On the arithmetic of commutative group rings

Klaus Hoechsmann

Unlike the other chapters in this volume, the present one does not deal with a specific aspect of Hans Zassenhaus's mathematical legacy, but rather with recent work by one of his older students. There seems to be no deeper meaning to its inclusion here than that it actually represents one of the talks given at the memorial colloquium.

One of the off-shoots of Zassenhaus's life-long interest in the arithmetic of orders in $\mathbb{Q}$-algebras was his recurrent work on units in integral group rings $\mathbb{Z}G$ for finite groups G. Initially, his purpose here seems to have been the characterization of finite subgroups of units with a view toward solving the so-called isomorphism problem. In fact, he conjectured that any finite subgroup H of the unit group $\mathcal{U}\,\mathbb{Z}G$ would have to be conjugate, within $\mathcal{U}\,\mathbb{Q}G$, to a subgroup of G itself. Eventually Roggenkamp and Scott were able to prove this for $|H| = |G|$ and G nilpotent — and to show that it failed for certain metabelian G. The full conjecture, without the restriction on the order of H, was later established by Weiss, of course only for nilpotent G.

Meanwhile, new questions had arisen and drawn all of $\mathcal{U}\,\mathbb{Z}G$ into the scope of these investigations, on which Zassenhaus worked mostly in collaboration with his former student Sudarshan Sehgal of Edmonton (Canada). With the help of Al Weiss, a Zassenhaus pupil of the youngest generation, Sehgal had turned his home base into a focal point for this kind of research. As a fellow Zassenhaus student living in nearby Vancouver — a mere 1000 km away — I was bound to get involved in this activity sooner or later. In fact, I became so engrossed with the commutative side of the story, that I never rejoined the main stream.

I am much obliged to the organizers of this colloquium for the opportunity to give a coherent summary of the following results, which I cannot really call mine, since they owe so much to my collaborators Sudarshan Sehgal and Jürgen Ritter. Among the great number of Zassenhaus's mathematical progeny, many a contributor could have been found with a better story to tell. Therefore I am grateful that the chance has fallen on me to write this belated homage to my teacher.

1. Introduction

The easiest way to introduce the subject at hand is by the very simple problem Sehgal proposed in December 1983: find an explicit formula for the units in the group ring $\mathbb{Z}A$ of an abelian group $A = \langle x, y\rangle$ with $x^p = y^p = 1$ — for starters, take $p = 5$.

To put this more precisely, let us recall the splitting

$$\mathcal{U}(A) = \pm A \times \mathcal{U}_1^+(A), \tag{1.1}$$

valid for any finite abelian group A of odd order *. It represents the decomposition of $\mathcal{U}(A)$ into its torsion subgroup $\pm A$ and the torsion-free complement $\mathcal{U}_1^+(A)$, consisting of those units which have coefficient sum ("augmentation") $= 1$ and are left fixed by the standard involution coming from $z \mapsto z^{-1}$ $(z \in A)$. The problem was to find a basis of $\mathcal{U}_1^+(A)$ for A non-cyclic of order 25.

We knew that $\mathcal{U}_1^+(C)$ for the cyclic group $C = \langle z\rangle$ of order 5 was generated by the single unit $w(z) = z - 1 + z^{-1}$ and (via Dirichlet and Wedderburn) that $\mathcal{U}_1^+(A)$ had rank 6 for the A in question. Therefore we 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 of the map

$$\mu : \prod_{C\subseteq A} \mathcal{U}_1^+(C) \longrightarrow \mathcal{U}_1^+(A)\,, \tag{1.2}$$

where C runs over the non-trivial cyclic subgroups of A, and the product is direct. We eventually managed to do this, not only for $|A| = p^2$, but for all elementary abelian A, provided p was a *regular* prime. Indeed, this bijectivity turned out to be characteristic of regular primes: for irregular p, we found a lower bound on the index of μ (i.e., the order of its cokernel) and an identification of that index with the order of a certain group of (projective) ideal classes in $\mathbb{Z}A$.

In fact, the map μ remains surjective for any abelian p-group A, as long as p is regular. But without its injectivity, it is no longer suitable for defining bases, and its index is no longer so easily related to ideal classes. In collaboration with Ritter, we therefore modified our approach in two ways. Firstly, we restricted our attention to the subgroup $\mathcal{U}_1^{\oplus}(A) \subseteq \mathcal{U}_1^+(A)$ of *circular* units, i.e., those which map into cyclotomic units under every character of A. Secondly, we looked for bases in an even smaller subgroup $\mathcal{Y}(A) \subseteq \mathcal{U}_1^{\oplus}(A)$ of *constructible* units, which is the direct product of very explicit groups $\mathcal{W}(C)$ attached to the various cyclic $C \subseteq A$.

Instead of μ, we now had a pair of inclusions

$$\prod_{C\subseteq A} \mathcal{W}(C) = \mathcal{Y}(A) \subseteq \mathcal{U}_1^{\oplus}(A) \subseteq \mathcal{U}_1^+(A) \tag{1.3}$$

---

* Here begins our policy of omitting reference to the coefficient ring if the latter is $\mathbb{Z}$. Note further: in this introduction, groups of even order will be left aside, as they require certain finicky modifications in our procedure.

and were interested in the exploration of the factor group $\Gamma(A) = \mathcal{U}_1^{\oplus}(A)/\mathcal{Y}(A)$, whose order $c(A)$ we called the *circular index* of A. If $|C| = p$, it so happens that $\mathcal{W}(C) = \mathcal{U}_1^{\oplus}(C)$. Hence, for elementary abelian A, our new scenario is just the old one restricted to $\mathcal{U}_1^{\oplus}(-)$. Under a very mild condition on p, which is certainly satified for $p < 50^3$ and may even be completely vacuous (cf. "Vandiver's Conjecture"), the index of $\mathcal{U}_1^{\oplus}(A)$ in $\mathcal{U}_1^{+}(A)$ is prime to p for any p-group A; this leads to the divisibility

$$\mathrm{ind}(\mu) \mid c(A), \tag{1.4}$$

since both these numbers turn out to be p-powers *a priori*. Of course, they are equal for elementary abelian A.

Whenever the exponent of A is "small" (this notion being different for prime powers and composites but including all numbers ≤ 67), we even have $\mathcal{U}_1^{\oplus}(A) = \mathcal{U}_1^{+}(A)$. Thus, not much seems to be lost by the restriction to circular units, and a lot of transparency is gained. Since these investigations were initially conducted and recorded in terms of $\mathrm{ind}(\mu)$, one of the purposes of the present write-up is to reorganize the whole story around $c(A)$. Another task is the systematic inclusion of groups of even order.

In the sequel, we shall mainly deal with the following three questions:

1. For what abelian p-groups A is $c(A) = 1$?
2. How is $c(A)$ related to the class number of $\mathbb{Z}A$?
3. What can be said about $c(A)$ if A is not a p-group ?

The answer to the first question, explained in Sections 6 and 7 below, is remarkably simple: $c(A) = 1$ if and only if $|A| \leq p$ or p is regular. If this seems surprising, it should be noted that, unlike $\mathrm{ind}(\mu)$, the circular index is not automatically trivial for cyclic groups. If A is cyclic of order p^2, for instance, $\mathcal{Y}(A) = \mathcal{W}(A) \times \mathcal{W}(A^p)$ is a direct product of lattices of lower rank.

So far, the second question can be answered only for p-groups A, when p satisfies the "semi-regularity" condition which is the object of Vandiver's Conjecture. However, the simplicity of the result in that case provides some reason to believe that $c(A)$ is not as unnatural as it looks at first sight. In fact,

$$c(A)\chi(A) = |D^+(A)|\,, \tag{1.5}$$

where $\chi(A)$ is an easily computable quantity related to the complexity of the subgroup lattice of A (being $= 1$ for cyclic A), and $D^+(A)$ denotes the group of ideal classes, invariant under the standard involution, which become trivial in the maximal order $\mathbb{M}(A)$ of $\mathbb{Q}A$.

This is the subject of Section 8.

The third question is deliberately vague, since little is known apart from cyclic groups of order $n = pq$ (two distinct primes), which are dealt with in Section 9. For instance, we can say that $c(A) = 1$ whenever $(p-1)(q-1) \leq 72$, except for A of order 65, 85, or 91 — in which cases $c(A) \leq 3$. As an example, let us take $A = \langle x, y \rangle$ with $x^5 = y^7 = 1$; then we can use our old $w(z) = z^{-1} - 1 + z$ to write

down a basis for $\mathcal{Y}(A) = \mathcal{U}_1^{\oplus}(A) = \mathcal{U}_1^{+}(A)$ as follows: $\{w(x), w(y^i), w(z^j)\}$, where $z = xy$, $i = 1, 2$, and $j = 2^k$ with $0 \leq k \leq 10$.

After describing the genesis and nature of $\mathcal{Y}(A)$ in Section 2, we deal exclusively with p-groups until we come to Section 9. Here is an outline of what happens in the intervening pages.

Section 3 establishes an inductive formula of the form $c(K) = c(K^p)\, i(K^p)$ for the case of *cyclic* p-groups K. The new index $i(K)$ will later turn out to be trivial for regular p, thanks to a generalization of a lemma by Kummer. In the derivation of this inductive formula for $c(K)$, the pivotal question concerns "liftabilty": when is a cyclotomic number u in the image, under the obvious character, of $\mathcal{U}_1^{\oplus}(K)$? The answer is that u must be in the (explicitly describable) image of $\mathcal{W}(K)$.

Section 4 builds one of the bridges from cyclic p-groups to more general ones by showing that maps of type (1.2) — even when applied to subfunctors like $\mathcal{U}_1^{\oplus}(A)$ — are *a priori* of p-power index. Combined with some results of Section 3, this shows that $c(A)$, too, is a power of p.

A second bridge is built by Section 5, which deals with units in the p-adic group ring $\mathbb{Z}_pA$, and shows that maps of type (1.2) — here applied to $\mathcal{U}_1^{+}\mathbb{Z}_pA$ — are *a priori* surjective. Actually, this surjectivity will be required for a certain subgroup $\acute{\mathcal{U}}_1^{+}\mathbb{Z}_pA$, and this occasions some preliminary work on "polarized bases". Thereafter, the main tool is a logarithmic map into the additive structure of $\mathbb{Z}_pA$ which, however, functions only on very small pieces of $\mathcal{U}_1^{+}\mathbb{Z}_pA$.

Section 6 proves that $c(A) = 1$ if A is a p-group for regular p. In that case, the natural image of $\mathcal{U}_1^{\oplus}\mathbb{Z}A$ in $\acute{\mathcal{U}}_1^{+}\mathbb{Z}_pA$ is shown to be dense in the p-adic topology ("Density Lemma"), and the index $i(K)$ defined in Section 3 is found to be trivial ("Kummer's Lemma"); hence so is $c(K)$. Kummer's Lemma requires some logarithmic input from Section 5, restricted to cyclic groups. Via the Density Lemma for non-cyclic A, which uses Section 4, and the surjectivity result of Section 5, we finally establish the triviality of $c(A)$.

For any p-group A with $|A| > p$ and p irregular, Section 7 shows that $c(A) > 1$, thus providing a complete answer to Question (1) above. Since it is always true that $A \subset A'$ implies $c(A) \mid c(A')$, this problem reduces to groups of order p^2. For these, explicit (but ugly) non-constructible generators of $\Gamma(A)$ are described.

The regular prime $p = 2$, which complicates formulas and arguments in all prior sections except the seventh, is excluded by fiat in Section 8: it does not fit into the scenario of the first part, and is irrelevant to the ultimate aim of the section. We begin by showing, for $p > 2$, that $\mathcal{U}_1^{+}\mathbb{Z}_pA$ is a direct product of canonical subgroups $\mathcal{V}_p(C)$ associated with the various cyclic subgroups $C \subseteq A$. This is definitely false for $p = 2$. It eventually leads to a comparison between the "local" situation (with coefficients $\mathbb{Z}_p$) and the global one (with coefficients $\mathbb{Z}$), which in turn permits the derivation of the formula $|D^{+}(A)| = c(A)\chi(A)$ mentioned above.

2. Constructible units

This section gives a brief description of the unit groups to be studied. For details, the reader is referred to the first three paragraphs of [H8] or Chapter 2 of [S2].

For any finite group G, let $\Delta(G)$ denote the kernel of the augmentation map $\mathbb{Z}G \longrightarrow \mathbb{Z}$. Given a cyclic group C of order n, put $G = \mathrm{Aut}(C)$, and consider the factor group $H = G/\langle\star\rangle$, where $\star$ is the standard involution given by $z \mapsto z^{-1}$, for $z \in C$. We shall construct an injective H-homomorphism

$$w:\ \Delta^2(H) \longrightarrow \mathcal{U}_1^+(C) \tag{2.1}$$

whose image will be the group $\mathcal{W}(C)$ mentioned in the introduction. Of course, $\Delta^2(-)$ stands for the square of $\Delta(-)$. The map w will depend on the choice of a generator x of C, and we shall write $w_\alpha(x)$ for the image of $\alpha \in \Delta^2(H)$.

> The groups used by Bass in his seminal paper [B1] were essentially the w-images of $m\Delta(H) \subseteq \Delta^2(H)$, where m is a multiple of $|G|$. Apart from their dependence on m, which ruins certain functorial properties, these groups tend to have large indices, namely $m^{|H|-1|}/|H|$, in the corresponding $\mathcal{W}(C)$. For instance, $|C| = 67$ gives $\mathcal{W}(C) = \mathcal{U}_1^+(C)$, while the best Bass group has an index $> 10^{56}$ in $\mathcal{U}_1^+(C)$.

We begin with a homomorphism from $\Delta(G)$ to the units of the maximal order $\mathbb{M}(C)$ of $\mathbb{Q}C$,

$$u:\ \Delta(G) \longrightarrow \mathcal{U}_1\mathbb{M}(C) \simeq \prod_{d|n} \mathcal{U}(\zeta_d)\,, \tag{2.2}$$

where $d \neq 1$ ranges over the divisors of $n = |C|$, and ζ_d denotes a primitive d-th root of unity. It is defined by mapping the canonical basis $\{\sigma - 1) \mid 1 \neq \sigma \in G\}$ of $\Delta(G)$ according to the rules: $\quad u_{\sigma-1}(1) = 1, \quad$ and

$$u_{\sigma-1}(\zeta) = (\zeta - 1)^{\sigma-1} = 1 + \zeta + \cdots + \zeta^{c-1}\,, \tag{2.3}$$

with c chosen so that $\sigma(x) = x^c$, and ζ denoting a non-trivial n-th root of unity. For $\sigma = \star$, this formula gives $(\zeta^{-1} - 1)/(\zeta - 1) = -\zeta^{-1}$, a torsion element. Letting $\dot{\mathcal{U}}(-)$ stand for $\mathcal{U}(-)$ modulo torsion, we can therefore define a homomorphism on $\Delta(H)$, namely

$$\dot{u}:\ \Delta(H) \longrightarrow \dot{\mathcal{U}}_1\mathbb{M}(C) \simeq \prod_{d|n} \dot{\mathcal{U}}(\zeta_d) \tag{2.4}$$

in the obvious way. A slight variation on a fundamental lemma of Wolfgang Franz [Fra] now says that $\dot{u}$ is *injective.* The proof of this lemma, though compact and transparent, hinges on a "transcendental" result: the non-vanishing of Dirichlet L-functions at $s = 1$. In the present context, the injectivity of $\dot{u}$ is therefore something of a *deus ex machina.*

By algebraic means, Hyman Bass [B1] later proved that all the $\dot{u}$-maps attached to the various cyclic subgroups $C \subseteq A$ of a given finite abelian A could be strung

together and still yield an injection

$$\bigoplus_{C\subseteq A} \Delta(H_C) \longrightarrow \dot{\mathcal{U}}_1\mathbb{M}(A) \simeq \prod_K \dot{\mathcal{U}}(\zeta_K)\,, \tag{2.5}$$

where K runs over all non-trivial cyclic factor groups of A, and H_C is derived from $G_C = \mathrm{Aut}(C)$ as above, the subscript C now being unavoidable. By Dirichlet's Unit Theorem (transcendental tools again!), source and target of this map have the same $\mathbb{Z}$-rank; hence it is of finite index. So much for background.

To get from the maximal order back into the group ring, we use Lemma 2.1 of [H8], which states the following fact about the original map $\Delta(G) \xrightarrow{u} \mathcal{U}_1\mathbb{M}(C)$:

$$u_\delta(x) \in \mathcal{U}(C) \iff \delta \in \Delta^2(G). \tag{2.6}$$

By restriction, Franz's Lemma thus gives an injection $\dot{u} : \Delta^2(H) \longrightarrow \dot{\mathcal{U}}(C)$.

Example. If $|C|$ is prime to 6, consider the automorphisms $\sigma : x \mapsto x^2$ and $\tau : x \mapsto x^3$, as well as the elements $\delta = \sigma - 1 \in \Delta(G)$ and $\alpha = (\sigma-1)(\tau-1) \in \Delta^2(G)$. Then, for any non-trivial ζ, we have $u_\delta(\zeta) = (\zeta-1)^{\sigma-1} = \zeta + 1$, which cannot be lifted to $\mathcal{U}(C)$, and $u_\alpha(\zeta) = (\zeta+1)^{\tau-1} = (\zeta^3+1)/(\zeta+1)$, which corresponds to $u_\alpha(x) = x^2 - x + 1 \in \mathcal{U}_1(C)$.

To eliminate torsion, we invoke Lemma 2.6 of [CSW], which guarantees a direct decomposition

$$\mathcal{U}_1(A) = A \times \mathcal{U}_2(A)\,, \tag{2.7}$$

with $\mathcal{U}_2(A) = \mathcal{U}(A) \cap \big(1 + \Delta^2(A)\big) \subseteq \mathcal{U}_1^+(A)$ *torsion-free*. Explicitly, the projection $e : \mathcal{U}_1(A) \longrightarrow A$ is given by the formula

$$e : \sum c_z z \longmapsto \prod z^{c_z}\,, \tag{2.8}$$

with both the sum and product indexed by $z \in A$. Since e is clearly compatible with homomorphisms $h : A \longrightarrow B$, so is the formula (2.7).

This functoriality is obviously inherited by the split $\mathcal{U}_1^+(A) = A_2 \times \mathcal{U}_2(A)$. Thus, if $\mathcal{U}_2(B) = \{1\}$ — i.e., $\mathcal{U}_1(B)$ is a torsion group — it follows that $\mathcal{U}_2(A)$ is contained in the kernel of the induced map $\mathcal{U}_1^+(A) \to \mathcal{U}_1^+(B)$, with equality if and only if h yields an injection $A_2 \hookrightarrow B_2$. If A has no elements of order 8, we can take $B = A/A^4$ in this scenario and hence characterize $\mathcal{U}_2(A)$ by

$$\mathcal{U}_2(A) = \ker\big[\mathcal{U}_1^+(A) \to A_2\big]\,,$$

with the map to $A_2 = \mathcal{U}_1^+(A/A^4)$ induced by the canonical projection $A \to A/A^4$. *Note:* we may sometimes use the redundant notation $\mathcal{U}_2(A) = \mathcal{U}_2^+(A)$; if A has odd order, we can avoid reference to $\mathcal{U}_2(A)$ altogether by using its alias $\mathcal{U}_1^+(A)$.

The map w advertised in (2.1) above is now obtained by letting $w_\alpha(x)$ be the projection of $u_\alpha(x)$ onto the second component in the decomposition (2.7). For

$\alpha = (\sigma - 1)(\tau - 1)$ as in the example above, we retrieve the element $w_\alpha(x) = x^{-1} - 1 + x$ already encountered in the introduction. Let us summarize.

Theorem 2.1. *For a finite cyclic group $C = \langle x \rangle$, the formula $w_\alpha(x) = u_\alpha(x)^{1-e}$ defines an H_C-isomorphism $\alpha \mapsto w_\alpha(x)$ from $\Delta^2(H_C)$ onto a subgroup $\mathcal{W}(C)$ of $\mathcal{U}_2(C)$. The direct product $\mathcal{Y}(A)$ of these groups $\mathcal{W}(C)$, as C ranges over the cyclic subgroups of a finite abelian group A, is a sublattice of $\mathcal{U}_2(A)$, the canonical torsion-free component of $\mathcal{U}(A)$.*

Elements of $\mathcal{Y}(A)$ will be called *constructible* units.

Remark 2.2. It is important to realize that a unit $u \notin \mathcal{Y}(A)$ cannot become constructible in a larger group $A' \supset A$. Indeed, we would have $u = v \cdot v'$ by the direct decomposition $\mathcal{Y}(A') = \mathcal{Y}(A) \times \prod_{C'} \mathcal{W}(C')$, where $C' \not\subseteq A$, and since $u^N \in \mathcal{Y}(A)$ for some $N \in \mathbb{Z}$, it would follow that $(v')^N = 1$. Thus $\Gamma(A) \longrightarrow \Gamma(A')$ is injective, and $c(A)$ divides $c(A')$

The following proposition gives explicit formulas for u and w in terms of the sums $f_i(x) = 1 + x + \cdots + x^{i-1}$ defined for any $i > 0$. It is proved in [H8], where it happens to have the same number as here. Without risk of confusion, we use the same notation for elements of G and their counterparts in H.

Proposition 2.3. *Let $\alpha = (\sigma - 1)(\tau - 1) \in \Delta^2(G)$ with $\sigma : x \mapsto x^c$, and let b, k be positive integers with $bc = 1 + kn$. Then $u_\alpha(x) = f_b(x^\sigma) f_c(x^\tau) - k f_n(x)$ and $w_\alpha(x) = x^{-(\tau-1)(c-1)/2} u_\alpha(x)$.*

Most of our structures are H-modules, where $H = H_K$ for a maximal cyclic subgroup K of A. Except when we need the bijectivity of each $\Delta^2(H_C) \xrightarrow{w} \mathcal{W}(C)$, we usually compose these maps with the canonical surjections $\Delta^2(H) \longrightarrow \Delta^2(H_C)$, using a single $H = H_n$ derived from $G_n = (\mathbb{Z}/n\mathbb{Z})^\times$, where n is such that $A^n = \{1\}$.

