward application of Proposition 4.3 in the guise of Corollary 4.4.

For $n = 11 \times 13$, we can take $w(yz, 2, 7)$ as the generating unit for $\mathcal{W}(A)$. With $q = 11$ and $\tau = \tau_q$, we have $q^2 - 1 = 4 \times 3 \times 10$, whence $(q^6 - 1)/3(q - 1) = 4(1 + q^2 + q^4)$. Using $\gamma = 4(1 + \tau^2 + \tau^4)$, we get the co-induced unit

$$\tilde{\varepsilon}\big(w(z)^{\gamma}\big) = 1 + S(y)\big(594 - 228\, T_6(z) + 129\, T_6(z^2)\big)\,, \tag{4.9}$$

where $S(y)$ is the sum over the powers of y, and T_k denotes the trace over the subgroup of order k in G_p. The calculations for $n = 11 \times 17$ are amazingly similar — except that an alternating unit will not generate $\mathcal{W}(A)$, so we take $w(yz, 3, 3)$ instead. For the same reason as above, $\gamma = 4\,(1 + \tau^2 + \tau^4 + \tau^6)$ is a suitable operator, but this one yields

$$\tilde{\varepsilon}\big(w(z)^{\gamma}\big) = 1 + S(y)\big(811008 + 158304\, T_8(z) - 259680\, T_8(z^2)\big)\,. \tag{4.10}$$

Both of these have order 3 modulo $\mathcal{Y}(A)$ and can be incorporated into bases of $\mathcal{U}_*(A) = \mathcal{U}_*^{\oplus}(A)$ according to the prescriptions of Proposition 4.3.

For more variety, let us look outside the range $n < 200$, even if that means retreating from $\mathcal{U}_*(A)$ to $\mathcal{U}_*^{\oplus}(A)$. Lest it be thought that q is always the smaller prime, we mention the case $q = 47$, $p = 5$ — which also has $d_q(p) = 3$ — but leave it as an exercise. A more difficult example is $q = 11$, $p = 31$ — which has $d_q(p) = 19$. Using $w(yz, 3, 3)$ and $\gamma = 7\,(1 + \tau^3 + \tau^6 + \tau^9 + \tau^{12})$ one obtains

$$\tilde{\varepsilon}\big(w(z)^{\gamma}\big) = 1 + S(y)\big(k_0 + k_1\, T_{10}(z) - k_3\, T_{10}(z^3) + k_9\, T_{10}(z^9)\big)\,, \tag{4.11}$$

$$\begin{array}{ll} k_0 = -10613099410760939400 & \qquad k_1 = +3499213745161912052 \\ k_3 = -3272944392078799562 & \qquad k_9 = +835040587992981450\,. \end{array}$$

This shows incidentally that co-induced units in p-groups, as seen in Section 3, have no monopoly on large coefficients. Despite its fearsome appearance, this unit fits into a basis of $\mathcal{U}_*^{\oplus}(A)$ for $|A| = 341$ as easily as the previous ones.

References

[Ba] Bass, H., *The Dirichlet unit theorem, induced characters, and Whitehead groups of finite groups.* Topology 4 (1966), 391 - 410

[BS] Borevich, Z.I., Shafarevich, I.R., *Number Theory,* Academic Press, N.Y. (1966)

[CSW] Cliff, G.H., Sehgal, S.K., Weiss, A.R., *Units of integral group rings of metabelian groups.* J. of Alg. 73 (1981), 167 - 185

[Fe] Ferguson, R., *Units in integral cyclic group rings for order $l^r p^s$.* Doctoral thesis, University of British Columbia (1997).

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

[H2] —, *Constructing units in commutative group rings.* Man. Math. 75 (1992), 5 - 23

[H3] —, *Exotic units in group rings of rank p^2.* Arch. d. Math. 58 (1992), 239 - 247

[H4] —, *Units in integral group rings for order pq.* Can. J. Math. 47 (1995), 113 - 131

[H5] —, *Cyclotomic units over finite fields.* Rendiconti Palermo XLIV (1995), 5 - 20

[H6] —, *On the arithmetic of commutative group rings.* in Group Theory, Algebra, Number Theory, Ed.: Zimmer; Walter de Gruyter, Berlin (1996), 145 - 201

[HR] —, Ritter, J, *Constructible units in abelian p-group rings.* J. Pure and Appl. Alg. 68 (1990), 325 - 339

[HS] —, Sehgal, S.K., *Units in regular abelian p-group rings.* J. Numb. Th. 30 (1988), 375 - 381

[HSW] —, —, Weiss, A., *Cyclotomic units and the unit group of an elementary abelian group ring.* Arch. d. Math. 45 (1985), 5 - 7

[Ku] Kummer, E., *Beweis des Fermat'schen Satzes der Unmöglichkeit von $x^\lambda + y^\lambda = z^\lambda$ für eine unendliche Anzahl Primzahlen λ.* Monatsber. Akad. Wiss. Berlin (1847). Collected Papers I. Springer Verlag, N.Y. (1975), 274 - 297

[Se] Sehgal, S.K., *Units in integral group rings.* J.Wiley, N.Y. (1993)

[Wa] Washington, L., *Introduction to Cyclotomic Fields (Second Edition).* Springer Verlag, N.Y. (1996)