The kind of bases for $\mathcal{Y}(A)$ shown in the introduction are available whenever H happens to be cyclic. In that case, if $H = \langle \sigma \rangle$, multiplication by $(\sigma - 1)$ yields isomorphisms

$$\mathbb{Z}H/\Sigma(H) \xrightarrow{\sim} \Delta(H) \xrightarrow{\sim} \Delta^2(H)\,, \tag{2.9}$$

where $\Sigma(H)$ denotes the ideal generated by the sum of the elements of H. Mapping 1 to $w_\alpha(x)$, where α generates $\Delta^2(H)$ and x generates K, we get an isomorphism $\mathbb{Z}H/\Sigma(H) \longrightarrow \mathcal{W}(K)$. Hence the product over the H-orbit $\{w_\alpha(z) \mid \langle z \rangle = K\}$ is trivial, and a basis of $\mathcal{W}(K)$ is obtained by leaving out one element of the orbit. Bases of the groups $\mathcal{W}(C)$ for other $C \subseteq A$ are formed analogously, always using the same $w_\alpha(-)$. This is how we got the bases mentioned in the introduction.

H_n is cyclic in exactly the following cases ($p \neq q$ odd primes): $n = 2^r p^s$, with $r \leq 2$ or $s = 0$, and $n = 2^r p^s q^t$, with $r \leq 1$ and $|H_{p^s}|$ relatively prime to $|H_{q^t}|$.

Here is the argument for $n = pq$. Let $J \subseteq H_n$ be the image of the subgroup generated by $(-1,1)$ and $(1,-1)$ in $G_p \times G_q = G_n$. Then $H_n/J \simeq H_p \times H_q$, and therefore the cyclicity of H_n implies that of $H_p \times H_q$. Conversely, suppose that $|H_q|$ is odd and thus relatively prime to $|G_p|$. Then $G_p \times G_q^2$ is a cyclic subgroup of G_n, which maps onto H_n because it does not contain the involution $\star = (-1,-1)$. This argument works just as well for $n = p^s q^t$. The rest is easy.

An element of $\mathcal{U}_1^+(A)$ will be called *circular*, if every character $\psi : A \longrightarrow \mathbb{C}^\times$ maps it into a real cyclotomic unit, i. e., a unit of $\mathbb{Z}[\zeta_d + \zeta_d^{-1}]$ in the multiplicative semi-group generated by ζ_d and $\{1 - \zeta_d^a \mid a \in \mathbb{Z}\}$, where d is the order of ψ. For $k = 1, 2$, the group $\mathcal{U}_k^\oplus(A)$ of circular units in $\mathcal{U}_k(A)$ obviously contains $\mathcal{Y}(A)$, and we wind up with a pair of inclusions

$$\mathcal{Y}(A) \subseteq \mathcal{U}_2^\oplus(A) \subseteq \mathcal{U}_2(A) \tag{2.10}$$

whose indices will be denoted by $c(A)$ and $c'(A)$, respectively. In practice, $\mathcal{U}_1(-)$ is easier to handle than $\mathcal{U}_2(-)$, and we shall usually read off the same indices from the inclusions $A_2 \cdot \mathcal{Y}(A) \subseteq \mathcal{U}_1^\oplus(A) \subseteq \mathcal{U}_1^+(A)$, where $A_2 = \{z \in A \mid z^2 = 1\}$.

The index $c'(A)$ is related to the class number $h^+(A)$ of the maximal order in the real subalgebra of $\mathbb{Q}A$. Of course, this is a product of class numbers h_d^+ for rings $\mathbb{Z}[\zeta_d + \zeta_d^{-1}]$ with $d \mid n$. In fact, if n has fewer than four distinct prime divisors — which will certainly be the case in the present paper — Sinnott's formula (cf. [Si], p.107) implies $c'(A) \mid h^+(A)$.

For small n, we simply have $h^+(A) = 1$, "small" meaning < 136 if one assumes the generalized Riemann hypothesis (cf. [Wa], p.352). More importantly, for prime powers $n = p^m$, it is prime to p for at least $p < 50^3$ and maybe always (Vandiver's Conjecture). At any rate, $c'(A)$ is very elusive, leaving the *circular index* $c(A)$ as the more tractable invariant and one of the main objects of this study.

3. Cyclic p-groups

Constructible units were introduced in [HR2] by means of *ad hoc* formulas and restricted to p-groups of odd order. Moreover, the main result for *cyclic* groups — Formula (3.2) below — was left implicit, hidden away in a commutative square, *loc. cit.*, Diagram (9). The present section tries to repair these shortcomings as well as those of a previous attempt ([H8], §4) in this direction. Apart from its deliberate sketchiness, the latter is flawed by a gap in the proof of its first lemma and some imprecisions involving the prime 2.

All subgroups of a cyclic p-group $C = \langle x \rangle$ can be described in terms of repeated applications of the single endomorphism $\pi : x \mapsto x^p$. Many properties of $\mathbb{Z}C$ thus become accessible by induction, especially with the help of the fundamental pull-

back diagram (cf. [KM], §1)

$$\begin{array}{ccc} \mathbb{Z}C & \xrightarrow{\psi} & \mathbb{Z}[\zeta_n] \\ \pi\downarrow & & \downarrow \\ \mathbb{Z}C^p & \xrightarrow{\rho} & \mathbb{F}_pC^p \end{array} \tag{3.1}$$

in which $\psi : x \mapsto \zeta_n$ is a character of order $n = |C|$, and $\rho : \mathbb{Z} \longrightarrow \mathbb{F}_p$ is just reduction modulo p of the coefficient ring $\mathbb{Z}$. Incidentally, a similar pull-back is available with the p-adic integers $\mathbb{Z}_p$ in the place of $\mathbb{Z}$.

The eventual aim of this section is to establish a recursion relation of the form

$$c(C) = c(C^p) \cdot i(C^p)\,, \tag{3.2}$$

for the circular index of C. For any non-trivial subgroup $K \subseteq C$, the number $i(K)$ is defined as follows. Since t^π and t^p are congruent modulo p for any $t \in \mathbb{Z}C$, the map $t \mapsto t^{\pi-p} = t^\pi/t^p$ produces a homomorphism from $\mathcal{U}(K)$ to the kernel of $\rho : \mathcal{U}(K) \longrightarrow \mathcal{U}\mathbb{F}_pK$. For any subgroup $\mathcal{V} \subseteq \mathcal{U}(K)$, let us abbreviate $\mathcal{V} \cap \ker(\rho)$ by $\ker_p \mathcal{V}$. Then $i(K)$ is the order of cokernel $I(K)$ of the map

$$\mathcal{U}_2^\oplus(K) \xrightarrow{\pi-p} \ker\nolimits_p \mathcal{U}_2^\oplus(K) \tag{3.3}$$

so obtained. Most of the arguments required can be gleaned from the first two paragraphs of [HR2].

Some of the fine points missed in [H8] have to do with the case $p = 2$. For instance, the pull-back derived from (3.1) for $\star$-symmetric 1-units has a slight asymmetry because π maps $\mathcal{U}_1^+(C) = C_2 \times \mathcal{U}_2(C)$ into $\mathcal{U}_2(C^p)$. We record the result for the subgroup of circular units, which is our main concern:

$$\begin{array}{ccc} \mathcal{U}_1^\oplus(C) & \xrightarrow{\psi} & \mathcal{U}^\oplus(\zeta_n) \\ \pi\downarrow & & \downarrow \\ \mathcal{U}_2^\oplus(C^p) & \xrightarrow{\rho} & \mathcal{U}\mathbb{F}_pC^p \end{array} \tag{3.4}$$

is a pull-back. Remember that the difference between $\mathcal{U}_1^\oplus(-)$ and $\mathcal{U}_2^\oplus(-)$ does not exist for groups of odd order.

In order to use (3.4) for induction, one needs to clarify what goes on in the upper right corner. For cyclic p-groups, it turns out that the ψ-images of $\mathcal{W}(C)$ and $\mathcal{U}_1^\oplus(C)$ are essentially (i.e., up to $\pm$ for $p = 2$) identical, and that the restriction of ψ to $\mathcal{W}(C)$ is injective. This will follow from the next two lemmas.

Lemma 3.1. *Let $\delta \in \Delta(G)$. Then $(\zeta_n - 1)^\delta \in \psi\big(\mathcal{U}_1(C)\big)$ implies that $\delta \in \Delta^2G$ or $\delta \in (\star - 1) + \Delta^2G$, the latter occurring only for $p = 2$.*

Proof. Recall the unique decomposition $\delta = (\sigma - 1) + \alpha$ with $\alpha \in \Delta^2(G)$ and $\sigma = e(\delta)$, where e is as given in (2.8). According to (2.6), there is an element $u_\alpha(x) \in \mathcal{U}_1(C)$ such that $u_\alpha(\zeta_d) = (\zeta_d - 1)^\alpha$, for all $1 \neq d \mid n$. Therefore we need only show that $(\zeta_n - 1)^{\sigma-1} \in \psi\big(\mathcal{U}_1(C)\big)$ implies $\sigma = 1$ or $\sigma = *$.

The fact that $(\zeta_n - 1)^\alpha \in \psi\big(\mathcal{U}_1(C)\big)$ for all $\alpha \in \Delta^2(G)$ also means that the standard isomorphism $G \longrightarrow \Delta(G)/\Delta^2(G)$ induces a homomorphism

$$h : G \longrightarrow \mathcal{U}(\zeta_n)/\psi\big(\mathcal{U}_1(C)\big)\,, \tag{3.5}$$

given by $\sigma \mapsto (\zeta_n - 1)^{\sigma-1}\psi\big(\mathcal{U}_1(C)\big)$. We will show that its kernel contains at most $\star$ (and that only if $p = 2$). Suppose that $\sigma \neq 1$ lies in the kernel of h.

Then $\sigma : x \mapsto x^c$ for some c prime to p, and $f_c(\zeta_n) = (\zeta_n^c - 1)/(\zeta_n - 1) = 1 + \zeta_n + \cdots + \zeta_n^{c-1}$ is equal to $\psi(v(x))$ for some unit $v(x) \in 1 + \Delta(C)$. Obviously $f_c(\zeta_n)$ must be congruent to 1 modulo $\zeta_n - 1$, and since it is visibly congruent to c, we have $c \equiv 1 \pmod{p}$.

This settles the matter for $n = p$. Moreover, unless $p = 2$ and $\sigma = \star$, it means that a suitable power of σ is the automorphism $x \mapsto x^{1+n/p}$. If σ is in the kernel of h, then so is that power. Without loss of generality, we may therefore assume that $c = 1 + n/p$ and $\sigma \neq \star$.

The hypothetical unit $v(x)$ must have the form $v(x) = f_c(x) - \Phi_n(x)k(x)$, where $f_c(x) = 1 + x + \cdots + x^{c-1}$ and Φ_n is the n-th cyclotomic polynomial. Since $v(\zeta_n) = f_c(\zeta_n)$ is perfectly good, whatever is amiss must show up in the unit $v(y) = f_c(y) - pk(y) \in \mathcal{U}_1(C^p)$, where $y = x^p$. Since $c = 1 + n/p$, we have $f_c(\eta) = 1$ for all non-trivial (n/p)-th roots of unity η. Therefore $v(y)$ looks like the element $l(y) = 1 - pk(y) \in \mathbb{Z}C^p$ under all non-trivial characters of C^p, while the condition $v(1) = 1$ translates via $1 = c - pk(1)$ to $l(1) = 1 - n/p$. We shall see that such a pair $v(y)$, $l(y)$ cannot exist.

Multiplication by $l(y) = a_0 + a_1 y + \cdots + a_{\mu-1}y^{\mu-1}$ is given by a matrix whose columns are cyclic permutations of $[a_0, a_1, \ldots, a_{\mu-1}]$. If, as in this case, p divides $a_0 - 1$ as well as all a_i for $i > 0$, Lemma 1.4 of [HR2] makes the determinant of such a matrix congruent to 1 modulo n. On the other hand, it is the product of the absolute Galois norms of all Wedderburn components of $l(y)$. In other words,

$$(1 - n/p) \cdot \prod_{\varphi \neq 1} N_\varphi\, \varphi\big(v(y)\big) \equiv 1 \pmod{n}\,, \tag{3.6}$$

where φ runs over the non-trivial rational characters of C^p, and N_φ denotes the norm on the field $\mathbb{Q}(\varphi(y))$. Since $v(y) \in \mathcal{U}_1(C^p)$, each of these norms is ± 1 (with -1 occurring only if $p = 2$). Hence (3.6) implies $1 - n/p \equiv \pm 1 \pmod{n}$ — an impossibility unless $n = 4$ and $\sigma = \star$. □

Lemma 3.2. *If $n > p$, let $s_1 = 1 + \tau_1 + \cdots + \tau_1^{p-1} \in \mathbb{Z}G$ with $\tau_1 : x \mapsto x^{1+n/p}$. Then $w(\zeta_n^p) = w(\zeta_n)^{s_1}$ for any $w(x) \in C_2 \cdot \mathcal{W}(C)$.*

Proof. It is well-known and elementary that $(\zeta_n - 1)^{s_1} = (\zeta_n^p - 1)$ and that $\zeta_n^{s_1} = \pm\zeta_n^p$, with the minus sign occurring only for $p = 2$. It follows that $v(\zeta_n)^{s_1} = v(\zeta_n^p)$ for any $v(\zeta_n) = \zeta_n^a(\zeta_n - 1)^\beta$, with $a \in \mathbb{Z}$ and $\beta \in \Delta(G)$ — as long as a is even when

$p = 2$. For $\beta = (\sigma - 1)(\tau - 1) \in \Delta^2(G)$, one easily checks that $v(\zeta_n)$ is real (i.e., invariant under $\star$) if and only if $2a \equiv (1 - c)(1 - d) \pmod{n}$, where $\sigma : x \mapsto x^c$ and $\tau : x \mapsto x^d$. If $p = 2$, this makes $2a$ divisible by 4. □

Proposition 3.3. *The character ψ defined by $\psi(x) = \zeta_n$ induces a bijection of $C_2 \cdot \mathcal{W}(C)$ onto $\psi\big(\mathcal{U}_1^{\oplus}(C)\big)$.*

Proof. For $w(x) \in C_2\mathcal{W}(C)$ suppose that $w(\zeta_n) = 1$. Then $w(\zeta_n^p) = 1$ as well, either because all of $\mathcal{W}(C^p)$ is trivial (i.e. n is too small) or because $w(\zeta_n^p) = w(\zeta_n)^{s_1} = 1$ by Lemma 3.2. By induction, $w(\zeta_d) = 1$ for all $d \mid n$, whence the injectivity.

For the surjectivity, let $v(x) \in \mathcal{U}_1^{\oplus}(C)$ and consider $v(\zeta_n) = \zeta_n^a(\zeta_n - 1)^\beta$, with $a \in \mathbb{Z}$ and $\beta \in \Delta(G)$. Lemma 3.1 ensures that $\beta = (\iota - 1) + \alpha$ with $\alpha \in \Delta^2(G)$ and $\iota = 1$ or $= \star$. Putting $u(x) = v(x)/w_\alpha(x)$, we now get $u(\zeta_n) = \zeta_n^c$ for some $c \in \mathbb{Z}$. Since $v(\zeta_n)$ was real, it follows that $u(\zeta_n) = \pm 1$. Replacing $w_\alpha(x)$ by $x^{n/2}w_\alpha(x)$, if necessary, we can always get $u(\zeta_n) = 1$. □

Remark. Abbreviating $\psi(\mathcal{U}_1^{\oplus}(C))$ by $\mathcal{L}(\zeta_n)$ — the $\mathcal{L}$ stands for "liftable" — Proposition 3.3 yields an isomorphism $\psi : C_2\mathcal{W}(C) \to \mathcal{L}(\zeta_n)$, and an inductive application of Lemma 3.2 says that all the Galois norms $\mathcal{L}(\zeta_n) \to \mathcal{L}(\zeta_{n/p^i})$ are surjective.

Proposition 3.4. *There exists a short exact sequence of finite H-modules of the form $1 \longrightarrow \Gamma(C^p) \longrightarrow \Gamma(C) \longrightarrow I(C^p) \longrightarrow 1$.*

Proof. For use with the decomposition $\mathcal{U}_1^{\oplus}(C) = C_2\mathcal{W}(C) \times \ker(\psi)$ inferred from Proposition 3.3, we shall modify the product $C_2\mathcal{Y}(C) = C_2\mathcal{W}(C) \times \mathcal{Y}(C^p)$ so as to make the second factor fit into $\ker(\psi)$. Indeed, if $n = p^m$, we write

$$\mathcal{Y}(C) = W_0 \times \prod_{k=1}^{m-1} W_k = W_0 \times \prod_{k=1}^{m-1} W_{k-1}^{\pi - s_k}\,, \tag{3.7}$$

where $W_k = \mathcal{W}(C^{p^k})$ and $s_k = 1 + \tau_k + \cdots + \tau_k^{p-1} \in \mathbb{Z}G$, with $\tau_k : x \mapsto x^{1+n/p^k}$. The point is that each s_k acts as the Galois norm $\mathbb{Q}(\zeta_d)^\times \longrightarrow \mathbb{Q}(\zeta_d^p)^\times$ for $d = n/p^{k-1}$, and that $W_{k-1}^{\pi - s_k}$ lies in the kernel of ψ by Lemma 3.2 applied to $C^{p^{k-1}}$.

Now consider the commutative square

$$\begin{array}{ccc} \prod_{k=1}^{m-1} W_{k-1} & \xrightarrow{\ \kappa\ } & \ker(\psi) \\ \pi \downarrow & & \downarrow \simeq \\ \mathcal{U}_2^{\oplus}(C^p) & \xrightarrow{\ \pi - p\ } & \ker(\rho) \end{array} \tag{3.8}$$

whose horizontal arrows denote the product $\kappa = (\pi - s_1) \times \cdots \times (\pi - s_{m-1})$ and the map shown as (3.3) for $K = C^p$, respectively. By the preceding discussion, the cokernel $\ker(\psi)/\mathrm{im}(\kappa)$ of the former is isomorphic to $\Gamma(C)$, while the cokernel of the latter is clearly $I(C^p)$.

The pull-back property of (3.4) makes the right vertical arrow of (3.8) bijective. Moreover, the bottom arrow represents an injection: $u^p = u^\pi$ inductively implies $u^{p^m} = u^{\pi^m} = 1$, but $\mathcal{U}_2(-)$ has no torsion. Hence by a standard diagram chase (e.g., the "snake lemma"), the natural map $\ker(\psi)/\mathrm{im}(\kappa) \to I(C^p)$ of the horizontal cokernels in (3.8) is surjective, and its kernel is canonically isomorphic to $\Gamma(C^p)$, the cokernel of the left vertical arrow. □

Remark. The recursion relation (3.2) is immediate from this proposition. Indeed, since $c(C_p) = 1$ always, we inductively obtain the explicit formula

$$c(C) = i(C^p) \cdots i(C^{p^{m-1}}) \,. \tag{3.9}$$

In Section 6, the condition $i(K) = 1$ will be seen to characterize regular primes, by a generalization of a well-known lemma of Kummer. For $p = 2$, the latter has an elementary proof (avoiding the p-adic logarithms of Section 5) via the index $j(K) = \left[\ker_p \mathcal{Y}(K) : \mathcal{Y}(K)^{\pi-p}\right]$ and the following corollary. All induction arguments below start from the fact that $c(C_p) = 1$.

Corollary 3.5. $c(C) = i(C^p) \cdots i(C^{p^{m-1}}) = 1 \iff j(K) = 1$ *for all proper subgroups* $K \subset C$.

Proof. $c(C) = 1 \implies c(K) = i(K) = 1$, by (3.9). But $c(K) = 1$ means $\mathcal{U}_2^{\oplus}(K) = \mathcal{Y}(K)$ and hence $i(K) = j(K)$. Conversely, we may assume $c(C^p) = 1$ by induction hypothesis. Then $i(C^p) = j(C^p)$, and $c(C) = c(C^p)j(C^p) = 1$. □

Proposition 3.6. *The indices* $j(C)$, $i(C)$, *and* $c(C)$ *are powers of* p.

Proof. We will show first: for every $u \in \mathcal{Y}(C)$, a certain power u^{p^s} lies in $\mathcal{Y}(C)^{\pi-p}$. By induction, we may assume that a certain p^r-th power of u^π lies in $\mathcal{Y}(C^p)^{\pi-p}$. In other words, $u^{\pi p^r} = v^{\pi(\pi-p)}$ for a suitable $v \in \mathcal{Y}(C)$, because $\pi : \mathcal{Y}(C) \longrightarrow \mathcal{Y}(C^p)$ is surjective. Now $w = u^{p^r}/v^{\pi-p}$ lies in the kernel of that surjection, and hence $w^{p-\pi} = w^p = u^{p^{r+1}}/v^{p(\pi-p)}$, so that finally $u^{p^{r+1}} = (v^p w)^{p-\pi}$.

We have shown that the index $\left[\mathcal{Y}(C) : \mathcal{Y}(C)^{\pi-p}\right]$ is a p-power. Hence so is its divisor $j(C)$. As for $c(C)$, we may inductively assume that $c(K)$ is a p-power for all proper subgroups $K \subset C$. Then $\mathcal{U}_2^{\oplus}(K)^{p^r} \subseteq \mathcal{Y}(K)$ together with $\mathcal{Y}(K)^{p^s} \subseteq \mathcal{Y}(K)^{\pi-p}$ implies that $i(K)$ is a p-power, too. Now apply (3.9). □

4. Functors on cyclotomic algebras

The proof that $c(A)$ is a p-power for *any* p-group A depends, oddly enough, on a property of maximal orders. Let $\mathcal{E}(A)$ denote the subgroup of the those units of $\mathbb{M}(A)$ which are congruent to 1 modulo the ideal $\Delta(A)\mathbb{M}(A)$. This means that $u \in \mathcal{E}(A)$ if and only if every projection $\psi : \mathbb{M}(A) \longrightarrow \mathbb{Z}[\zeta]$ onto a Wedderburn

component gives $\psi(u) \in \mathcal{E}(\zeta)$, i.e. $\psi(u) \equiv 1$ modulo the ideal $(\zeta-1)\mathbb{Z}[\zeta]$. The units $u \in \mathcal{E}(A)$ which furthermore always have $\psi(u) \in \mathcal{U}^{\oplus}(\zeta)$ are collectively denoted by $\mathcal{E}^{\oplus}(A)$. The crucial result concerns the $\mathcal{E}^{\oplus}$-version of the map μ shown in (1.2).

Proposition 4.1. *The natural map*

$$\mu : \prod_{C \subseteq A} \mathcal{E}^{\oplus}(C) \longrightarrow \mathcal{E}^{\oplus}(A)\,, \tag{4.1}$$

as C ranges over all cyclic subgroups of A, has p-power index.

This is not so much a property of $\mathcal{E}^{\oplus}(-)$ as a result of the combinatorics of cyclic subgroups and factor groups of A. As we shall see, it applies to any sufficiently well-behaved functor on cyclotomic $\mathbb{Q}$-algebras, i.e., finite direct products of cyclotomic fields. The reason for using $\mathcal{E}^{\oplus}(-)$ is the following simple fact.

Lemma 4.2. *$\mathcal{U}_1^{\oplus}(A)$ is a subgroup of p-power index in $\mathcal{E}^{\oplus}(A)$.*

Proof. Let $\mathcal{E}\mathbb{Z}_pA$ denote the p-adic analog of $\mathcal{E}(A)$, i.e., units of the maximal order in $\mathbb{Q}_pA$ which are $\equiv 1$ modulo the appropriate $(\zeta-1)\mathbb{Z}_p[\zeta]$ in each component. Then $\mathcal{E}\mathbb{Z}_pA$ (a multiplicative group!) is a free $\mathbb{Z}_p$-module by II.15.5 of [Ha].

By general principles (cf. [S1], proof of II.2.9), however, the unit group of $\mathbb{Z}_pA$ must be of finite index in that of the maximal p-adic order.

Hence the right vertical arrow in the following square of injections,

$$\begin{array}{ccc} \mathcal{U}_1(A) & \longrightarrow & \mathcal{U}_1\mathbb{Z}_pA \\ \downarrow & & \downarrow \\ \mathcal{E}(A) & \longrightarrow & \mathcal{E}\mathbb{Z}_pA \end{array} \tag{4.2}$$

can only be of p-power index. This diagram is a pull-back, that is: if we read the arrows as inclusions, we have $\mathcal{U}_1(A) = \mathcal{E}(A) \cap \mathcal{U}_1\mathbb{Z}_pA$. Indeed, $v \in \mathbb{M}(A)$ implies $|A| \cdot v \in \mathbb{Z}A$ (cf. [Re], Theorem 41.1), whereas $v \in \mathbb{Z}_pA$ implies $N \cdot v \in \mathbb{Z}A$ with N prime to p. It follows that the left vertical arrow,too, has p-power index. Now throw in a couple of $\oplus$ superscripts, and the proof is done. □

Remark. It is clear how this lemma translates Proposition 4.1 into the statement that the first horizontal arrow in

$$\begin{array}{ccc} \prod_C \mathcal{U}_1^{\oplus}(C) & \longrightarrow & \mathcal{U}_1^{\oplus}(A) \\ \downarrow & & \downarrow \\ \prod_C \mathcal{E}^{\oplus}(C) & \longrightarrow & \mathcal{E}^{\oplus}(A) \end{array} \tag{4.3}$$

is also of p-power index, and how this leads, via Proposition 3.6, to the desired property of $c(A)$. For the rest of this section, we shall deal with the proof of Proposition 4.1.

4.1. Admissible functors

Keeping $n = p^m$ fixed, let ε_k stand for the particular p^k-th root of unity $\varepsilon_k = \exp(2\pi i p^{-k}) \in \mathbb{C}$ for $k = 0, 1, \ldots, m$. Let $\mathcal{C}_{p^m}$ denote the full subcategory of finite dimensional $\mathbb{Q}$-algebras whose simple components are isomorphic to some of the cyclotomic fields $F_k = \mathbb{Q}[\varepsilon_k]$. Note that G acts naturally on all objects of $\mathcal{C}_{p^m}$, and that F_k is the subfield of F_m corresponding to the group $G(k)$ generated by the automorphism $\varepsilon_m \mapsto \varepsilon_m^{1+p^k}$, for $k > 0$, whereas $G(0) = G$. We shall also need to refer to the standard inclusions $\iota_{k,l} : F_k \to F_l$ given by $\varepsilon_k \mapsto \varepsilon_l$, for $k \leq l$.

For any commutative ring Λ, a finitely generated free Λ-module will be referred to as a Λ-*lattice*.

Definition 4.3. A Λ-lattice valued functor V on $\mathcal{C}_{p^m}$ is said to be *admissible*, if
(i) it commutes with direct products, and $V(\mathbb{Q}) = \{0\}$;
(ii) $V(\iota_{k,l})$ bijects $V(F_k)$ onto $V(F_l)^{G(k)}$ for all $0 \leq k \leq l \leq m$;
and is said to be *cyclogenic* (mod p) for the abelian p-group A, if the map

$$\mu_{V,A} : \prod_{C \subseteq A} V(\mathbb{Q}C) \longrightarrow V(\mathbb{Q}A)$$

is of p-power index.

N.B. Conditions (i) and (ii) ensure in particular that the image-lattices never have (non-trivial) G-invariant elements, no non-zero submodules on which G acts via the trivial character.

If V satisfies (i), any epimorphism $A \to A'$ will entail surjections $\mathbb{Q}A \to \mathbb{Q}A'$ and $V(\mathbb{Q}A) \to V(\mathbb{Q}A')$; hence V is cyclogenic for A', if it is cyclogenic for A. This will allow us to concentrate on the case $A = C \times \cdots \times C$ with $|C| = p^m$.

Lemma 4.4. *Let V be the functor which commutes with products and associates with $\mathbb{Q}(\varepsilon_k)$ the $\mathbb{Z}$-lattice formed by $\mathcal{E}^{\oplus}(\varepsilon_k)$ modulo torsion. Then V is admissible.*

Proof. For $k > 0$, the group $G(k)$ injects into H because it does not contain the involution $\star$. Suppose that $u = (\varepsilon_m - 1)^\delta$ with $\delta \in \Delta(G)$ is fixed *modulo torsion* by $\tau \in G_k$, i.e. that $(\varepsilon_m - 1)^{\delta(\tau-1)}$ has finite order. By Proposition 3.3, the finite order is inherited by $w_\alpha(\varepsilon_m)$, where $\alpha = \delta(\tau - 1) \in \Delta^2(H)$. This is impossible unless $\alpha = 0$, which means that δ is divisible by the sum over the powers of τ. If $\tau : \varepsilon_m \mapsto \varepsilon_m^{1+p^k}$, the order of τ is $\nu = p^{m-k}$, and $1 + \tau + \cdots + \tau^{\nu-1}$ equals $s_1 \cdots s_{m-k}$ in the notation of the proof of Proposition 3.4. Thus $\delta = s_1 \cdots s_{m-k}\beta$ for some $\beta \in \Delta(G)$, and by iterating the formula $(\varepsilon_m - 1)^{s_1} = (\varepsilon_m^p - 1)$ already met in the proof of Lemma 3.2, we see that $u = (\varepsilon_k - 1)^\beta$. We have proved:

$$\dot{\mathcal{U}}^{\oplus}(\varepsilon_m)^{G(k)} = \dot{\mathcal{U}}^{\oplus}(\varepsilon_k)\,, \tag{4.4}$$

where the dot means "modulo torsion", as usual. To finish the proof we must show that $\mathcal{E}$ may be substituted for $\mathcal{U}$ in this formula. But this is clear since the ideal $(\varepsilon_m - 1)\mathbb{Z}[\varepsilon_m]$ intersects F_k exactly in $(\varepsilon_k - 1)\mathbb{Z}[\varepsilon_k]$. □

If we were dealing only with $p > 2$, the references to torsion could have been omitted, because then $\mathcal{U}^{\oplus}(\varepsilon_k) = (\varepsilon_k^{-1} - \varepsilon_k)^{\Delta(G)}$ is torsion free. The slight advantage in working modulo torsion is that it makes every cyclotomic unit look like $(\varepsilon_k - 1)^{\delta}$. Note also that the torsion possible here does not interfere with the claim made in Proposition 4.1.

In view of this lemma, Proposition 4.1 follows from the main result of [H4], which says that an admissible $\mathbb{Z}$-lattice functor on $\mathcal{C}_{p^m}$ is automatically cyclogenic (cf. *ibid.*, Proposition 1.2). This is derived from a lengthy matrix-argument which the reader may wish to avoid. In the present treatment, we shall first prove a relative result to the effect that, for admissible functors, the cyclogenic property is *equivalent* to certain matrix-conditions. This will open an alternative route to the proof of Proposition 4.1.

Each of the matrices in question will have entries in one of the group rings $\mathbb{Z}G_{p^h}$, for $h = 1, \ldots, m$. Letting R_h denote the ring $\mathbb{Z}/p^h\mathbb{Z}$, we have $G_{p^h} = R_h^{\times}$. Every element $a \in R_m$ can be uniquely decomposed as

$$a = p^{v(a)}u(a)\,, \tag{4.5}$$

where $u(a) \in R_{l(a)}^{\times}$ for $l(a) = m - v(a)$. For every $h = 1, \ldots, m$ and $a \in R_m$, we put $u_h(a) = u(a)$ in case $l(a) = h$, and $u_h(a) = 0$ otherwise.

The test groups $A = C \times \cdots \times C$ (cf. "N.B." following Definition 4.3), will be written additively, i.e. as free R_m-modules $A = R_m^r$. For $x = (x_1, \ldots, x_r) \in A$, we define $l(x)$ to be the p-logarithm of the order $p^{l(x)}$ of x, in other words, the maximum of the numbers $l(x_k)$. For a pair $x, y \in A$, the "dot product" will be the usual $x \cdot y = \sum_k x_k y_k \in R_m$.

After choosing a set S of representatives for the G-orbits of A, we put $S_h = \{x \in S \mid l(x) \geq h\} \subseteq S$ and define the $S_h \times S_h$-matrix $M_{S,h}$ by its entries:

$$M_{S,h}(x, y) = u_h(x \cdot y)\,. \tag{4.6}$$

The determinant $D_{S,h}$ is an element of the group ring $\mathbb{Z}G_{p^h}$. If we replace an $x \in S$ by another element ux in its G-orbit, i.e., change one row and one column of $M_{S,h}$ by the factor $u \in R_m^{\times}$, the determinant changes by the factor u^2. Therefore the class $[D_{r,h}] = D_{S,h}G_{p^h}$ depends only on h and the rank r of A.

Though tedious, these definitions are, so far, internal to the world of finite free R_m-modules.

4.2. Cyclogenic functors

Now consider the p-group $J = G(1) \subset G$ generated by the automorphism $x \mapsto x^{1+p}$, and look at the ring $\Lambda = \mathbb{Z}[p^{-1}]$. The idempotents $e_1, \ldots, e_m$ which split $\mathbb{Q}J$ into simple components all lie in ΛJ and therefore produce a canonical decomposition $X_1 \oplus \cdots \oplus X_m$ of any ΛJ-module X. Each e_h corresponds to a certain G-orbit of characters $\chi : J \longrightarrow \mathbb{C}^{\times}$, namely the ones with conductor $G(h)$. The

fixed module $X^{G(h)}$ always equals $X_1 \oplus \cdots \oplus X_h$, and each X_h is a natural module for $G/G(h) = G_{p^h}$.

In particular, let $\tilde{V} = \Lambda \otimes V$ be the Λ-extension of an admissible $\mathbb{Z}$-lattice functor. Then $\tilde{V}$ splits functorially: $\tilde{V} = \tilde{V}_1 \oplus \cdots \oplus \tilde{V}_m$. Moreover, $\tilde{V}$ is an admissible Λ-lattice functor *, and consequently

$$\tilde{V}_h(F_k) = \begin{cases} \tilde{V}_h(F_h) & \text{if } h \le k; \\ 0 & \text{otherwise.} \end{cases} \tag{4.7}$$

For $h \le k < l \le m$, the maps $\tilde{V}_h(\iota_{k,l})$ are canonical ΛG_{p^h}-module isomorphisms.

Lemma 4.5. *An admissible $\mathbb{Z}$-lattice functor on $\mathcal{C}_{p^m}$ is cyclogenic for $A = R_m^r$ if and only if the determinant class $[D_{r,h}] \subset \mathbb{Z}G_{p^h}$ acts invertibly on $\tilde{V}_h(F_h)$, for all $h = 1, \ldots, m$.*

Proof. The beginning of the proof follows Section 2 of [H4]. We first need to describe the Wedderburn decomposition of $\mathbb{Q}A$ more closely than "up to isomorphism". Any functional $f : A \to R_m$ yields a $\mathbb{Q}$-algebra homomorphism $\mathbb{Q}A \to F_{l(f)}$ by $a \mapsto \varepsilon_m^{f(a)}$, and every G-orbit in $\mathrm{Hom}(A, R_m)$ constitutes a set of $\mathbb{Q}$-isomorphic irreducible representations. Choosing a set $T \subset \mathrm{Hom}(A, R_m)$ of representatives of G-orbits, we get an algebra isomorphism

$$\mathbb{Q}A \longrightarrow \prod_{f \in T} F_{l(f)} \quad \text{by} \quad a \mapsto (\ldots, \varepsilon_m^{f(a)}, \ldots)\,. \tag{4.8}$$

This is the Wedderburn isomorphism *with respect to* T. However, in case $A = C_x$ is cyclic with a chosen generator x, the standard isomorphism is induced by the map $x \mapsto (\ldots, \varepsilon_k, \ldots)$, with $0 \le k \le l(x)$. The question is how to describe the natural inclusion $\mathbb{Q}C_x \longrightarrow \mathbb{Q}A$ in terms of these two decompositions. Indeed, for a single $f \in T$, the map from $\mathbb{Q}C_x \simeq \prod_k F_k$ to the f-component of the decomposition (4.8) has three has three stages:

$$\prod_{k \le l(x)} F_k \longrightarrow F_{l'} \longrightarrow F_{l'} \longrightarrow F_{l(f)}\,. \tag{4.9}$$

The first of these is just the projection onto the l'-th component, where $l' = l(f(x))$, the second is the automorphism $\varepsilon_{l'} \mapsto \varepsilon_m^{f(x)}$, and the third is *the* inclusion given by $\varepsilon_{l'} \mapsto \varepsilon_{l(f)}$.

Since we have assumed that $A = R_m^r$, any $f : A \to R_m$ can be obtained in the form $y^* : x \mapsto x \cdot y$, so that the same set S of representatives of G-orbits in A can serve to index the cyclic subgroups $C_x \subset A$ as well as the simple components of $\mathbb{Q}A$, i.e., play the role of T as described above. Applying $\tilde{V}_h$, we now have the

---

* If X is a $\mathbb{Z}$-lattice, $\Lambda \otimes X$ is the union of all $p^{-\nu}X$. Hence, for any group Γ acting on X, the fixed set $(\Lambda \otimes X)^\Gamma$ is the union of $p^{-\nu}X^\Gamma$.

commutative square

$$\begin{array}{ccc} \prod_{x\in S}\tilde{V}_h(\ \mathbb{Q}C_x) & \xrightarrow{\sim} & \prod_{x\in S}\prod_{k\le l(x)}\tilde{V}_h(F_k) \\ \mu\downarrow & & \downarrow\mu' \\ \tilde{V}_h(\ \mathbb{Q}A) & \xrightarrow{\sim} & \prod_{y\in S}\tilde{V}_h(F_{l(y)}) \end{array} \tag{4.10}$$

whose horizontal arrows are ΛG_{p^h}-isomorphisms. The question is whether the two verticals are surjective (remember that p is invertible in Λ). Of course, we shall concentrate on μ'.

Since $\tilde{V}_h(F_k) = 0$ for $k < h$, the index set for x and y can be cut down to S_h without changing anything. The other components appearing in source and target of μ' are all canonically isomorphic to the module $\tilde{V}_h(F_h)$. The typical argument of μ' is a double array $(a_{x,k})$ with $x \in S_h$ and $h \le k \le l(x)$, and its image is a single array (b_y) with $y \in S_h$; all the entries $a_{x,k}$ and b_y are from $\tilde{V}_h(F_h)$. By (4.9), we have

$$b_y = \sum_{x\in S_h} u(x\cdot y)\, a_{x,l(x\cdot y)}\,, \tag{4.11}$$

because $\varepsilon_m^{x\cdot y} = \varepsilon_{l'}^{u(x\cdot y)}$ when $l' = l(x\cdot y)$, it being understood that $a_{x,k} = 0$ for $k < 0$. Surjectivity of μ' means that every array (b_y) with $y \in S_h$ can be obtained in this manner.

The "if" part of the lemma is now easy. In fact, the invertibilty of $D_{S,h}$ on $\tilde{V}_h(F_h)$ says precisely that the equation

$$b_y = \sum_{x\in S_h} u_h(x\cdot y)\, a_x \tag{4.12}$$

is always solvable for the single array a_x with $x \in S_h$. To solve (4.11), we simply set $a_{x,k} = 0$ for $k > h$, and $a_{x,h} = a_x$.

For the converse, we need to show that any equation of the form (4.11) can be recast to look like (4.12), so that if the former is always solvable, then $D_{S,h}$ must act invertibly. Given a double array $(a_{x,k})$ as above, we now create the single array

$$a_z = \sum_{cx=z} u(c)^{-1} a_{x,h+v(c)} \tag{4.13}$$

with $x, z \in S_h$ and suitable $c \in R_m$. Actually the sum extends over the set $S_z = \{x \in S \mid z \in C_x\}$. For each $x \in S_z$, there is a unique $c_{x,z} \in R_{l(x)}$ such that $c_{x,z}x = z$. For the sake of clarity, we have omitted these subscripts in the formula and lifted each c arbitrarily to R_m. Note that there is no reference to y in these prescriptions.

The proof will be finished if we can show that the substitution of (4.13) in (4.12) produces exactly (4.11). The relevant calculation depends, of course, on the formulas

$$u(cx\cdot y) = u(c)u(x\cdot y) \quad\text{and}\quad l(x\cdot y) = l(cx\cdot y) + v(c), \tag{4.14}$$

which are valid as long as $cx \cdot y \neq 0$. But it hinges even more delicately on an exact description of sets of x and z which can contribute non-trivial summands, and these sets do depend on the particular y involved !

Consider the sets $S_h(y) = \{x \in S \mid l(x \cdot y) \geq h\}$, $S_h^\circ(y) = \{x \in S \mid l(x \cdot y) = h\}$: they are the actual index sets for the sums in (4.11) and (4.12), respectively. Fixing $y \in S_h$, we record the sum (4.12), but with the summation index z restricted to $S_h^\circ(y)$ — which allows us to write $u(z \cdot y)$ instead of $u_h(z \cdot y)$ — and with a_z as given in (4.13). We get

$$\sum_{z \in S_h^\circ(y)} u(z \cdot y) \sum_{cx=z} u(c)^{-1} a_{x,h+v(c)} = \sum_{z \in S_h^\circ(y)} \sum_{cx=z} u(x \cdot y)\, a_{x,h+v(c)} \tag{4.15}$$

by using the first part of (4.14). Now remember that $l(z \cdot y) = h$ for all $z \in S_h^\circ(y)$, so that $cx = z$ implies $h + v(c) = l(x \cdot y)$. Recalling further that the summation "$cx = z$" really stands for "$x \in S_z$", we finally obtain

$$\sum_{z \in S_h^\circ(y)} \sum_{x \in S_z} u(x \cdot y)\, a_{x,l(x \cdot y)}\,, \tag{4.16}$$

which is the same as (4.11) because $S_h(y)$ is the disjoint union of the sets S_z as z ranges over $S_h^\circ(y)$. □

Corollary 4.6. *Suppose that two admissible $\mathbb{Z}$-lattice functors V and V' are such that $\mathbb{Q} \otimes V = \mathbb{Q} \otimes V'$. Then V is cyclogenic if and only V' is.*

Proof. With $\Lambda = \mathbb{Z}[p^{-1}]$, let X and X' be Λ-lattices such that $\mathbb{Q} \otimes X = \mathbb{Q} \otimes X'$, and consider a linear endomorphism L of $\mathbb{Q} \otimes X$ which maps X into X and X' into X'. Then $d = \det L$ is certainly in Λ. Now, L acts invertibly on $X \iff d$ is a unit in $\Lambda \iff L$ acts invertibly on X'.

The corollary results from applying this to $X = \tilde{V}_h(F_h)$, $X' = \tilde{V}'_h(F_h)$, and $L = D_{S,h}$. □

Conclusion. There are now several ways of finishing the proof of Proposition 4.1:

1. One could invoke the "Main Lemma" of [H4], according to which $|\chi(D_{S,h})|^2$ is a p-power for all characters $\chi : G \to \mathbb{C}^\times$ of conductor $G(h)$. This involves an eigenvalue calculation which is unpleasantly lengthy and convoluted — except in the simplest case $m = 1$ treated in [HSW].

2. A less direct but more conceptual way would use Corollary 4.6, with $V'(F_m)$ given by $\dot{\mathcal{U}}(\varepsilon_m)$, the group of *all* units (modulo torsion), in which $\dot{\mathcal{E}}^\oplus(\varepsilon_m)$ has finite index. By K-theory this V' is well known to be cyclogenic — cf. [B2], Chapter XI, Theorem 7.1 (c).

3. A possible third way would also use Corollary 4.6 (or a variant) with a V' for which the cyclogenic property is easy to prove, say, something made from the *additive* groups of the $\mathbb{Z}[\varepsilon_k]$. This remains to be explored.

5. Local units and logarithms

This section will summarize the papers [HR1] and [H3] in such a way as to include the case $p = 2$. For a quick idea of its content, the reader might want to skip the first three lemmas and have a peek at the second half, which deals with group rings over the p-adic integers $\mathbb{Z}_p$. In the first half, however, we have to establish some preliminaries which are just as true when the coefficient ring of the underlying group rings is $\mathbb{Z}$ and will therefore be discussed in that setting. They carry over *verbatim* to $\mathbb{Z}_p$.

5.1. Polarized bases

Let $K \subseteq A$ be finite abelian groups and put $B = A/K$. Working within $\mathbb{Z}A$, define

$$\Delta(A,K) = \ker\big[\Delta(A) \to \Delta(B)\big] \quad \text{and} \quad \Delta^\sharp(A,K) = \Delta(A)\Delta(A,K)\,. \tag{5.1}$$

For the moment, we are interested in the modules $\Delta^\sharp(A,K)$ and $\Delta^\sharp(A,K) \cap \Delta^+(A)$.

Lemma 5.1.

$$\Delta^\sharp(A,K) = \ker\big[\Delta^2(A) \to \Delta^2(B)\big]\,.$$

Proof. A standard basis of $\Delta(A,K)$ consists of all elements of the form $b(a-1) = (b-1)(a-1) + (a-1)$ with $a \in K$ and b from a system of representatives of A modulo K. Therefore $\Delta(A,K) = \Delta(A)\Delta(K) + \Delta(K)$ and $\Delta^\sharp(A,K) = \Delta(A)\Delta(K)$, in other words: $\Delta^\sharp(A,K) + \Delta(K) = \Delta(A,K)$. It follows that the first of the two homomorphisms

$$\frac{\Delta(K)}{\Delta^2(K)} \longrightarrow \frac{\Delta(A,K)}{\Delta^\sharp(A,K)} \longrightarrow \frac{\Delta(A,K)}{\Delta^2(A) \cap \Delta(A,K)} \tag{5.2}$$

is surjective, and evidently so is the second. On the other hand, the two end-terms of (5.2) are isomorphic to K: the first by canonical lore, the second by the exactness of the sequence

$$0 \longrightarrow \Delta^2(A) \cap \Delta(A,K) \longrightarrow \Delta(A,K) \xrightarrow{e} K \longrightarrow 0\,, \tag{5.3}$$

which is clearly the kernel of an epimorphism of short exact sequences, namely

$$\begin{array}{ccccccccc} 0 & \longrightarrow & \Delta^2(A) & \longrightarrow & \Delta(A) & \xrightarrow{e} & A & \longrightarrow & 0 \\ & & \downarrow & & \downarrow & & \downarrow & & \\ 0 & \longrightarrow & \Delta^2(B) & \longrightarrow & \Delta(B) & \xrightarrow{e} & B & \longrightarrow & 0\,, \end{array} \tag{5.4}$$

with $e : \Delta(A) \to A$ denoting the standard map (2.8). Consequently, the two maps of (5.2) are isomorphisms, whence

$$\Delta^2(A) \cap \Delta(A,K) = \Delta^\sharp(A,K)\,, \tag{5.5}$$

which is just what the lemma claims. □

Our next concern is to construct bases for certain submodules of $\Delta(A,K)$, tuned to the action of a given automorphism group $\Gamma \subseteq G$. Recalling that any full set V of representatives of A modulo K gives rise to a basis

$$\mathcal{B}(V) = \{b(a-1) \mid b \in V, 1 \neq a \in K\} \tag{5.6}$$

of $\Delta(A,K)$, we shall first concentrate on the shape of V with respect to the Γ-action.

For brevity, $b \in A$ will be called *naughty*, if $b^\sigma = ba$ for some $\sigma \in \Gamma$ and $1 \neq a \in K$, i.e. if the stabilizer Γ_{bK} of the coset bK is larger than the stabilizer Γ_b of b. The coset bK itself will be deemed naughty, if all its elements are. Clearly, this property (of elements as well as cosets) is inherited by Γ-conjugates and inverses. If b is *not* naughty, no two distinct conjugates of b lie in the same coset modulo K, and therefore the entire Γ-orbit of b can be incorporated into a system V of coset representatives. If this is done wherever possible, V becomes a disjoint union $V_1 \dot\cup V_2$, with V_1 forming a Γ-set, and all $b \in V_2$ belonging to naughty cosets. Such a V will be called Γ-*polarized*.

In particular, we can polarize V with respect to the involution $\star : b \mapsto b^{-1}$. For this special case, we write $V = V' \cup V''$, where $b \in V'$ means $b^{-1} \in V'$, and $b \in V''$ implies that $b^2 = a \in K$ with $a \neq 1$ of 2-power order. Indeed, if b is $\star$-naughty, i.e., if $b^{-1} = ba$ with $1 \neq a \in K$, we can put $a = c^2 a'$, where $a' \in K$ has 2-power order, and replace the representative b by bc. If $V = V_1 \cup V_2$ is already polarized with repect to some Γ, we can make these adjustments inside each V_i, and get the decomposition

$$V = V_1' \cup V_2' \cup V_1'' \cup V_2'' \,, \tag{5.7}$$

where $b \in V_1'$ implies $b^{\pm\sigma} \in V_1'$ for all $\sigma \in \Gamma$; $b \in V_2'$ means $b^{-1} \in V_2'$ but b is Γ-naughty; and so on. Some of these components may be empty: if $|K|$ is odd, V'' is empty; if Γ is trivial, V_2 is empty; if Γ includes the $\star$-involution, V_1'' is empty, etc.

Lemma 5.2. *Let the subgroup $\Gamma \subseteq G$ act trivially on the subgroup $K \subseteq A$ of prime order p. Then $\Delta^\sharp(A,K) \cap \Delta^+(A) = \Delta^+(A,K) \cap \Delta^2(A)$ has a basis $\mathcal{B} = \mathcal{B}_1 \cup \mathcal{B}_2$ with the following properties:*
(i) *every element of $\mathcal{B}$ lies in $\Delta^\sharp(S,K)$ for some subgroup $S = \langle b\rangle K$ with $b \in A$;*
(ii) *$\mathcal{B}_1$ is invariant under Γ, and all elements of $\mathcal{B}_2$ have Γ-trace zero.*

Proof. First we take $V = V' \cup V''$ to be $\star$-polarized and go after a basis of $\Delta^+(A,K)$. Under the present hypotheses, $b \in V''$ means that $b^2 = a$ with $\langle a\rangle = K$ and $a^2 = 1$. For any $\beta = b(a-1)$ with $b \in V$ and $a \in K$, we therefore have: either $b \in V'$ and $\beta, \beta^\star \in \mathcal{B}(V)$, or $b \in V''$ and $\beta^\star = ba(a-1) = -\beta$. Obviously, if $\delta = \sum n_\beta \beta \in \Delta(A,K)$ is $\star$-symmetric, the latter kind of β must have $n_\beta = 0$ and the former kind must satisfy $n_\beta = n_{\beta^\star}$. Hence $\delta = \delta^\star$ implies

$$\delta = \sum_{\beta \neq \beta^\star} n_\beta \, (\beta + \beta^\star) + \sum_{\beta = \beta^\star} n_\beta \, \beta \,. \tag{5.8}$$

Conclusion: $\Delta^+(A,K)$ *has the basis* $\{\beta+\beta^\star \mid \beta \neq \beta^\star\} \cup \{\beta \mid \beta = \beta^\star\}$, *where* $\beta = b(a-1)$ *with* $b \in V'$ *and* $a \in K$. Note: $\beta = \beta^\star$ means $a^2 = b^2 = 1$ and occurs only if $p = 2$. Let us agree to choose $V' \cap K \neq \{1\}$ if $p = 2$.

Turning to $\Delta^+(A,K) \cap \Delta^2(A)$, consider an element δ as in (5.8) and note that its first summand lies in $\Delta^2(A)$ because

$$\beta + \beta^\star = (b-1)(a-1) + (b^{-1}-1)(a^{-1}-1) - (a-1)(a^{-1}-1)\,. \tag{5.9}$$

The second term in (5.8) (zero unless $p = 2$) is a linear combination of $\beta = b(a-1) = (b-1)(a-1) + (a-1)$, with $b \in V'$, and lies in $\Delta^2(A)$ if and only if it can be rewritten as a linear combination of $(b-1)(a-1)$ with the same b's (and $b = a$ allowed). This yields the following basis $\mathcal{B}$ for $\Delta^+(A,K) \cap \Delta^2(A)$:

$$\mathcal{B} = \{\beta+\beta^\star \mid \beta = b(a-1), \beta \neq \beta^\star\} \cup \{(b-1)(a-1) \mid b^2 = a^2 = 1\} \tag{5.10}$$

with $b \in V'$ and $1 \neq a \in K$. Now let V be completely polarized as in (5.7), so that $V' = V_1' \cup V_2'$, and define $\mathcal{B}_i$ to be that part of $\mathcal{B}$ for which $b \in V_i'$. Then $\mathcal{B}_1$ is a Γ-set, which contains the (G-fixed) second term of (5.10) if $p = 2$. Thus, every element of $\mathcal{B}_2$ is of the form $\beta + \beta^\star$ with $\beta = b(a-1)$ and $b \in V_2'$ naughty. Such a β has zero Γ-trace. Indeed, since Γ acts trivially on K, the map $\varphi_b : \Gamma_{bK} \to K$ given by $\sigma \mapsto b^{\sigma-1}$ is a homomorphism; since $|K| = p$, it is surjctive. Therefore $a \in K$ implies $ba = b^\sigma$ and $\beta = b^\sigma - b$, for suitable $\sigma \in \Gamma$. □

Notation: We shall write $\Delta_*(A) = \Delta^2(A) \cap \Delta^+(A)$. The kernel $\Delta_*(A,K)$ of the map $\Delta_*(A) \to \Delta_*(B)$ thus equals $\Delta^\sharp(A,K) \cap \Delta^+(A) = \Delta^+(A,K) \cap \Delta^2(A)$.

Note: If the group order $|A|$ is odd, a basis of $\Delta^+(A)$ is given by the elements $(1-a)+(1-a^{-1}) = (1-a)(1-a^{-1})$. Therefore $\Delta^+(A) \subseteq \Delta^2(A)$, hence $\Delta_*(A) = \Delta^+(A)$, and $\Delta_*(A,K) = \Delta^+(A,K)$.

Lemma 5.3. *Let* Γ *and* K *be as in Lemma 5.2. If* $\mathcal{F}$ *denotes the family of all subgroups of the form* $S = \langle b\rangle K$ *with* $b \in A$, *we have natural surjections*

$$\prod_{S\in\mathcal{F}} \Delta_*(S,K) \longrightarrow \Delta_*(A,K) \quad \text{and} \quad \prod_{S\in\mathcal{F}} \ker{}_\Gamma\, \Delta_*(S,K) \longrightarrow \ker{}_\Gamma\, \Delta_*(A,K)\,,$$

where $\ker_\Gamma$ *stands for the kernel of the* Γ*-trace.*

Proof. The first of these is obvious from item (i) of Lemma 5.2. Now let $\mathcal{B} = \mathcal{B}_1 \cup \mathcal{B}_2$ be as in Lemma 5.2, and suppose that $\delta = \sum n_\alpha \alpha \in \Delta_*(A,K)$ with $\alpha \in \mathcal{B}$ has zero Γ-trace. Then $\delta = \delta_1 + \delta_2$ according to the partition of $\mathcal{B}$, and δ_2 is already in the image of the second map displayed above. Moreover,

$$\delta_1 = \sum_{\alpha\in\mathcal{B}_1} n_\alpha \alpha = \sum_T \sum_{\alpha\in T} n_\alpha \alpha = \sum_T \delta_T\,, \tag{5.11}$$

where T runs over the distinct Γ-orbits of $\mathcal{B}_1$, also has zero Γ-trace. Since the Γ-trace of each δ_T is an integer multiple of δ_T, it must be zero. On the other hand, since every $S = \langle b\rangle K$ is Γ-invariant, $\alpha \in \Delta(S)$ clearly implies $\delta_T \in \Delta(S)$ for the orbit T of α. □

5.2. Logarithms and applications

For the rest of this section, we let A be a p-group, and take the p-adic integers $\mathbb{Z}_p$ as our coefficient ring. However, for the sake of simplicity, we shall keep $\mathbb{Z}_p$ out of the notation except in formal statements of results.

Note that the preceding lemmas remain true when read over $\mathbb{Z}_p$. The first new item on the p-adic agenda concerns the unit group $\mathcal{U}^\sharp(A,A') = 1 + \Delta^\sharp(A,A')$.

Proposition 5.4. *For every subgroup $A' \subseteq A_p$, the logarithm*

$$\log : \mathcal{U}^\sharp\mathbb{Z}_p(A,A') \to \Delta^\sharp\mathbb{Z}_p(A,A')\,,$$

defined by the usual power-series, is an isomorphism of G-modules.

To appreciate the need for this, let us remind ourselves that the exp-series does not converge as easily as one would wish, and that the log-series does not always yield a homomorphism on its entire domain of convergence. We shall proceed inductively and by small steps, repeatedly using the diagram

$$\begin{array}{ccccccccc} 1 & \longrightarrow & \mathcal{U}^\sharp(A,K) & \longrightarrow & \mathcal{U}^\sharp(A,A') & \longrightarrow & \mathcal{U}^\sharp(B,B') & \longrightarrow & 1 \\ & & \downarrow & & \downarrow & & \downarrow & & \\ 0 & \longrightarrow & \Delta^\sharp(A,K) & \longrightarrow & \Delta^\sharp(A,A') & \longrightarrow & \Delta^\sharp(B,B') & \longrightarrow & 0\,, \end{array} \tag{5.12}$$

with $K \subseteq A' \subseteq A_p$. Its second row is exact by Lemma 5.1 restricted to the subgroup $\Delta^\sharp(A,A')$ of $\Delta^2(A)$, and the first row tags along because $\mathcal{U}^\sharp(A,A') = 1+\Delta^\sharp(A,A')$ and so on.

Proof of the proposition. The following statement summarizes the results of the first section of [HR1], whose arguments extend (almost *verbatim*) to the case $p = 2$.

The map $\log : \mathcal{U}^\sharp(A,A_p) \to \Delta^\sharp(A,A_p)$ *is an injective homomorphism of G-modules; it is bijective for cyclic A.*

It therefore induces injections $\mathcal{U}^\sharp(A,A') \to \Delta^\sharp(A,A')$ for all $A' \subseteq A_p$. In particular, (5.12) is a monomorphism of short exact sequences, and the surjectivity of the second vertical arrow implies that of the first one. This means that the A' occurring in the proposition can always be shrunk.

We shall prove the surjectivity of $\log : \mathcal{U}^\sharp(A,A_p) \to \Delta^\sharp(A,A_p)$ in three stages.

Stage 1: First, let $A = \langle a,b\rangle$ with $|A| = p^2$. Then $A_p = A$ and $\Delta^\sharp(A,A_p) = \Delta^2(A)$. Letting $K = \langle a\rangle$ and $A' = A$ in diagram (5.12), and noting that $B' = B$ is cyclic, we are reduced to showing the surjectivity of the left vertical arrow. This is where exponentials come in: since $t \in \Delta^\sharp(A,K)$ implies $t = \delta(a-1)$ with $\delta \in \Delta(A)$, it follows as in the proof of Lemma 2 of [HS2] that $\mathrm{ord}_p(t^p) \geq 2$, whence $\exp(t) = 1 + \sum t^k/k!$ lies in $\mathbb{Z}_p(A)$, and evidently even in $\mathcal{U}^\sharp(A,K)$. The fact that $t = \log(\exp(t))$ is a formality which is easily transplanted to group rings.

Stage 2: Next, let $A = \langle a,b\rangle$ be non-cylic with $a^p = 1$ and b of order $p^m > p$. Putting $K = A^q$, with $q = p^{m-1}$, we have $K = \langle b^q\rangle = L_p$ for *any* cyclic subgroup $L \subset A$ of order $> p$, and hence the bottom horizontal arrow in the commutative

square

$$\begin{array}{ccc} \mathcal{U}^\sharp(A_p,K)\times\prod_L \mathcal{U}^\sharp(L,L_p) & \longrightarrow & \mathcal{U}^\sharp(A,K) \\ \downarrow & & \downarrow \\ \Delta^\sharp(A_p,K)\times\prod_L \Delta^\sharp(L,L_p) & \longrightarrow & \Delta^\sharp(A,K) \end{array} \tag{5.13}$$

is surjective (cf. Lemma 3.2 of [HR1]), the verticals again being logarithms. The left vertical is bijective by Stage 1 and the cyclic result quoted earlier; hence so is the right vertical. Again turning to diagram (5.12), with $A' = A_p$ — hence $B = A/K$ and $B' = A_p/K = \langle a\rangle$ — we may assume by induction that $\log : \mathcal{U}^\sharp(B,B') \to \Delta^\sharp(B,B')$ is surjective. By (5.13) so is $\log : \mathcal{U}^\sharp(A,K) \to \Delta^\sharp(A,K)$ and we are done.

Stage 3: In the general case, every generator $(b-1)(a-1)$ of $\Delta^\sharp(A,A_p)$ lies in $\Delta^\sharp(S,S_p)$ for some subgroup $S = \langle a,b\rangle$ of the type considered above. Therefore the bottom arrow of the diagram

$$\begin{array}{ccc} \prod_S \mathcal{U}^\sharp(S,S_p) & \longrightarrow & \mathcal{U}^\sharp(A,A_p) \\ \downarrow & & \downarrow \\ \prod_S \Delta^\sharp(S,S_p) & \longrightarrow & \Delta^\sharp(A,A_p) \end{array} \tag{5.14}$$

is surjective, and so (as shown above) is the left vertial. It follows that right vertical is surjective, too. □

Remark. By an easy induction, it follows that $\mathcal{U}_2\mathbb{Z}_pA = 1 + \Delta^2\mathbb{Z}_pA$ is torsion-free, just like its global counterpart.

In the sequel, we shall be mainly interested in $\Delta_* = \Delta^2 \cap \Delta^+$ and $\mathcal{U}_2^+ = 1+\Delta_*$, as well as in the kernels $\acute{\Delta}_*$ and $\acute{\mathcal{U}}_2^+$ of the H-trace and H-norm, respectively. Restricted to $\mathcal{U}^+$, the proposition clearly yields an H-isomorphism

$$\mathcal{U}_2^+\mathbb{Z}_p(A,A_p) \xrightarrow{\sim} \Delta_*\mathbb{Z}_p(A,A_p)\,, \tag{5.15}$$

which maps $\acute{\mathcal{U}}_2^+\mathbb{Z}_p(A,A_p)$ onto $\acute{\Delta}_*\mathbb{Z}_p(A,A_p)$.

Proposition 5.5. *As C runs over all cyclic subgroups of A, we obtain a natural surjection*

$$\prod_C \acute{\mathcal{U}}_2^+\mathbb{Z}_pC \longrightarrow \acute{\mathcal{U}}_2^+\mathbb{Z}_pA\,.$$

Again we proceed by induction and hide $\mathbb{Z}_p$ in the notation. Abbreviating $\mathcal{U}_2^+$ by $\mathcal{U}_*$, we now use the diagram

$$\begin{array}{ccccccccc} & & \prod_S \acute{\mathcal{U}}_*(S,K) & \longrightarrow & \prod_S \acute{\mathcal{U}}_*(S) & \longrightarrow & \prod_S \acute{\mathcal{U}}_*(S/K) & \longrightarrow & 1 \\ & & \downarrow & & \downarrow & & \downarrow & & \\ 1 & \longrightarrow & \acute{\mathcal{U}}_*(A,K) & \longrightarrow & \acute{\mathcal{U}}_*(A) & \longrightarrow & \acute{\mathcal{U}}_*(A/K) & , & \end{array} \tag{5.16}$$

where S ranges over a family $\mathcal{F}$ of subgroups of A each containing the fixed subgroup $K \subseteq A_p$. K and $\mathcal{F}$ will have to chosen in such a way that (a) S/K is cyclic for all $S \in \mathcal{F}$, (b) the right vertical arrow of (5.16) is surjective by induction hypothesis, and (c) the map

$$\prod_{S\in\mathcal{F}} \acute{\Delta}_*(S,K) \longrightarrow \acute{\Delta}_*(A,K) \tag{5.17}$$

is surjective. By the logarithmic isomorphism (5.15), the latter conditon will make the left vertical of (5.16) surjective. Condition (a) ensures that both rows of (5.16) are exact. In fact, the only problem is the right exactness of the first row, but by Lemma 4 of [H3] — whose proof is easily adapted to include $p = 2$ — we know: *the map*

$$\acute{\mathcal{U}}_2^+\mathbb{Z}_pS \longrightarrow \acute{\mathcal{U}}_2^+\mathbb{Z}_p(S/K) \tag{5.18}$$

is surjective whenever S/K is cyclic. Altogether, then, Conditions (a) – (c) make the center arrow of (5.16) surjective.

The proof of the proposition itself is again in three steps.

Step 1: Let $A = \langle x, y\rangle$ with $|A| = p^2$, and take $\mathcal{F}$ to be the family of cyclic subgroups. For this preliminary step, we shall not use (5.16) but a more summary argument based on the isomorphism $\log : \acute{\mathcal{U}}_2^+(A) \xrightarrow{\sim} \acute{\Delta}_*(A)$ available in this case. For $p = 2$, these groups are trivial because of the trace condition (!), and there is nothing to show. For $p > 2$, however, $\Delta_*(A) = \Delta^+(A)$ has generators of the form $(z-1)+(z^{-1}-1)$, which are obviously available from cyclic subgroups. Therefore

$$\prod_{C\in\mathcal{F}} \Delta_*(C) \longrightarrow \Delta_*(A) \tag{5.19}$$

is surjective. By a rank count, it is even bijective: we have $(p+1)$ non-trivial cyclic subgroups C, and hence a module of rank $(p+1)(p-1)/2 = (p^2-1)/2$ on both sides. Clearly this continues to be an isomorphism when restricted to the kernel of the G-trace. In view of the log-isomorphism, this yields the result.

Step 2: Let $A = \langle x, y\rangle$ with $|A| = p^{m+1} > p^2$ and $x^p = 1$. This time $\mathcal{F}$ will consist of all "large" cyclic subgroups of $L \subset A$ such that $|L| > p$ together with the elementary abelian group $A_p = \langle x, y^q\rangle$. Every L is generated by an element $x^r y^s$, where $0 \le r \le p-1$ and $s = p^t$ with $0 \le t \le m-2$. We shall use (5.16) with $K = \langle y^q\rangle$.

Let us now worry about Conditions (a) – (c). The first of these is automatic by definition. For Condition (b), note that A/K is a smaller group of the same type or elementary abelian. Moreover, L/K runs over all cyclic subgroups of A/K,

except for $\langle x\rangle = A_p/K$, so that Condition (b) is the induction hypothesis on the theorem. The trickiest part is Condition (c), the surjectivity of

$$\acute{\Delta}_*(A_p, K) \times \prod_L \acute{\Delta}_*(L, K) \longrightarrow \acute{\Delta}_*(A, K)\,. \tag{5.20}$$

This comes from Lemma 5.3: because of our choice of K, every group $S = \langle b\rangle K \neq K$ occurring in that context is either an L or equals A_p, depending on whether b has order $> p$ or not. Lemma 5.3 thus yields the desired kind of surjection for Δ_* itself and for $\ker_\Gamma \Delta_*$, where Γ stands for the maximal p-subgroup of G (which acts trivially on K). For $p = 2$ we have $G = \Gamma$, and all is well. For $p > 2$ we have $G = \Gamma \times G'$, with G' of order $p-1$, and $\Gamma = G(1)$ in the notation of Section 4. We now use the known surjectivity for the analogues of (5.20) with Δ_* and $\ker_\Gamma \Delta_*$ in the place of $\acute{\Delta}_*$, and invoke Lemma 1 of [H3], to wit:

If an epimorphism $X \to Y$ of $\mathbb{Z}_pG$-modules remains surjective when restricted to $\ker_\Gamma X$, it will also remain so on $\ker_G X$. (This easily follows from decomposing X, Y with respect to the characters of the p'-subgroup $G' \subset G$).

Using the resulting surjectivity of the center arrow of (5.16) and applying Step 1 to A_p, we get what we want.

Step 3: For general A, we let $K = \langle x\rangle$ of order p, and take $\mathcal{F}$ to be the family of all subgroups $S = \langle x, y\rangle$ with $y \in A$. Conditions (a) and (b) are straightforward. Condition (c) is a bit smoother than above but follows the same pattern. To get the surjectivity (5.17), we appeal to Lemma 5.3, which yields it for Δ_* and $\ker_\Gamma \Delta_*$, where Γ is again the maximal p-subgroup of G. For $p > 2$, we must once more use Lemma 1 of [H3]. Applying Step 2 to each $S \in \mathcal{F}$, we are finished. □

Corollary 5.6. *If $A \to B$ is an epimorphism of finite p-groups, the induced map $\acute{\mathcal{U}}_2^+\mathbb{Z}_pA \to \acute{\mathcal{U}}_2^+\mathbb{Z}_pB$ is surjective.*

Proof. This follows at once from Proposition 5.5 and the surjectivity of the map (5.18) for cyclic groups $S/K \subseteq B$ and suitable pre-images $S \subseteq A$. □

Remark. For $p > 2$, the proof of Proposition 5.5 also works — in fact, becomes a lot easier — without the restriction to the kernel of the H-norm (which is the same as $\ker_G$ on $\mathcal{U}_2^+$). Hence the proposition and its corollary have valid non-accented counterparts; in particular

$$\prod_C \mathcal{U}_2^+\mathbb{Z}_pC \longrightarrow \mathcal{U}_2^+\mathbb{Z}_pA \tag{5.21}$$

is surjective for odd order A (of course $\mathcal{U}_2^+ = \mathcal{U}_1^+$ in that case). For $p = 2$, on the other hand, the map (5.21) is *not* surjective: the unit $1 + (x-1)(y-1)$ is not a product of "cyclically induced" units in $\mathcal{U}_2^+\mathbb{Z}_pA$, if $A = \langle x, y\rangle$ with $x \neq y$ and $x^2 = y^2 = 1$.

6. Regular primes

A prime p is said to be *regular*, if the class number h_p of the field of p-th roots of unity is not divisible by p. For abelian p-groups A, regularity of p will be seen to mean that the group $\mathcal{U}_1^{\oplus}\mathbb{Z}A$ makes up as much of the p-adic group $\mathcal{U}_1^{+}\mathbb{Z}_pA$ as it possibly could (cf. Corollary 6.4 below). This will allow us to exploit certain convenient properties of the p-adic environment (notably logarithms) and eventually prove that all circular units are constructible, i.e., $c(A) = 1$.

This is stated as Theorem 6.6, whose proof requires the main results of the last three sections as well two new ingredients: Corollary 6.4 and Proposition 6.5. For odd p, these can be found in [HS3] and [H5], respectively.

6.1. Arithmetical background

Let us take this opportunity to list the properties of class numbers $h(F)$ of number fields F which will be needed in the sequel. For a primitive n-th root of unity ζ_n, let h_n and h_n^+ denote the class numbers of $\mathbb{Q}(\zeta_n)$ and $\mathbb{Q}(\zeta_n + \zeta_n^{-1})$, respectively. Let p be a prime not necessarily related to n.

(i) p divides $h(F)$ if and only if F has an unramified Galois extension of degree p.
(ii) h_n factors as $h_n^- h_n^+$, and for $n = p^m$, the index $\left[\mathcal{U}^+(\zeta_n) : \mathcal{U}^{\oplus}(\zeta_n)\right]$ equals h_n^+.
(iii) h_p^- is divisible by p if and only if the Bernoulli numbers $B_2, \ldots, B_{p-3}$ (which lie in $\mathbb{Z}_p$) are prime to p.

The notion of regularity was introduced by Kummer [Ku] in his famous proof of Fermat's Last Theorem for regular prime exponents. He also gave the characterization of regularity in terms of Bernoulli numbers hinted at by (iii). We picked up only the h_p^- part of this characterization, since we shall have to revisit the rest of it, in Lemma 7.2 below, for our present purposes.

Item (ii) comes from the analytic class number formula $h_n = P_n/R_n$, where $R_n = R_n^+$ is the regulator of the unit group of $\mathbb{Z}[\zeta_n]$ (or that of $\mathbb{Z}[\zeta_n + \zeta_n^{-1}]$) and P_n is essentially the product of $L(1,\chi)$ for the characters $\chi \neq 1$ of G. Separating odd characters from even ones yields the factorization $h_n = h_n^-(P_n^+/R_n^+)$, whose second factor is just h_n^+. For even χ, however, $L(1,\chi)$ can be expressed by sums, over $\sigma \in G$, of terms involving $\log|\zeta^\sigma - 1|$ with suitable ζ (cf. [Wa], Theorem 4.9). This expression, which is also behind the fundamental injectivity (2.4), reveals that, for $n = p^m$, the product P_n^+ is just the regulator of the *cyclotomic* units (cf. [Wa], Theorem 8.2). For general n, Sinnott [Si] has shown the index of the cyclotomic units to equal $2^b h_n^+$, where b depends on the number of distinct prime divisors of n, and $b = 0$ if that number is ≤ 3.

Finally, (i) is immediate from one of the core results of class field theory: the isomorphism between the ideal class group of F and the Galois group of its maximal unramified abelian extension ("Hilbert class field"). It will be used in Lemma 6.1.

In view of item (ii) we are also interested in primes p such that h_p^+ is prime to p: they will be called *semi-regular*. It has been conjectured (by Kummer and later, independently, by Vandiver) that every prime has this property. Although h_p^+ is difficult to compute, this has been checked for $p < 50^3$.

Notation. If X is a finitely generated $\mathbb{Z}$-module, we shall use $\dot{X}$ to denote the maximal torsion-free factor module. Most of the time we shall be dealing with torsion of exponent ≤ 2, non-trivial only if $p = 2$ — much ado about (almost) nothing. Furthermore, we write $X \otimes \mathbb{Z}_p = \widehat{X}$ and $X \otimes \mathbb{F}_p = \overline{X}$, and use analogous notations for similarly adjusted homomorphisms.

As in the preceding section, if the group H acts on X, we shall denote by $\ker_H X$ the kernel of the H-trace (called H-norm in the multiplicative case). If $H = G/\langle\star\rangle$ with $G = (\mathbb{Z}/n\mathbb{Z})^\times$ for some fixed n, we abbreviate $\ker_H X = \acute{X}$. As long as we are dealing with torsion-free H-modules, there is, of course, no difference between $\ker_G$ and $\ker_H$.

Our first aim is to extend the primeness of the class number from h_p to all h_{p^m}. This easily done by (i) and the following elegant argument of Iwasawa [Iw].

Lemma 6.1. *Let E/F be a cyclic number field extension of degree p, such that a single prime divisor v of F ramifies in E and is totally ramified. Then E has an unramified Galois extension of degree p if and only if F does.*

Proof. Let L'/E be an unramified Galois extension of degree p. Working in its Galois closure M over F, which is still unramified over E and of p-power degree, it is easy to see (since the commutator group of $\mathrm{Gal}(M/F)$ cannot have index p) that L'/E can be replaced by an unramified Galois extension L/E of degree p and such that L/F is abelian. Hence all prime divisors of v in L have the same inertia group $\Gamma \subset \mathrm{Gal}(L/F)$, and $|\Gamma| = [E : F]$. The fixed field of Γ is the desired unramified extension of F of degree p. The converse is obvious. □

Remark. By (i) it follows that $h(E)$ is divisible by p if and only if $h(F)$ is. Applied to $F = \mathbb{Q}(\zeta_{p^{m-1}})$ and $E = \mathbb{Q}(\zeta_{p^m})$, this shows that a regular prime p does not divide h_{p^m} for any m. Applied to the real subfields, it says that a semiregular prime p does not divide $h^+_{p^m}$ for any m. Note that $p = 2$ and $p = 3$ are allowed here.

Lemma 6.2. *If p is regular, the natural map $\overline{\mathcal{U}}\mathbb{Z}[\zeta_n] \to \overline{\mathcal{U}}\mathbb{Z}_p[\zeta_n]$ is injective for all $n = p^m > 1$.*

Proof. If $\varepsilon \in \mathcal{U}\mathbb{Z}[\zeta_n]$ is not a p-th power but becomes one in $\mathcal{U}\mathbb{Z}_p[\zeta_n]$, the polynomial $X^p - \varepsilon$ is irreducible in $\mathbb{Q}(\zeta_n)$ but splits completely in $\mathbb{Q}_p(\zeta_n)$. If $E = \mathbb{Q}(\zeta_n)$ and $L = E(\eta)$, where $\eta^p = \varepsilon$, the prime divisor of p in E splits completely in L. Since the different of L/E divides $p\eta^{p-1}$, no other finite prime of E can ramify in L. The infinite primes are already complex. Hence L/E is unramified, and p divides $h(E)$. □

6.2. Abelian p-groups

We now turn back to finite abelian p-groups A, keeping in mind that $\mathcal{E}(A)$ stands for the 1-units in the maximal order of $\mathbb{Q}A$ (cf. Section 4) and that $\mathcal{E}_p(A)$ denotes the analogous group in $\mathbb{Q}_pA$.

Proposition 6.3. *If p is regular, the natural map $\lambda : \widehat{\mathcal{E}}^{\oplus}\mathbb{Z}A \to \ker_G \mathcal{E}^+\mathbb{Z}_pA$ is an isomorphism for all for finite abelian p-groups A.*

Proof. It suffices to prove this for $\lambda_n : \widehat{\mathcal{E}}^{\oplus}\mathbb{Z}[\zeta_n] \to \ker_G \mathcal{E}^+\mathbb{Z}_p[\zeta_n]$. Note first that, while H-norms of $\mathcal{U}^+(\zeta_n)$ may be ± 1 (for $p = 2$), the G-norm is always 1. Abbreviating $\mathcal{E}\mathbb{Z}_p[\zeta_n]$ by $\mathcal{E}_p(\zeta)$, we have an injection $\overline{\mathcal{E}}(\zeta) \hookrightarrow \overline{\mathcal{E}}_p(\zeta)$ by Lemma 6.2, because $\mathcal{E}(\zeta)$ always has index $p-1$ in $\mathcal{U}(\zeta)$ and hence $\overline{\mathcal{E}}(\zeta) = \overline{\mathcal{U}}(\zeta)$.

If we now go from $\mathcal{E}$ to $\mathcal{E}^+$, i.e., restrict our attention to *real* units, we still have an injection. Indeed, for $p > 2$, even $\overline{\mathcal{E}}^+(\zeta) \longrightarrow \overline{\mathcal{E}}(\zeta)$ is injective: if $u = v^p$ with u real, then $v^\star = \varepsilon v$ with $\varepsilon^p = 1$ and also $\varepsilon^2 = 1$, so v must be real. For $p = 2$, however, we could have $v^\star = -v$, so that $-u = (iv)^2$ is a square of a real unit; but if such a u became a square in $\mathcal{E}_p^+(\zeta)$, say $u = w^2$, we would have the impossible equation $-1 = y^2$ with $y = iv/w \in \mathcal{E}_p^+(\zeta)$. Thus $\overline{\mathcal{E}}^+(\zeta) \hookrightarrow \overline{\mathcal{E}}_p^+(\zeta)$ is injective for all regular p.

Finally, since $[\mathcal{U}^+(\zeta) : \mathcal{U}^{\oplus}(\zeta)] = h_n^+$ by (ii), where n is the order of ζ, and since h_n^+ as a divisor of h_n is also prime to p, the groups $\overline{\mathcal{E}}^+(\zeta)$ and $\overline{\mathcal{E}}^{\oplus}(\zeta)$ coincide. All in all, we conclude that the reduction modulo p of the map λ_n is injective. But, except for the nuisance factor -1 on both sides for $p = 2$, source and target of λ_n are free $\mathbb{Z}_p$-modules of the same rank — the left one by Dirichlet's Unit Theorem, the right one by an analogous p-adic result (cf. [Ha], II.15.5). Hence their reductions modulo p have the same $\mathbb{F}_p$-dimension and are therefore isomorphic. By Nakayama's Lemma, λ_n is surjective.

For odd p, the aforementioned equality of $\mathbb{Z}_p$-ranks on both sides of λ_n, immediately implies the desired isomorphism. For $p = 2$, each of the groups mentioned in the proposition is a free module times the group $\{\pm 1\}$. In that case, too, the surjectivity of λ_n does the trick, but the argument is left to the reader. □

> For $p = 2$, we sometimes have to deal with maps $T \times V \longrightarrow T \times W$, where T is a group of order 2 and V, W are free modules over $\mathbb{Z}$ or $\mathbb{Z}_p$, and where T is mapped onto itself. This is not very different from a similar map $V \longrightarrow W$ without the T, and we shall not elaborate on the fastidious details, unless there is a real difficulty.

Corollary 6.4. *(Density Lemma) For any finite abelian p-group A and regular p, the natural inclusion $\widehat{\mathcal{U}}_2^{\oplus}\mathbb{Z}A \longrightarrow \acute{\mathcal{U}}_2^+\mathbb{Z}_pA$ is an isomorphism.*

Proof. The preceding result can be restated as saying that $\acute{\mathcal{E}}^{\oplus}(\zeta)$ is dense in the $\mathbb{Z}_p$-module $\acute{\mathcal{E}}_p^+(\zeta)$, the acute accent denoting the kernel of the H-norm. Indeed, if $\theta \in \mathcal{E}^{\oplus}(\zeta)$ has H-norm -1, it yields the disjoint unions $\mathcal{E}^{\oplus}(\zeta) = \acute{\mathcal{E}}^{\oplus}(\zeta) \cup \theta\acute{\mathcal{E}}^{\oplus}(\zeta)$

and $\ker_G \mathcal{E}_p^+(\zeta) = \acute{\mathcal{E}}_p^+(\zeta) \cup \theta\acute{\mathcal{E}}_p^+(\zeta)$. Since the first of these is dense in the second, the same is true for the individual (open) components.

A modified version of the pull-back (4.2), namely

$$\begin{array}{ccc} \mathcal{U}_2^{\oplus}(A) & \longrightarrow & \acute{\mathcal{U}}_2^+\mathbb{Z}_pA \\ \downarrow & & \downarrow \\ \acute{\mathcal{E}}^{\oplus}(A) & \longrightarrow & \acute{\mathcal{E}}_p^+(A) \end{array} \tag{6.1}$$

says that $\mathcal{U}_2^{\oplus}(A) = \acute{\mathcal{E}}^{\oplus}(A) \cap \acute{\mathcal{U}}_2^+\mathbb{Z}_pA$, the intersection taken inside $\acute{\mathcal{E}}_p^+(A)$. We know, however, that $\acute{\mathcal{E}}^{\oplus}(A)$ is dense in $\acute{\mathcal{E}}_p^+(A)$. Since $\acute{\mathcal{U}}_2^+\mathbb{Z}_pA$ is of finite index in $\acute{\mathcal{U}}_1^+\mathbb{Z}_pA$, hence open in $\acute{\mathcal{E}}_p^+(A)$, a simple argument of general topology shows that it contains the intersection $\mathcal{U}_2^{\oplus}(A)$ as a dense subset. In other words, $\widehat{\mathcal{U}}_2^{\oplus}(A)$ fills up all of $\acute{\mathcal{U}}_2^+\mathbb{Z}_pA$. □

Remark. For semi-regular p, we have the much weaker isomorphisms (equalities) $\widehat{\mathcal{E}}^{\oplus}(A) = \widehat{\mathcal{E}}^{+}(A)$ and $\widehat{\mathcal{U}}_2^{\oplus}(A) = \widehat{\mathcal{U}}_2^{+}(A)$. But these do not require the arguments of Lemma 6.2 or Proposition 6.3: the first follows simply from the fact that $h_n^+ = [\mathcal{U}^+(\zeta_n) : \mathcal{U}^{\oplus}(\zeta_n)]$ is prime to p, and the second follows from this as in the corollary.

> Actually, Proposition 5.5 reduces the Density Lemma to the cyclic case $A = C$. In that form, it could have been derived from the pull-back (3.4), according to which $\mathcal{U}_1^{\oplus}(C)$ is the kernel of a surjective "difference map" $\mathcal{U}_2^{\oplus}(C^p) \times \mathcal{E}^{\oplus}(\zeta) \to V$, where V is a suitable finite p-group. By mapping this arrangement into its p-adic counterpart, one can avoid an overtly toplogical argument by an appeal to the exactness of the "hat"-functor on finitely generated modules — cf. [HS3].

Our next proposition returns to the questions and the notation of Section 3. It says that $i(C) = 1$ in the regular case.

Proposition 6.5. *(Kummer's Lemma)* $\ker_p \mathcal{U}_2^{\oplus}(C) = \mathcal{U}_2^{\oplus}(C)^{\pi-p}$ *for any cyclic p-group C and regular p.*

Proof. By formula (3.9) and induction hypothesis, we may assume that $\mathcal{U}_2^{\oplus}(C^p) = \mathcal{Y}(C^p)$. Since $\pi : \mathcal{Y}(C) \longrightarrow \mathcal{Y}(C^p)$ is surjective, we obtain a short exact sequence

$$1 \longrightarrow \mathcal{U}_2^{\oplus}(C, C_p) \longrightarrow \mathcal{U}_2^{\oplus}(C) \xrightarrow{\pi} \mathcal{U}_2^{\oplus}(C^p) \longrightarrow 1 \tag{6.2}$$

in which $\mathcal{U}_2^{\oplus}(C, C_p)$ just denotes the appropriate kernel. By induction and a standard diagram chase, it suffices to show that any $u = 1 + p\delta \in \mathcal{U}_2^{\oplus}(C, C_p)$ is a p-th power in $\mathcal{U}_2^{\oplus}(C, C_p)$.

With u transferred to $\mathcal{U}_2^+\mathbb{Z}_p(C, C_p)$, the logarithmic isomorphism (5.15) yields $v \in \mathcal{U}_2^+\mathbb{Z}_p(C, C_p)$ such that $v^p = u$. Since the H-norm of u is 1, that of v must have order $\leq p$. But there is no torsion in $\mathcal{U}_2^+\mathbb{Z}_p(C, C_p) \simeq \Delta_*\mathbb{Z}_p(C, C_p)$, and hence v has G-norm 1.

Reducing the map shown in the Density Lemma modulo p-th powers, we get an isomorphism whose inverse takes the class (modulo p-th powers) of v into the class of some $w \in \mathcal{U}_2^+(C)$ with $w^p = u$. Now $u^\pi = 1$ implies $w^\pi = 1$, because $\mathcal{U}_2^+(C)$ certainly has no torsion either. Therefore w lies in the kernel $\mathcal{U}_2^+(C, C_p)$ of π, and since regularity makes h_n^+ prime to p, we have $w^r \in \mathcal{U}_2^\oplus(C, C_p)$ for some r prime to p. This means that u^r is a p-th power in $\mathcal{U}_2^\oplus(C, C_p)$, and hence so is u itself. □

If $p = 2$, there is an elementary argument in which $\mathbb{Z}_p$ is eschewed in favor of $\mathbb{F}_p$, and $\mathcal{U}_2^\oplus(C)$ is replaced by $\mathcal{Y}(C)$ with the help of Corollary 3.5. We are then reduced to showing that the kernel of $\rho : \mathcal{Y}(C, C_2) \longrightarrow \mathcal{U}_1^+\mathbb{F}_2(C, C_2)$ consists entirely of squares. On the elementary abelian 2-group $\mathcal{U}_1^+\mathbb{F}_2(C, C_2) = 1 + \Delta^+\mathbb{F}_2(C, C_2)$, we have the delightfully simple logarithm $\log(1 + \delta) = \delta$, which together with ρ induces a homomorphism

$$\frac{\mathcal{Y}(C, C_2)}{\mathcal{Y}(C, C_2)^2} \longrightarrow \frac{\Delta^+\mathbb{F}_2(C, C_2)}{\Delta^+\mathbb{F}_2 C_4},$$

for $n \geq 8$. To show inductively that this map is bijective, it suffices to establish the surjectivity of its relative

$$\frac{\mathcal{W}(C, C_2)}{\mathcal{W}(C, C_2)^2} \longrightarrow \frac{\Delta^+\mathbb{F}_2(C, C_2)}{\Delta^+\mathbb{F}_2(C^2, C_2)}.$$

This is done in [GH] by exhibiting a suitable $w_\alpha(x) \in \mathcal{W}(C, C_2)$ whose image is an $\mathbb{F}_2 H$-generator of the module on the right.

Remark. The original form of Kummer's Lemma concerns $\mathcal{U}(\zeta_p)$ and is equivalent to Proposition 6.5 for the case $|C| = p$, cf. [Ku], p.297. Our proof required the restriction to cyclic groups C only to get the right exactness of (6.2). This could have been obtained for general A by using the Density Lemma together with Corollary 5.6, proving that

$$\ker_p \mathcal{U}_2^\oplus(A) = \mathcal{U}_2^\oplus(A)^{\pi - p} \tag{6.3}$$

in general, as long as p is regular.

At long last, we are ready to answer Question (1) of the introduction.

Theorem 6.6. *$\mathcal{U}_2^\oplus(A) = \mathcal{Y}(A)$, for any finite abelian p-group A and regular p.*

Proof. For cyclic A, Kummer's Lemma together with formula (3.9) implies $c(A) = 1$, as claimed. For general A, the Density Lemma guarantees the vertical arrows in the commutative square

$$\begin{array}{ccc} \prod_C \widehat{\mathcal{U}}_2^\oplus(C) & \longrightarrow & \widehat{\mathcal{U}}_2^\oplus(A) \\ \downarrow & & \downarrow \\ \prod_C \acute{\mathcal{U}}_2^+\mathbb{Z}_p C & \longrightarrow & \acute{\mathcal{U}}_2^+\mathbb{Z}_p A \end{array} \tag{6.4}$$

to be isomorphisms (actually this is needed only on the left). Proposition 5.5 produces a surjection on the bottom horizontal, and hence we have one on the top as well. By the results of Section 4 — cf. especially formula (4.3) — the top horizontal map *without* the hats, namely

$$\mu^{\oplus} : \prod_{C \subseteq A} \mathcal{U}_2^{\oplus}(C) \longrightarrow \mathcal{U}_2^{\oplus}(A)\,, \tag{6.5}$$

has p-power index. Since tensoring with $\mathbb{Z}_p$ cannot hide a non-trivial p-cokernel, it follows that the map (6.5) is also surjective. In other words, every $u \in \mathcal{U}_2^{\oplus}(A)$ can be written as $u_1 \cdots u_t$, with $u_i \in \mathcal{U}_2^{\oplus}(K_i)$ for certain cyclic subgroups $K_1, \ldots, K_t$. Since $c(K_i) = 1$, every u_i is constructible, and therefore so is u. □

Example. Using the explicit formulas of Proposition 2.3, let us look at $\mathcal{U}_2^{\oplus}(A) = \mathcal{Y}(A)$ in case $A^n = \{1\}$ with $n = 2^m$. Choosing $\tau : x \mapsto x^3$ and $\beta = (\tau - 1)^2$, we can use the unit $w(x) = w_\beta(x^{\tau^{-1}})$ to generate $\mathcal{Y}(A)$. It turns out that $w(x) = (x^{-1} + 1 + x)s_b(x) - \kappa s_n(x)$, where $b - 1$ is the sum of all $2^{2k+1} < n$. This means: the set $\{w(z) \mid z \in A\}$ can be thinned out to a $\mathbb{Z}$-basis of $\mathcal{Y}(A)$ by omitting one element from each of its non-trivial $(\mathbb{Z}/n\mathbb{Z})^\times$-orbits. For $n = 128$ (with $b = 43$ and $\kappa = 1$), this actually yields all of $U_1^+(A) = U_1^{\oplus}(A)$ because $h_{128}^+ = 1$.

Remark. For semi-regular $p > 2$, the remark following the Density Lemma implies that the top horizontal arrow of (6.4) equals the map $\widehat{\mu}$ obtained by p-adic completion of the map μ displayed in (1.2). Since they are p-powers, the indices of the maps μ and $\mu^{\oplus}$ are therefore equal. The composite homomorphism

$$\prod_{C \subseteq A} \mathcal{Y}(C) \to \prod_{C \subseteq A} \mathcal{U}_1^{\oplus}(C) \to \mathcal{U}_1^{\oplus}(A)\,, \tag{6.6}$$

whose index obviously equal $c(A)$, shows that $\mathrm{ind}(\mu) \mid c(A)$ in this case, as claimed in the introduction.

7. Irregular primes

In this section, which is essentially an account of [H7], we shall see that $c(A) > 1$ whenever $|A| = p^m > p$ and p is irregular. By the remark following Lemma 2.1, it suffices to show this for $|A| = p^2$. So there are two cases: cyclic and elementary abelian.

7.1. A converse

As we want assurance that Kummer's Lemma fails for irregular p, we might as well take $p > 3$ and concentrate on a group K of order p. Since $\mathcal{U}_2^{\oplus}(K) = \mathcal{W}(K)$

in this case, Proposition 6.5 asserts the injectivity of the composite

$$\overline{\mathcal{W}}(K) \xrightarrow{\overline{\iota}} \overline{\mathcal{U}}_1^+(K) \xrightarrow{\overline{\rho}} \acute{\mathcal{U}}_1^+ \mathbb{F}_p K, \tag{7.1}$$

Since the group $G = \mathrm{Aut}(K)$ is cyclic of order $p-1$, both $\mathcal{W}(K)$ and $\mathcal{U}_1^+(K)$ have rank $(p-3)/2$. Since each of the $\mathbb{F}_p$-spaces in (7.1) has the same dimension $(p-3)/2$, injectivity and surjectivity of each of the maps $\overline{\iota}$, $\overline{\rho}$, or $\overline{\rho} \circ \overline{\iota}$ are logically equivalent.

This can be said more precisely in terms of the $\mathbb{F}_p G$-structure of the underlying spaces and of characters of G. Every homomorphism $G \longrightarrow \mathbb{F}_p^\times$ is of the form τ^d for suitable $1 \le d \le p-1$, where τ denotes the canonical identification of $G = \mathrm{Aut}(\mathbb{Z}/p\mathbb{Z})$ with $\mathbb{F}_p^\times$. Accordingly, every $\mathbb{F}_p G$-module V is a direct sum of *characteristic submodules* V_d, and every G-map $g : V \longrightarrow V'$ of such modules decomposes into "slices" $g_d : V_d \longrightarrow V'_d$. When G acts via $H = G/\{\pm 1\}$, only *even* characters are involved, that is, $d = 2k$ with $k = 1, \ldots, (p-3)/2$, the trivial character, $d = p-1$, being absent in the scenario (7.1).

Lemma 7.1. *Each of the three $\mathbb{F}_p G$-modules shown in (7.1) splits into $(p-3)/2$ distinct submodules of dimension 1. Thus, each of the maps $\overline{\iota}_{2k}$ and $\overline{\rho}_{2k}$, for $1 \le k \le (p-3)/2$, is either null or an isomorphism.*

Proof. We shall see that each of the modules is isomorphic to $\Delta \mathbb{F}_p H$. For the first one this follows from the fact that $\Delta(H) \simeq \Delta^2(H)$. For the third one, it is shown by the logarithmic isomorphism

$$\mathcal{U}_1 \mathbb{F}_p K = 1 + \Delta \mathbb{F}_p K \xrightarrow{\sim} \Delta \mathbb{F}_p K \tag{7.2}$$

available at characteristic p. In fact, if $K = \langle x \rangle$, the standard basis $\{x^\sigma - 1 \mid \sigma \in G\}$ of $\Delta \mathbb{F}_p K$ is clearly normal with respect to G, so that $\mathcal{U}_1 \mathbb{F}_p K$ is isomorphic to $\mathbb{F}_p G$. The restriction to G-norm 1 knocks out the G-invariant component and hence produces an isomorphism with $\Delta \mathbb{F}_p G$. It follows that $\mathcal{U}_1^+ \mathbb{F}_p K$ is isomorphic to $\Delta \mathbb{F}_p H$.

To the middle term of (7.1) we can apply the general argument, that, for any $\mathbb{Z}G$-module Y, the isomorphism type of $\widehat{Y}$ (and hence of $\overline{Y}$) is determined by that of $Y \otimes \mathbb{Q}_p$. Indeed, since $\mathbb{Z}_p G$ contains the minimal idempotents of $\mathbb{Q}_p G$, the module $\widehat{Y}$ splits into submodules of rank 1, each suffering the action of G via a specific character (τ^d followed by the natural inclusion $\mathbb{F}_p^\times \hookrightarrow \mathbb{Z}_p^\times$); the multiplicities of these characters can be read off from $\mathbb{Q}_p Y$.

Now, any injection $X \hookrightarrow Y$ between $\mathbb{Z}G$-modules of the same $\mathbb{Z}$-rank clearly induces a G-isomorphism $X \otimes F \xrightarrow{\sim} Y \otimes F$ for any field F of characteristic 0, e.g. $F = \mathbb{Q}_p$. In the present situation, we can take $X = \mathcal{W}(K)$, and $Y = \mathcal{U}_1^+(K)$. □

Remark. The surjectivity of $(\overline{\iota})_d$ is clearly equivalent to the vanishing of the d-th component of $\left[\mathcal{U}_1^+(K)/\mathcal{W}(K)\right] \otimes \mathbb{F}_p$. For this to happen at all d, it is necessary and sufficient that the order of $\mathcal{U}_1^+(K)/\mathcal{W}(K)$ be prime to p. By (ii), this means that h_p^+ is prime to p.

Lemma 7.2. *For a prime $p > 3$, and $2 \le d \le p-3$, the d-th slice of the composite $\overline{\rho} \circ \overline{\iota} : \overline{\mathcal{W}}(K) \longrightarrow \acute{\mathcal{U}}_1^+ \mathbb{F}_p K$, as shown in (7.1), is non-trivial if and only if the numerator of the Bernoulli number B_d is not divisble by p.*

Proof. By means of a classical calculation (cf. [BS], Ch. V, §6.3) derived from [Ku], together with the logarithmic isomorphism (7.2) in the refined form

$$\log : \acute{\mathcal{U}}\mathbb{F}_p K \xrightarrow{\sim} \mathbb{F}_p \Delta K / \mathbb{F}_p \Delta^{p-1} K \,, \tag{7.3}$$

we will show that $\mathrm{im}(\log \circ \overline{\rho} \circ \overline{\iota})_d = \mathbb{F}_p B_d (\log x)^d$, where B_d is the d-th Bernoulli number and x generates K. It seems to be the only calculation in this game which cannot be restricted to the $\star$-symmetric part of $\Delta \mathbb{F}_p K$ (which does not contain $\log x$).

By integrating the appropriate logarithmic derivative in the field $\mathbb{Q}((z))$ of formal Laurent series, one first obtains the identity

$$(*) \qquad \log \frac{e^z - 1}{z} = \frac{z}{2} + \sum_{k \ge 1} \frac{B_{2k}}{(2k)!2k} z^{2k}$$

in the ring of formal power series $\mathbb{Q}[[z]]$, and hence in any truncated polynomial ring $\mathbb{Q}[z]/z^\nu$ for $\nu > 2$. On the other hand, since $(e^z - 1)/z$ is a sum of terms of the form $z^{k-1}/k!$, this truncated polynomial has coefficients in $\mathbb{Z}_p$ as long as $\nu < p$. It follows that $B_2, \ldots, B_{p-3}$ are in $\mathbb{Z}_p$, and that $(*)$ is valid in $\mathbb{F}_p[z]/z^{p-1}$.

Now consider the unit $y = e^z$ in $\mathbb{F}[z]/z^p$, and note that the equation

$$(**) \qquad \frac{1}{r}(1 + y + \cdots + y^{r-1}) = \frac{e^{rz} - 1}{rz} \cdot \frac{z}{e^z - 1}$$

holds for any $1 < r < p$, in the "shorter" ring $\mathbb{F}_p[z]/z^{p-1}$ (because of the "division" by a generator of the maximal ideal of the original $\mathbb{F}_p[z]/z^p$).

After this excursion, let us get back to group rings. Since $y^p = 1$, we can set $x = y$ and identify $\mathbb{F}_p[z]/z^p$ with our modular group ring $R = \mathbb{F}_p K$. The shorter ring $\mathbb{F}_p[z]/z^{p-1}$ then turns into a copy of $R' = \mathbb{F}_p K / \mathbb{F}_p \Delta^{p-1} K$. Combining the equations $(*)$ and $(**)$ and remembering that $z = \log x$, we get

$$\log v_r - \frac{r-1}{2} \log x = \sum_{k \ge 1} (r^{2k} - 1) \frac{B_{2k}}{(2k)!2k} (\log x)^{2k} \tag{7.4}$$

in R', with $v_r = (1 + x + \cdots + x^{r-1})/r$. The group $G = (\mathbb{Z}/p\mathbb{Z})^\times$ operates on the $\mathbb{F}_p$-algebras R and R' by automorphisms of the form $\sigma_c : x \mapsto x^c$. In fact, the eigenspaces of this action are spanned by the powers of z, since σ_c maps $z = \log x$ to cz, and hence z^i to $c^i z^i$. For a typical minimal idempotent e_j of $\mathbb{F}_p G$, we therefore have $e_j \cdot z^i = \delta_{ij} z^i$, the delta being Kronecker's. Putting $w_r = v_r x^{(1-r)/2}$, we thus conclude from (7.4) that

$$e_d \cdot \log w_r = \frac{r^d - 1}{d!d} B_d (\log x)^d \tag{7.5}$$

for even $d = 2k = 2, \ldots, p-3$, all this to be read in R', i.e., modulo $\mathbb{F}_p \Delta^{p-1} K$. Now, if σ_r is a generator of H, every one of the factors $r^d - 1$ is non-zero in

$\mathbb{F}_p$. To prove our inital claim about the image of $(\log\circ\overline{\rho}\circ\overline{\iota})_d$, it only remains to check that w_r, with σ_r generating H, is a $\mathbb{Z}H$-generator of the natural image of $\mathcal{W}(K) = \mathcal{W}(K)$ in $\mathcal{U}\mathbb{F}_pK$. We leave that task to reader, with the hint that $(1+x+\cdots+x^{r-1})^{p-1}\cdot(1+x+\cdots+x^{r-1})/r = 1$ in $\mathbb{F}_pK$. □

Corollary 7.3. *A prime p is regular if and only if the map $\overline{\rho}\circ\overline{\iota}$ is injective, in other words, if and only if $\ker_p\mathcal{U}_2^{\oplus}(K) = \mathcal{U}_2^{\oplus}(K)^p$ for $|K| = p$.*

Proof. Since $\mathcal{U}_2^{\oplus}(K)$ is trivial for $p = 2, 3$, we may assume that $p > 3$. By the lemma, the injectivity of $\overline{\rho}\circ\overline{\iota}$ is equivalent to the non-triviality, modulo p, of all the pertinent B_d. Hence by item (iii) at the beginning of Section 6, the class number factor h_p^- is prime to p. The injectivity of $\overline{\iota}$ yields the same property for the factor h_p^+. □

For cyclic A of order p^2, we have $c(A) = i(K)$ by formula (3.9). Therefore this corollary says that $c(A) = 1$ if and only if p is regular. However, we shall wait for a more precise result. In fact, whatever the size of the p-group A, its automorphism group contains a canonical copy of $(\mathbb{Z}/p\mathbb{Z})^\times$, whose action allows the decomposition of any associated p-group like $\Gamma(A)$ according to the characters τ^d. Theorem 7.7 will deal with the individual components $\Gamma(A)_d$.

Definition 7.4. We shall say that the prime p is *semi-regular* or *regular at d* if the d-th slice of $\overline{\iota}$ or $\overline{\rho}\circ\overline{\iota}$ (respectively) is non-trivial *. An element $u \in \mathcal{W}(K)$ which is not a p-th power in $\mathcal{W}(K)$ but does fall into the kernel of $(\overline{\rho}\circ\overline{\iota})_d$ will be called a *Kummer unit at d*.

A Kummer unit clearly is unique, modulo p-th powers, up to G-conjugation. Its existence is equivalent to p being irregular at d. It can be produced explicitly by applying a pre-image in $\mathbb{Z}G$ of the idempotent $e_d \in \mathbb{F}_pG$ to a $\mathbb{Z}G$-generator $w_\alpha(x)$ of $\mathcal{W}(K)$.

7.2. Non-constructible units

We first describe a process by which units can be pulled back along an epimorphism $A \to A'$. This method will then be used to produce generators of $\mathcal{U}_1^{\oplus}(A)/\mathcal{Y}(A)$ for $|A| = p^2$ and p irregular.

Lemma 7.5. *Let $\varepsilon : A \longrightarrow A'$ be an epimorphism of finite abelian groups, with kernel B. For any $u \in \mathcal{U}_1(A')$ congruent to 1 modulo $|B|$, there exists a unique $\tilde{\varepsilon}(u) \in \mathcal{U}_1(A)$ such that*

$$\psi\big(\tilde{\varepsilon}(u)\big) = \begin{cases} \psi'(u) & \text{if } \psi = \psi'\circ\varepsilon, \\ 1 & \text{if } \psi(B) \neq 1, \end{cases}$$

* An analogous notion of *quasi-regularity*, pertaining to the non-triviality of $\overline{\rho}$, and used in [HS1], would be weaker than regularity only if Vandiver's Conjecture fails.

for any character ψ of A.

Proof. If S_B denotes the sum, in $\mathbb{Z}A$, over all elements of B, we have an induced bijection $S_B\Delta(A) \xrightarrow{\sim} |B|\Delta(A')$, which is an isomorphism of $\mathbb{Z}A$-modules (ideals) in the obvious sense. Therefore it yields an isomorphism of multiplicative semigroups $1+S_B\Delta(A) \xrightarrow{\sim} 1+|B|\Delta(A')$, which in turn can be restricted to invertible elements, producing a group isomorphism

$$\big(1+S_B\Delta(A)\big)\cap U(A) \xrightarrow{\sim} \big(1+|B|\Delta(A')\big)\cap U(A') \tag{7.6}$$

between the groups of units which are $\equiv 1$ modulo S_B and $|B|$, respectively. We are interested in its inverse $\tilde{\varepsilon}$, which is explicitly given by

$$\tilde{\varepsilon}\left(1+|B|\sum_{z\in A'} a_z\cdot z\right) = 1+\sum_{x\in A} a_{\varepsilon(x)}\cdot x = 1+S_B\sum_{y\in R(B)} a_{\varepsilon(y)}\cdot y, \tag{7.7}$$

where $R(B)\subset A$ is any system of representatives of A/B. If $\psi : A \longrightarrow \mathbb{C}^\times$ is any character of A, we have $\psi(S_B) = |B|$ or $= 0$ depending on whether or not $B\subset \ker\psi$, or equivalently, whether or not $\psi = \psi'\circ\varepsilon$ for suitable $\psi' : A' \longrightarrow \mathbb{C}^\times$. Therefore $\psi(\tilde{\varepsilon}(u))$ equals $\psi'(u)$, if $\psi = \psi'\circ\varepsilon$, and 1 otherwise. □

Remark. Before going on, we should once and for all explain the "slicing" of a $\mathbb{Z}_pG$-module X according to the characters of the subgroup $G'\simeq \mathbb{F}_p^\times$ of G. (In this section, we have so far only had the case $G = G'$). Since $\mathbb{Z}_p^\times$ is the inverse limit of the groups $(\mathbb{Z}/p^m\mathbb{Z})^\times$, the canonical surjection $\mathbb{Z}_p^\times \to \mathbb{F}_p^\times \simeq G'$ has a natural right inverse τ called the *Teichmüller character*. All characters $G'\to \mathbb{Z}_p^\times$ are powers τ^d of τ, and — since $(p-1)^{-1}$ exists in $\mathbb{Z}_p$ — the module X splits à la Maschke into $p-1$ "slices" X_d (some perhaps trivial) on each of which G' acts via the appropriate τ^d.

Lemma 7.6. *Let $|K| = p$ and suppose that $u\in\mathcal{W}(K)$ is a Kummer unit at d. Then, if $|A| = p^2$, the d-th component $\Gamma(A)_d$ of $\Gamma(A) = \mathcal{U}_2^\oplus(A)/\mathcal{Y}(A)$ is generated by units of the form $\tilde{\varepsilon}(u)$ for epimorphisms $\varepsilon : A\to K$.*

Proof. For cyclic A of order p^2, Proposition 3.4 says that π induces an isomorphism $\Gamma(A)_d \xrightarrow{\sim} I(K)_d$, where $K = A^p$. If $I(K)_d$ is non-trivial (i.e., p irregular at d), then it is of order p and generated by the Kummer unit u. Hence $\Gamma(A)$ is generated by $\tilde{\pi}(u)$.

Now suppose that A is elementary abelian and consider the set $\{C_0, C_1, \ldots, C_p\}$ of its subgroups, as well as the corresponding factor groups $K_i = A/C_i$ and the canonical maps $\varepsilon_i : A\longrightarrow K_i$. Together, these yield an injection

$$\beta : \mathcal{U}_2^\oplus(A) \longrightarrow \prod_{i=0}^{p}\mathcal{W}(K_i)\,. \tag{7.8}$$

By Lemma 7.5, we have $\varepsilon_i : \tilde{\varepsilon}_j(u)\mapsto u^{\delta_{ij}}$, with Kronecker's δ. Since u generates $\overline{\mathcal{W}}(K)_d$, this says that $\overline{\beta}_d = (\beta\otimes\mathbb{F}_p)_d$ is surjective, and hence, by a rank count,

bijective. In other words, the $\tilde{\varepsilon}_i(u)$ generate $\mathcal{U}_2^{\oplus}(A)$ modulo p-th powers, hence (Nakayama) modulo p^N-th powers for any N, hence *a fortiori* modulo $\mathcal{Y}(A)$. □

Theorem 7.7. *For $|A| > p$, and $d = 2k$ with $2 \le d \le p-3$, the component $\Gamma(A)_d$ is non-zero, whenever p is irregular at d.*

Proof. By Remark 2.2, any inclusion $A \hookrightarrow A'$ entails an injection $\Gamma(A)_d \hookrightarrow \Gamma(A')_d$. Hence we may assume $|A| = p^2$. For cyclic A, the isomorphism $\Gamma(A)_d \xrightarrow{\sim} I(K)_d$ says it all; so suppose that A is elementary abelian.

Since the map β of (7.8) is injective, $\Gamma(A)$ is naturally contained in the cokernel of γ, the restriction of β to $\mathcal{Y}(A)$, for any elementary abelian A. Now,

$$\gamma : \prod_i \mathcal{W}(C_i) \longrightarrow \prod_j \mathcal{W}(K_j) \tag{7.9}$$

is given by an obvious matrix with entries in the endomorphism ring of $\mathcal{W}(K)$. Using that matrix, the $\mathbb{F}_p$-corank of $\overline{\gamma}_d$ was computed in [H1], and found to be > 0 for all d. However, if p is irregular at d, the proof of Lemma 7.6 shows that $\overline{\beta}_d$ is bijective. Hence $\overline{\Gamma}(A)_d$ is *equal* to the cokernel of $\overline{\gamma}_d$. □

> For A cyclic of order p^2, we obviously have an "if and only if". The same is true, a little less obviously, for elementary abelian A. If p is regular at d, the injection $\overline{\mathcal{W}}(K)_d \hookrightarrow (\mathcal{U}_1\mathbb{F}_pK)_d$ is easily converted to $\overline{\mathcal{W}}(K)_d \hookrightarrow (\overline{\mathcal{U}}_1\mathbb{Z}_pK)_d$. In fact, $w = v^p$ with $v \in 1 + \Delta\mathbb{Z}_pK$ clearly makes u trivial in $\mathcal{U}_1\mathbb{F}_pK$. Using Nakayama's Lemma and a rank count, we then obtain an isomorphism $\widehat{\mathcal{W}}(K)_d \xrightarrow{\sim} (\acute{\mathcal{U}}^+\mathbb{Z}_pK)_d$, i.e., a Density Lemma for the d-th slice, and can argue as in the proof of Theorem 6.6 to show that $\Gamma(A)_d$ is trivial. If we could "slice" the Density Lemma for $|K| = p^m$, we would stand a good chance of proving such a converse for general A.

For elementary abelian A with $|A| = p^2$, the cokernel of γ turns out to be elementary abelian as well, and its d-th slice has $\mathbb{F}_p$-dimension $p - d$ (cf. [H1]). Hence the same holds for $\Gamma(A)_d$, if p is irregular at d. By Lemma 7.6, this group is generated by the $p+1$ "lifts" $\tilde{\varepsilon}(u)$ produced from the Kummer unit u by the explicit formula (7.7). It is shown in [H7] that these units are not constructible.

Example. As an illustration, we shall work this out for $p = 37$. If $K = \langle z \rangle$ with $z^{37} = 1$, we have $G = \mathrm{Aut}(K) = (\mathbb{F}_{37})^\times$. For an integer r prime to 37, let $\sigma(r)$ be the corresponding element of G. Since G is generated by $\sigma(2)$ as well as by $\sigma(5)$, the prescriptions of [H8] show that $w(z) = z^{-2} - z^{-1} + 1 - z - z^2$ is a $\mathbb{Z}G$-generator of $\mathcal{W}(K)$. It is well-known that $p = 37$ is irregular only for $d = 32$. Therefore the critical character is $\tau^d : \sigma(a) \mapsto a^{32} = a^{-4}$ (values to be read in $\mathbb{F}_p$), and the corresponding idempotent of $\mathbb{F}_pG$ is

$$e_{32} = -\sum_{r=1}^{36} r^4\sigma(r) = -\sum_{n\in N} n^4\lambda(n), \tag{7.10}$$

where $N = \{1, 2, 3, 4, 5, 8, 9, 10, 15\}$ is a set of representatives modulo the multiplicative subgroup $G_4 = \{6, -1, -6, 1\}$ and $\lambda(n) = \sigma(n) + \sigma(-n) + \sigma(6n) + \sigma(-6n)$.

If we now choose a preimage $\eta_{32} \in \mathbb{Z}G$ of e_{32} by replacing the n^4 in (7.10) by suitable integers $a_n \equiv n^4 \bmod 37$, the resulting Kummer unit will have the form

$$u_{32}(z) = w(z)^{\eta_{32}} = 1 + 37 \sum_{n \in N} c_n (z^n + z^{-n} + z^{6n} + z^{-6n} - 4)\,, \tag{7.11}$$

because it must be invariant under G_4. For a group $A = \langle x, y \rangle$ of order p^2 and an epimorphism $\varepsilon : A \longrightarrow K$ with $\ker \varepsilon = \langle y \rangle$, we can finally write down the unit $\tilde{\varepsilon}(u_{32})$ as

$$u(x, y) = 1 + S_{\langle y \rangle} \sum_{n \in N} c_n (x^n + x^{-n} + x^{6n} + x^{-6n} - 4)\,. \tag{7.12}$$

The coefficients c_n are as follows:

$c_1 = -114755710504066734144 2808$ $\quad$ $c_2 = +681732566824536933894968$
$c_3 = -54182301438440608270800$ $\quad$ $c_4 = -559998713102984680018224$
$c_5 = +995966533834975557490332$ $\quad$ $c_8 = -610334679098778334688974$
$c_9 = +120977500856010523455712$ $\quad$ $c_{10} = +324974773291376818267889$
$c_{15} = -813868801301242469710 03$

In both the cyclic and the elementary case, the units $u(x, y)$ together with the constructible $w(z)$ generate $\mathcal{U}_1^{\oplus}(A)$. If A is elementary, they even generate all of $U_1^+(A)$ because it so happens that $h_{37}^+ = 1$.

Remark. For elementary abelian A of any order $p^{\nu+1}$, the $\mathbb{F}_p$-dimension of $\Gamma(A)_d \otimes \mathbb{F}_p$ equals

$$1 + p + \cdots + p^{\nu} - \binom{d+\nu}{d}\,, \tag{7.13}$$

whenever p is irregular at d, giving an improved lower bound on $|\Gamma(A)_d|$ — cf. Theorem 3.4 of [H7]. However, nothing is known about generators of $\Gamma(A)$ for $\nu > 1$. The assumption of semi-regularity made *loc.cit.* is required for the statement about the cokernel of the map (1.2), and can be dropped in the present context.

8. Local units and global ideal classes

The ultimate aim of this section is to establish, for abelian p-groups A, a connection between the circular index $c(A)$ and the order of a certain group $D^+(A)$ of ideal classes in $\mathbb{Z}A$. The way this is done is foreshadowed in [H2], which deals with the very transparent case of elementary abelian A. The first step is to show that the group $\mathcal{U}_1^+\mathbb{Z}_pA$ of "local" units has a kind of normal basis with respect to $\mathbb{Z}_p(H, \pi)$ — cf. Theorem 8.1 below — as long as p is odd. By the remark at the end of Section 5, this is false for $p = 2$. On the other hand, both $c(A)$ and $D(A)$ are trivial for 2-groups (indeed, for any regular p-groups), so that there is nothing to prove at that level anyway. Hence $p > 2$ throughout this section.

The following account differs from [H6] mainly by substituting the explicit normal basis obtained in [HR3] for the pure existence proof, based on the results of [Bo], used in the earlier paper.

8.1. Normal bases for local units

Let p be an odd prime. In the ring of formal power series $\mathbb{Q}\big[[T]\big]$ consider the element

$$E(T) = \exp\Big(\sum_{k=0}^{\infty} p^{-k} T^{p^k}\Big). \tag{8.1}$$

It is well known that $E(T)$, which was invented by Artin and Hasse [AH], actually lies in $\mathbb{Z}_p\big[[T]\big]$ (cf. [L2] for a quick proof). Therefore it makes sense to substitute $T \mapsto t$, if t is in some $\mathbb{Z}_p$-algebra, and t^k converges to 0 in the p-adic topology. This works, in particular, for $t = z - 1 \in \mathbb{Z}_p A$ with $z \in A$, because the p^m-th power of that element is divisible by p. It works even more easily in the finite group ring $\mathbb{F}_p A$, again with $t = z - 1$ for any $z \in A$.

Theorem 8.1. *$\mathcal{U}_1^+\mathbb{Z}_p A$ has a $\mathbb{Z}_p$-basis consisting of the elements $E(z^{-1} - 2 + z)$, as (z, z^{-1}) ranges over all reciprocal pairs of non-trivial elements of A.*

Proof. The crux of the problem resides in the cyclic case $A = C$, which is dealt with in [HR3]. According to Proposition 1.2 of that paper, the multiplicative group $\mathcal{U}_1^+\mathbb{F}_p C = 1 + \Delta^+\mathbb{F}_p C$ can be generated by the set $\{E(z^{-1} - 2 + z) \mid z \in C\}$, and this suffices (by Principle 4.3, *ibidem*) to establish the present theorem for $A = C$. In particular,

$$\mathcal{U}_1^+\mathbb{Z}_p C = \mathcal{V}_p(C) \times \mathcal{V}_p(C^p) \times \cdots \times \mathcal{V}_p(C_p) \tag{8.2}$$

is a direct product, with $\mathcal{V}_p(C)$ generated over $\mathbb{Z}_p H$ by the single element $v(x) = E(x - 2 + x^{-1})$, where x generates C. Moreover, in the notation of Lemma 2.1, the theorem says that $\mathcal{V}_p(C)$ is free module of rank 1 over $\mathbb{Z}_p H_C$

For general A, Remark 5.7 says that $\mathcal{U}_1^+\mathbb{Z}_p A$ is the product of $\mathcal{U}_1^+\mathbb{Z}_p C$ as C runs over the cylic subgroups of A. Hence, Equation (8.2) can be stretched to become

$$\mathcal{U}_1^+\mathbb{Z}_p A = \prod_{C \subseteq A} \mathcal{V}_p(C)\,, \tag{8.3}$$

and the product is direct by an easy rank count, if we note that the $\mathbb{Z}_p$-rank of $\mathcal{E}_p^+(\zeta_n)$ equals the order of H_C, for $n = |C| = p^m$. □

Corollary 8.2. *If $H = \langle\sigma\rangle$, the kernel of the H-norm on $\mathcal{U}_1^+\mathbb{Z}_p A$ is of the form*

$$\acute{\mathcal{U}}_1^+\mathbb{Z}_p A = \prod_{C \subseteq A} \mathcal{W}_p(C)\,,$$

where $\mathcal{W}_p(C)$ denotes $\mathcal{V}_p(C)^{\sigma-1}$, and the product is direct.

Proof. Since $\mathcal{V}_p(C) \simeq \mathbb{Z}_pH$, each of the components in Equation 8.3 has trivial H-cohomology. In particular, $\acute{\mathcal{V}}_p(C) = \mathcal{V}_p(C)^{\sigma-1}$. □

Remark. If $v(x)$ is a $\mathbb{Z}_pH$-generator of $\mathcal{V}_p(C)$, it follows that $w(x) = v(x)^{\sigma-1}$ is a $\mathbb{Z}_pH$-generator of $\mathcal{W}_p(C)$. The corollary can then be restated by saying:

$\acute{\mathcal{U}}_1^+\mathbb{Z}_pA$ is generated over $\mathbb{Z}_p$ by the set $w(z)$, as (z, z^{-1}) ranges over all reciprocal pairs of non-trivial elements of A; this set can be thinned out to a $\mathbb{Z}_p$-basis by omitting one element from each of its H-orbits.

Let us fix a particular $v(x)$, for instance $v(x) = E(x - 2 + x^{-1})$. Another possibility allowed by [HR3] would be $v(x) = E(x-1)E(x^{-1}-1)$.

Next we need to make a connection between $w(\zeta_n)$ and $w(\zeta_n^p)$ in analogy to Lemma 3.2. Starting *in abstracto*, put $K = \mathbb{Q}_p$ and let F/K be a finite field extension. In the group $\mathcal{U}_F$ of units consider the subgroup $\mathcal{E}_F$ of those elements which are $\equiv 1$ modulo the prime ideal.

Lemma 8.3. *Let F/K be totally ramified and cyclic, with $\mathrm{Gal}\,(F/K) = \langle\sigma\rangle$. If $L \subset F$ is a subfield such that $[F : L] = p$, the norm $N_{F/L}$ surjects $\mathcal{E}_F^{\sigma-1}$ onto $\mathcal{E}_L^{\sigma-1}$.*

Proof. Consider the obvious short exact sequence

$$1 \to \mathcal{E}_K \to \mathcal{E}_F \to \mathcal{E}_F^{\sigma-1} \to 1\,, \tag{8.4}$$

and note that the lemma says something about its $\mathrm{Gal}\,(F/L)$-cohomology, namely that $H^0(\tau, \mathcal{E}_F^{\sigma-1})$ is trivial, where $\langle\tau\rangle = \mathrm{Gal}\,(F/L)$. Since $\mathcal{E}_K = (1 + p\mathbb{Z}_p)^\times$ is torsion-free, it follows that $H^1(\tau, \mathcal{E}_K)$ is trivial, and we get the exact sequence

$$H^0(\tau, \mathcal{E}_K) \to H^0(\tau, \mathcal{E}_F) \to H^0(\tau, \mathcal{E}_F^{\sigma-1}) \to 0\,. \tag{8.5}$$

To win our point, we will prove that the first arrow in this sequence is bijective, by showing (i) that it is not the zero map, and (ii) that its target has order p.

If yon arrow were the zero map, we would have $1+p = N_\tau(u)$, for some $u \in \mathcal{E}_F$, and hence $N_\sigma(u) = (1+p)^{s/p}$, where $s = [F : K]$ is the order of σ. Since $1 + p$ is a p-adic generator of $\mathcal{E}_K$, this would imply that $H^0(\sigma, \mathcal{E}_F) = \mathcal{E}_K/N_\sigma(\mathcal{E}_F)$ had order at most $p^{\mu-1}$, where $s = p^\mu t$ with t prime to p. However, we shall presently see that

$$H^0(\sigma, \mathcal{E}_F) \simeq \mathbb{Z}/p^\mu\mathbb{Z} \quad \text{and} \quad H^0(\tau, \mathcal{E}_F) \simeq \mathbb{Z}/p\mathbb{Z}\,, \tag{8.6}$$

which proves both (i) and (ii). We first shift our attention to $\mathcal{U}_F$ by noting that, modulo the prime ideal of F, the unit group $\mathcal{U}_F$ appears as $\mathbb{F}_p^\times$ (because of the total ramification), and the Teichmüller character $\mathbb{F}_p^\times \to \mathbb{Z}_p^\times$ yields a splitting $\mathcal{U}_F = (\mathbb{Z}_p^\times)_{\mathrm{tor}} \times \mathcal{E}_F$. Consequently, $H^i(\rho, \mathcal{U}_F) = H^i(\rho, \mathbb{F}_p^\times) \times H^i(\rho, \mathcal{E}_F)$ for any i and $\rho = \sigma^j$. In other words, $H^i(\rho, \mathcal{E}_F)$ is always the p-primary component of

$H^i(\rho,\mathcal{U}_F)$. Hence (8.6) will follow from the composite isomorphism

$$H^0(\rho,\mathcal{U}_F) \simeq H^0(\rho,F^\times) \simeq \langle\rho\rangle\,, \tag{8.7}$$

whose second step is the central result of local class field theory — cf. [L1], IX.3, Lemma 4 — and whose first step comes from the total ramification as follows. We start with the exact sequence $1 \to \mathcal{U}_F \to F^\times \to \mathbb{Z} \to 0$, in which the map to $\mathbb{Z}$ is given by the valuation on F. In cohomology this yields

$$0 \to H^0(\rho,\mathcal{U}_F) \to H^0(\rho,F^\times) \to H^0(\rho,\mathbb{Z}) \to H^1(\rho,\mathcal{U}_F) \to 0\,, \tag{8.8}$$

the end terms representing $H^1(\rho,\mathbb{Z})$ and $H^1(\rho,F^\times)$, respectively. It suffices to show that the middle arrow is the zero map. Indeed: to any $a \in F$ left fixed by ρ, the valuation on F will assign a multiple of the order of ρ. □

Corollary 8.4. *Under the hypotheses of Lemma 8.3, the group $\acute{\mathcal{E}}_F/\mathcal{E}_F^{\sigma-1}$ is cyclic of order p^μ, the highest p-power dividing the order of σ.*

Proof. By the preceding proof, the transition map $H^0(\sigma,\mathbb{Z}) \to H^1(\sigma,\mathcal{U}_F)$ is bijective, too — in other words, $H^i(\sigma,\mathcal{U}_F) \simeq \langle\rho\rangle$ for $i = 1, 2$ — whence the result by taking p-primary components. □

Here comes the local analogue of Proposition 3.3.

Proposition 8.5. *The character ψ defined by $\psi(x) = \zeta_n$ induces a bijection of $\mathcal{W}_p(C)$ onto $\mathcal{E}_p^+(\zeta_n)^{\sigma-1} = \psi\big(\acute{\mathcal{U}}_1^+\mathbb{Z}_pC\big)$.*

Proof. Because of the surjectivity $\psi : \mathcal{U}_1^+\mathbb{Z}_pC \to \mathcal{E}_p^+(\zeta_n)$, we get the identity indicated at the end of the proposition. Lemma 8.3, applied to $F = \mathbb{Q}_p(\zeta_n+\zeta_n^{-1})$, now yields a surjection $\nu_1 : \mathcal{E}_p^+(\zeta_n)^{\sigma-1} \to \mathcal{E}_p^+(\zeta_{n/p})^{\sigma-1}$, where ν_1 is the appropriate Galois norm. The composite $\nu_1 \circ \psi$ therefore maps $\acute{\mathcal{U}}_1^+\mathbb{Z}_pC = \mathcal{W}_p(C) \times \acute{\mathcal{U}}_1^+\mathbb{Z}_pC^p$ onto $\mathcal{E}_p^+(\zeta_{n/p})^{\sigma-1}$. Since ν_1 turns $\acute{\mathcal{U}}_1^+\mathbb{Z}_pC^p$ into p-th powers, it follows that $\nu_1 \circ \psi$ induces a map

$$\mathcal{W}_p(C) \longrightarrow \mathcal{E}_p^+(\zeta_{n/p})^{\sigma-1} = \psi\big(\acute{\mathcal{U}}_1^+\mathbb{Z}_pC^p\big) \tag{8.9}$$

which is surjective modulo p-th powers. Since it is a morphism of finitely generated $\mathbb{Z}_p$-modules, it is surjective by Nakayama's Lemma. But clearly,

$$\psi\big(\acute{\mathcal{U}}_1^+\mathbb{Z}_pC^p\big) = \nu_1 \circ \psi\big(\mathcal{W}_p(C)\big) = \psi\big(\mathcal{W}_p(C)^{\nu_1}\big) \subset \psi\big(\mathcal{W}_p(C)\big)\,, \tag{8.10}$$

whence the result, by using the split $\acute{\mathcal{U}}_1^+\mathbb{Z}_pC = \mathcal{W}_p(C) \times \acute{\mathcal{U}}_1^+\mathbb{Z}_pC^p$ once more. □

Remark. Abbreviating $\psi(\acute{\mathcal{U}}_1^+\mathbb{Z}_pC)$ by $\mathcal{L}_p(\zeta_n)$ — the $\mathcal{L}$ stands for "liftable" — we inductively get a sequence of surjections

$$\nu_i : \mathcal{L}_p(\zeta_n) \to \mathcal{L}_p(\zeta_{n/p^i})\,, \tag{8.11}$$

induced by the Galois norms ν_i for $i = 1, \dots, m-1$. Together with the bijections

$$\psi : \mathcal{W}_p(C^{p^i}) \to \mathcal{L}_p(\zeta_{n/p^i}) \tag{8.12}$$

these will form an essential ingredient in the planned comparison of the present local (i.e.,p-adic) pattern and the global one met in Lemmas 3.2 and 3.3.

As we have seen, it all hinges on the surjectivity of ν_1, which was here derived from the subtle "reciprocity" isomorphism $H^0(\rho, F^\times) \simeq \langle\rho\rangle$, while in Lemma 3.2, it resulted from the simple equation $\nu_1(\zeta_n - 1) = (\zeta_{n/p} - 1)$. It would be desirable to have such an explicit identity for the local case, too. The most obvious guess, namely $\nu_1(u_n) = u_{n/p}$ is certainly wrong for $u_k = E(\zeta_k - 1)$. Indeed, since $u_k u_k^\star$ generates $\mathcal{E}_p^+(\zeta_k)$, it would imply the triviality of $H^0(\tau, \mathcal{E}_p^+(\zeta_k))$ — in contradiction to (8.6).

8.2. Comparison with global units

We begin in an abstract setting. Let Z be a principal ideal domain such that Z/nZ is finite for every natural number n, let $\mathcal{G}$ be a finite abelian group with a filtration

$$\mathcal{G} = \mathcal{G}_0 \supset \mathcal{G}_1 \supset \cdots \supset \mathcal{G}_m = 1\,, \tag{8.13}$$

and let L be a monogenic $Z\mathcal{G}$-module, free over Z and with $H^0(\mathcal{G}_\mu, L) = 0$ for $\mu = 1, \dots, m$. With Y_μ denoting the part of L left fixed by $\mathcal{G}_\mu$, we then have an induced filtration

$$L = Y_m \supseteq Y_{m-1} \supseteq \cdots \supseteq Y_0\,. \tag{8.14}$$

Since the cohomology condition makes the appropriate traces $Y_m \to Y_\mu$ surjective, each of the Y_μ is again $Z\mathcal{G}$-monogenic. Now choose a $Z\mathcal{G}$-generator y_μ of Y_μ for each $\mu = 1, \dots, m$, and in the direct sum $Y = Y_m \oplus \cdots \oplus Y_1$, consider the m-tuples $x_k = [y_k, y_{k-1}, \dots, y_1, 0, \dots, 0]$, where the first component lies in Y_m and the last one in Y_1. Note that Y_0 does *not* figure as a component of Y. The following lemma is the upshot of Section 6 in [H6].

Lemma 8.6. *The index in Y of the $Z\mathcal{G}$-submodule X generated by $x_1, \dots, x_m$ is finite and independent of the choice of $y_1, \dots, y_m$.*

The proof hinges on verifying that the index calculation yields the same result as if we had chosen all the y_μ to be traces of a single y_m. To state that result, let r_μ be the Z-rank of $Y_\mu/Y_{\mu-1}$, which is free since it obviously has no Z-torsion. Moreover let n_μ be the product of the indices $[\mathcal{G}_\mu : \mathcal{G}_k]$ for k running from μ to m. Then

$$(*) \qquad [Y : X] = \prod_{\mu=1}^{m} |n_\mu|_Z^{r_\mu}\,,$$

where $|n|_Z$ stands for the cardinality of Z/nZ. In our application Z will be $\mathbb{Z}_p$ and $\mathcal{G}_1$ will be a p-group, so this is no mystery. Note: in Formula (25) of [H6], bases and exponents of $(*)$ were erroneously switched.

Staying within our abstract shell, we still need a simple lemma about indices of Z-module homomorphisms $f : X \longrightarrow X'$. By the *index* of f (denoted $\mathrm{ind}f$), we mean the cardinality (possibly ∞) of its cokernel. We are particularly interested in morphisms of the form

$$X_1 \oplus \cdots \oplus X_N \xrightarrow{f} X'_1 \oplus \cdots \oplus X'_N \,. \tag{8.15}$$

Let $f_i : X_i \to X'_i$ be the map obtained by first applying f and then projecting onto the i-th component. The following observation is an easy exercise in the use of triangular determinants.

Lemma 8.7. *Let f be a Z-module homomorphism as in (8.15) with the property that $f(X_i) \subset X'_1 \oplus \cdots \oplus X'_i$, for each i, and such that the components X_i and X'_i are free Z-modules of the same rank. Then* $\mathrm{ind}f = \prod_i \mathrm{ind}f_i$.

Now we come back to the multiplicative groups of $\mathbb{Z}A$ and $\mathbb{Z}_pA$, ready to tackle the main result of this subsection.

Proposition 8.8. *In the notation of Section 4, we have the following equality of indices*

$$\left[\mathcal{E}^{\oplus}(A) : \mathcal{Y}(A)\right] = \left[\acute{\mathcal{E}}_p^{+}(A) : \acute{\mathcal{U}}_1^{+}\mathbb{Z}_pA\right] .$$

Proof. Noting that equivalence classes of characters ψ of A are in bijective correspondence with cyclic factor groups $K = A/\ker\psi$, we represent $\mathcal{E}(A)$ as the direct product of $\mathcal{E}(\zeta_K)$, where ζ_K is a suitable $|K|$-th root of unity, and every K comes up exactly once. Concerning the commutative square of $\mathbb{Z}_pH$-module inclusions,

$$\begin{array}{ccc} \prod_C \widehat{\mathcal{W}}(C) & \xrightarrow{f} & \prod_C \mathcal{W}_p(C) \\ h\downarrow & & \downarrow h_p \\ \prod_K \widehat{\mathcal{E}}^{\oplus}(\zeta_K) & \xrightarrow{g} & \prod_K \acute{\mathcal{E}}_p^{+}(\zeta_K) \end{array} \tag{8.16}$$

with C and K running over cylic subgroups and factor groups, respectively, we must then show that the indices of the two vertical arrows — or equivalently, of the two horizontal ones — are equal. The permission to put hats on the left hand side comes from Propositions 3.6 and 4.1, with an assist from Lemma 4.2: they say that the index of h is a p-power *a priori*.

Now g is diagonal because $\mathcal{E}^{\oplus}(\zeta_K) \subset \acute{\mathcal{E}}_p^{+}(\zeta_K)$ for each K. On the other hand, since $\mathcal{W}(C) \subset \acute{\mathcal{U}}_1^{+}\mathbb{Z}_pC$, we can make f satisfy the triangularity condition of Lemma 8.7 by numbering the C so that $|C_i| < |C_j|$ implies $i < j$. Therefore we have the identities

$$\mathrm{ind}g = \prod_K \mathrm{ind}g_K \,, \qquad \mathrm{ind}f = \prod_C \mathrm{ind}f_C \,, \tag{8.17}$$

where g_K and f_C are the composites with the obvious projections. Note that, while f is canonical, the component map f_C depends on the generator chosen for $\mathcal{W}_p(C)$. On the other hand, $\mathrm{ind} g_K = \big[\acute{\mathcal{E}}_p^+(\zeta_K) : \widehat{\mathcal{E}}^\oplus(\zeta_K)\big] = e_{|K|}$ depends only on the order $|K|$. We shall finish the proof by showing

$$\mathrm{ind} f_C = e_{|C|}\,, \tag{8.18}$$

in other words: $|C| = |K| \implies \mathrm{ind} f_C = \mathrm{ind} g_K$. Since the cyclic subgroups and factor groups of A are in one-to-one correspondence, this together with (8.17) will imply the desired equality of indices.

We now reduce the proposition to the special case where $A = C$ is cyclic of order $n = p^m$. In this setting, the diagram (8.16) has the form:

$$\begin{array}{ccc} \widehat{\mathcal{W}}(C) \times \cdots \times \widehat{\mathcal{W}}(C_p) & \xrightarrow{\ f\ } & \mathcal{W}_p(C) \times \cdots \times \mathcal{W}_p(C_p) \\ h \downarrow & & \downarrow h_p \\ \widehat{\mathcal{E}}^\oplus(\zeta_n) \times \cdots \times \widehat{\mathcal{E}}^\oplus(\zeta_p) & \xrightarrow{\ g\ } & \acute{\mathcal{E}}_p^+(\zeta_n) \times \cdots \times \acute{\mathcal{E}}_p^+(\zeta_p)\,. \end{array} \tag{8.19}$$

Moreover, (8.17) boils down to

$$\mathrm{ind} g = e_n \times \cdots \times e_p\,, \qquad \mathrm{ind} f = \mathrm{ind} f_C \times \cdots \times \mathrm{ind} f_{C_p} \tag{8.20}$$

and (8.18) would easily obtained by recursively applying the equality $\mathrm{ind} f = \mathrm{ind} g$ to the cyclic groups of order $p^\mu \le p^m$ — if that were known.

At this point, we abandon f and g in favour of the original objects of attention h and h_p, but in the cyclic context (8.19). Before we can apply Lemma 8.6 to it, we must make another small adjustment: replace the $\mathcal{E}^\oplus(\zeta_q)$ and $\acute{\mathcal{E}}_p^+(\zeta_q)$ on the bottom line of (8.19) by their subgroups $\mathcal{L}(\zeta_q) = \psi(\mathcal{W}(C_q))$ and $\mathcal{L}_p(\zeta_q) = \psi(\mathcal{W}_p(C_q))$ of "liftable" elements, where $q = p^\mu \le n$ and $\psi : x \mapsto \zeta_n$. To keep things on an even keel, we first show that

$$[\mathcal{E}^\oplus(\zeta_q) : \mathcal{L}(\zeta_q)] = [\acute{\mathcal{E}}_p^+(\zeta_q) : \mathcal{L}_p(\zeta_q)]\,. \tag{8.21}$$

Let us do this for $q = n$. On the right hand side of this desired equation, we have p^{m-1} by Corollary 8.4 and Proposition 8.5. To compute the left hand side, we consider the homomorphism

$$G \longrightarrow \mathcal{U}^\oplus(\zeta_n)/\mathcal{L}(\zeta_n) \tag{8.22}$$

defined almost as in (3.5) by $\tau \mapsto (\zeta_n^{-1} - \zeta_n)^{\tau-1}$. The change from $(\zeta_n - 1)$ to $(\zeta_n^{-1} - \zeta_n) = \zeta_n^2(\zeta_n - 1)$ ensures that the images are $\star$-symmetric, but makes no other difference in the proof of Lemma 3.1 when n is odd. Therefore the map (8.22) is bijective, whence

$$(p-1)p^{m-1} = \big[\mathcal{U}^\oplus(\zeta_n) : \mathcal{E}^\oplus(\zeta_n)\big]\big[\mathcal{E}^\oplus(\zeta_n) : \mathcal{L}(\zeta_n)\big]\,. \tag{8.23}$$

This implies (8.21) since $\mathcal{E}^{\oplus}(\zeta_n)$ is the kernel of the surjection $\mathcal{U}^{\oplus}(\zeta_n) \to \mathbb{F}_p^{\times}$ given by $\zeta_n \mapsto 1$. Finally it remains to prove that the vertical arrows in the diagram

$$\begin{array}{ccc} \widehat{\mathcal{W}}(C) \times \cdots \times \widehat{\mathcal{W}}(C_p) & \xrightarrow{f} & \mathcal{W}_p(C) \times \cdots \times \mathcal{W}_p(C_p) \\ h' \downarrow & & \downarrow h'_p \\ \widehat{\mathcal{L}}(\zeta_n) \times \cdots \times \widehat{\mathcal{L}}(\zeta_p) & \xrightarrow{g} & \mathcal{L}_p(\zeta_n) \times \cdots \times \mathcal{L}_p(\zeta_p)\,, \end{array} \tag{8.24}$$

have equal indices. This is where Lemma 8.6 comes in, with the role of L played by $\widehat{\mathcal{L}}(\zeta_n)$ or by $\mathcal{L}_p(\zeta_n)$ — which are both isomorphic to $\mathbb{Z}_pH/\Sigma(H)$ — and X being the image of h' or h'_p, respectively. The filtered group $\mathcal{G}$ is just H with its obvious filtration, and the cohomology condition is equivalent to the surjectivity of the norms explained in the remarks following Propositions 3.3 and 8.5. The details of this translation are left to the reader. □

Corollary 8.9. *The circular index $c(A)$ is equal to $\left[\acute{\mathcal{E}}_p^+(A) : \mathcal{E}^{\oplus}(A)\acute{\mathcal{U}}_1^+\mathbb{Z}_pA\right]$. If p is semi-regular, this equals $\left[\acute{\mathcal{E}}_p^+(A) : \mathcal{E}^{+}(A)\acute{\mathcal{U}}_1^+\mathbb{Z}_pA\right]$*

Proof. Let $T^{\oplus}(A)$ stand for the factor group $\acute{\mathcal{E}}_p^+(A)/\mathcal{E}^{\oplus}(A)\acute{\mathcal{U}}_1^+\mathbb{Z}_pA$. Since $\mathcal{U}_1^{\oplus}(A)$ equals $\mathcal{E}^{\oplus}(A) \cap \acute{\mathcal{U}}_1^+\mathbb{Z}_pA$ by the pull-back (6.1), we have an exact sequence

$$1 \to \mathcal{E}^{\oplus}(A)/\mathcal{U}_1^{\oplus}(A) \to \acute{\mathcal{E}}_p^+(A)/\acute{\mathcal{U}}_1^+\mathbb{Z}_pA \to T^{\oplus}(A) \to 1 \tag{8.25}$$

which is easily enlarged to

$$1 \to \mathcal{U}_1^{\oplus}(A)/\mathcal{Y}(A) \to \mathcal{E}^{\oplus}(A)/\mathcal{Y}(A) \to \acute{\mathcal{E}}_p^+(A)/\acute{\mathcal{U}}_1^+\mathbb{Z}_pA \to T^{\oplus}(A) \to 1\,. \tag{8.26}$$

This would have worked with *any* subgroup of $\mathcal{U}_1^{\oplus}(A)$ in the place of $\mathcal{Y}(A)$, but the way it is, the orders of the two middle terms are equal by Proposition 8.8 — whence the first statement. As for the second, note that all the terms of (8.25) are finite p-groups. Hence we may tensor the whole mess with $\mathbb{Z}_p$ without changing anything. However, if p is semi-regular, $\widehat{\mathcal{E}}^{\oplus}(A)/\widehat{\mathcal{U}}_1^{\oplus}(A)$ equals $\widehat{\mathcal{E}}^{+}(A)/\widehat{\mathcal{U}}_1^{+}(A)$ by the remark following Corollary 6.4. In other words, (8.25) changes into

$$1 \to \widehat{\mathcal{E}}^{+}(A)/\widehat{\mathcal{U}}_1^{+}(A) \to \acute{\mathcal{E}}_p^+(A)/\acute{\mathcal{U}}_1^+\mathbb{Z}_pA \to T^{\oplus}(A) \to 1\,. \tag{8.27}$$

Taking the hats off again, this shows $T^{\oplus}(A)$ to equal the potentially smaller group $T^{+}(A) = \acute{\mathcal{E}}_p^+(A)/\mathcal{E}^{+}(A)\acute{\mathcal{U}}_1^+\mathbb{Z}_pA$, in this case. □

8.3. Kernel groups

Let $\mathcal{A} \subset \mathcal{B}$ be orders of the rational group algebra $\mathbb{Q}(A)$, and $\mathcal{A}_p \subset \mathcal{B}_p$ their p-adic counterparts. It follows easily from the work of Fröhlich [Frö] (cf. also [H2]) that there is an exact sequence

$$1 \to \mathcal{U}(\mathcal{B})/\mathcal{U}(\mathcal{A}) \to \mathcal{U}(\mathcal{B}_p)/\mathcal{U}(\mathcal{A}_p) \to D(\mathcal{A},\mathcal{B}) \to 1\,, \tag{8.28}$$

where $\mathcal{U}$ stands for units, and $D(\mathcal{A},\mathcal{B}) = \ker(\mathrm{cl}(\mathcal{A}) \to \mathrm{cl}(\mathcal{B}))$ is the kernel of the natural map between the ideal class groups — whence the name "kernel group". Another way of saying this is that $\mathcal{U}(\mathcal{A})$ is the kernel of the obvious difference map $\delta : \mathcal{U}(\mathcal{B}) \times \mathcal{U}(\mathcal{A}_p) \to \mathcal{U}(\mathcal{B}_p)$, and that $D(\mathcal{A},\mathcal{B})$ is its cokernel. Splitting off augmentations, we can also get $D(\mathcal{A},\mathcal{B})$ as the cokernel of $\delta_1 : \mathcal{U}_1(\mathcal{B}) \times \mathcal{U}_1(\mathcal{A}_p) \to \mathcal{U}_1(\mathcal{B}_p)$, where $\mathcal{U}_1(\mathcal{B})$ denotes the kernel of the augmentation map on $\mathcal{U}(\mathcal{B})$. Moreover, the kernel of δ_1 is $\mathcal{U}_1(\mathcal{A})$.

If $\mathcal{B} = \mathbb{M}$ is the maximal order and $\mathcal{A} = \mathbb{Z}A$ the group ring, we shall write $D(A)$ instead of $D(\mathcal{A},\mathbb{M})$. Then $D(A)$ is the cokernel of

$$\prod_{\varphi\neq 1} \mathcal{U}(\varphi) \times \mathcal{U}_1(\mathcal{A}_p) \to \prod_{\varphi\neq 1} \mathcal{U}_p(\varphi)\,, \tag{8.29}$$

where φ runs through a complete set of rationally inequivalent characters of A, and $\mathcal{U}(\varphi)$ stands for the units of the φ-th component of $\mathbb{M}$. For each φ, we have $\mathcal{U}(\varphi) = \mathcal{U}(\zeta)$ for a suitable root $\zeta \neq 1$ of unity. It is straightforward to verify that all these $\mathcal{U}(\zeta)$ can be replaced by the corresponding $\mathcal{E}(\zeta)$ without changing the kernel $\mathcal{U}_1(A)$ or the cokernel $D(A)$ of (8.29) — cf. Lemma 7.1 of [H6]. Changing back to the format of (8.28), we now have the exact sequence

$$1 \to \mathcal{E}(A)/\mathcal{U}_1(A) \to \mathcal{E}_p(A)/\mathcal{U}_1(\mathcal{A}_p) \to D(A) \to 1\,, \tag{8.30}$$

where $\mathcal{U}_1(\mathcal{A}_p)$ is, of course, the group denoted heretofore by $\mathcal{U}_1\mathbb{Z}_pA$. This shows that $D(A)$ is a finite p-group, because the other terms are. Moreover, since p is odd, we can take their $\star$-symmetric parts individually and still keep the sequence exact. We now do that and simultaneously replace $\mathcal{E}_p^+(A)$ by $\acute{\mathcal{E}}_p^+(A)$, to obtain the sequence

$$1 \to \mathcal{E}^+(A)/\mathcal{U}_1^+(A)) \to \acute{\mathcal{E}}_p^+(A)/\acute{\mathcal{U}}_1^+(\mathcal{A}_p) \to T^+(A) \to 1\,, \tag{8.31}$$

where $T^+(A) \subseteq D^+(A)$ is the group already met in the proof of Corollary 8.9. The factor group $D^+(A)/T^+(A)$ will be examined presently.

Definition 8.10. Let $\mathcal{I}$ be the set of non-trivial cyclic subgroups of A, and $\mathcal{J}$ be the analogous set for the dual group of A. Define a matrix (e_{ij}) on $\mathcal{I} \times \mathcal{J}$ by setting $e_{ij} = 0$ or $= 1$, depending on whether j does or does not annihilate i. The *character index* $\chi(A)$ is defined to be the absolute value of its determinant.

Lemma 8.11. *For the aforementioned groups, we have* $|D^+(A)| = |T^+(A)|\chi(A)$.

Proof. There is an obvious monomorphism of short exact sequences from (8.31) to the $\mathcal{E}_p^+$-version of (8.31). Taking cokernels, we see that $D^+(A)/T^+(A)$ is the cokernel of the injection

$$\acute{\mathcal{E}}_p^+(A)/\acute{\mathcal{U}}_1^+(\mathcal{A}_p) \to \mathcal{E}_p^+(A)/\mathcal{U}_1^+(\mathcal{A}_p)\,, \tag{8.32}$$

or, by elementary reshuffling, the cokernel of

$$\mathcal{U}_1^+(\mathcal{A}_p)/\acute{\mathcal{U}}_1^+(\mathcal{A}_p) \to \mathcal{E}_p^+(A)/\acute{\mathcal{E}}_p^+(A)\,. \tag{8.33}$$

By Theorem 8.1 and Corollary 8.2, the source of the morphism (8.33) is a direct product whose components are of the form $\mathcal{V}_p(C)/\mathcal{W}_p(C)$, each isomorphic to $\mathbb{Z}_pH_C/\Delta\mathbb{Z}_pH_C \simeq \mathbb{Z}_p$. The target of that morphism is also a direct product, indexed by the cyclic factor groups K of A, with each component being of the form $\mathcal{E}_p^+(\zeta_K)/\acute{\mathcal{E}}_p^+(\zeta_K)$, hence isomorphic to the multiplicative group of possible H_C-norm values, i.e., $1+p\mathbb{Z}_p \simeq \mathbb{Z}_p$. Hence source and target of (8.33) are free $\mathbb{Z}_p$-modules on the index sets $\mathcal{I}$ and $\mathcal{J}$ mentioned in Definition 8.10. It is easy to see that the matrix of this map is just the (e_{ij}) described in the definition. □

Theorem 8.12. *$|D^+(A)| = c(A)\chi(A)$, if p is semi-regular.*

Proof. Obvious from Corollary 8.9 and Lemma 8.11. □

Remark. In view of the fact that no prime has yet been found to violate the condition of semi-regularity, this is a potentially far-reaching theorem.

If p is regular, we have $|D^+(A)| = \chi(A)$. If A is cyclic, the matrix (e_{ij}) is easily seen to be triangular with 1's on the diagonal, so that $|D^+(A)| = c(A)$. In that case, the results of Ullom [Ul] concerning $|D^+(A)|$ can be used to obtain $c(A)$.

On the other hand, any surjective homomorphism $A \to A'$ clearly induces an epimorphism of the corresponding sequences (8.33) and hence a divisibility $\chi(A') \mid \chi(A)$. Thus, if A is non-cyclic, we can take A' to be non-cyclic of order p^2, and since $\chi(A') = p$ in that case by Proposition 3.2 of [H2], we have $\chi(A) \neq 1$. In particular, $|D^+(A)| = 1$ if and only if p is regular and A is cyclic.

9. Cyclic groups of composite order

Let A be a cyclic group of order n with $n = pq$, the product of two distinct primes, and with generator $x = yz$, where y is of order q and z is of order p. We shall reduce the computation of the circular index $c(A) = \left[\mathcal{U}_2^{\oplus}(A) : \mathcal{Y}(A)\right]$ to calculations inside the multiplicative groups of the finite semi-simple rings $\mathbb{F}_q[\zeta_p]$ and $\mathbb{F}_p[\zeta_q]$. Here ζ_p denotes a primitive p-th root of unity; in other words, $\mathbb{F}_q[\zeta_p]$ stands for the polynomial ring $\mathbb{F}_q[X]$ modulo $1+X+\cdots+X^{p-1}$. Roughly speaking, a non-trivial $c(A)$ is due to the failure of the circular units in $\mathbb{Z}[\zeta_p]$ and $\mathbb{Z}[\zeta_q]$ to generate sufficiently large subgroups of $\mathbb{F}_q[\zeta_p]^\times$ and $\mathbb{F}_p[\zeta_q]^\times$, respectively.

This section is a partial amalgam of [H9] and Section 6 of [H8]. While $q = 2$ is allowed, we shall always suppose that p is odd.

9.1 An exact sequence

In order to simplify the appearance of certain formulas, we shall usually write $\xi = \zeta_n$, $\eta = \zeta_q$, and $\zeta = \zeta_p$, with $\xi = \eta\zeta$. From Section 7 of [KM], we take the

asymmetric pair of pull-backs

$$\begin{array}{ccc} \mathbb{Z}A & \longrightarrow & \mathbb{Z}[\eta]A_p \\ \downarrow & & \downarrow \\ \mathbb{Z}A_p & \longrightarrow & \mathbb{F}_q A_p \end{array} \qquad \text{and} \qquad \begin{array}{ccc} \mathbb{Z}[\eta]A_p & \longrightarrow & \mathbb{Z}[\xi] \\ \downarrow & & \downarrow \\ \mathbb{Z}[\eta] & \longrightarrow & \mathbb{F}_p[\eta]\,, \end{array} \tag{9.1}$$

where $A^q = A_p$ and $A^p = A_q$ are the subgroups of order p and q, respectively. It is not difficult to amalgamate these two pull-backs into a single symmetric one:

$$\begin{array}{ccc} \mathbb{Z}A & \longrightarrow & \mathbb{Z}[\xi] \\ \downarrow & & \downarrow \\ \mathbb{Z}A_q \times_1 \mathbb{Z}A_p & \longrightarrow & \mathbb{F}_p[\eta] \times \mathbb{F}_q[\zeta]\,, \end{array} \tag{9.2}$$

in which $\times_1$ 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 $\mathrm{red}_Q : \mathbb{Z}[\xi] \longrightarrow \mathbb{F}_q[\zeta]$ is the reduction modulo the ideal $Q = (\eta - 1)\mathbb{Z}[\xi]$, and red_P is its counterpart for $P = (\zeta - 1)\mathbb{Z}[\xi]$.

When we apply any of the functors $\mathcal{U}_1$, $\mathcal{U}_1^+$, or $\mathcal{U}_1^\oplus$ to the rings on the left hand side of (9.2), and the corresponding $\mathcal{U}$, $\mathcal{U}^+$, or $\mathcal{U}^\oplus$ on the right hand side, we obtain a pull-back of groups — now with a *direct* product in the lower left. We are especially interested in the $\mathcal{U}_1^\oplus$-version, which we modify somewhat in order to involve $\mathcal{U}_2^\oplus(A)$. Of course, for odd $|A|$ nothing needs to be done, since then $\mathcal{U}_2^\oplus(A) = \mathcal{U}_1^\oplus(A)$ anyway. For $q = 2$ however, the fact that $\mathcal{U}_1^\oplus(A) = A_2 \times \mathcal{U}_2^\oplus(A)$ and $\mathcal{U}_1^\oplus(A_2) = A_2$, with $A_2 \neq \{1\}$, would make for an awkward complication. By the comment following the formula (2.8), we have $\mathcal{U}_2^\oplus(A) = \ker\big[\mathcal{U}_1^\oplus(A) \to A_2\big]$ and hence can easily derive the pull-back

$$\begin{array}{ccc} \mathcal{U}_2^\oplus(A) & \longrightarrow & \mathcal{U}^\oplus(\xi) \\ \downarrow & & \downarrow \\ \mathcal{W}(A_q) \times \mathcal{W}(A_p) & \longrightarrow & \mathcal{U}\mathbb{F}_p[\eta] \times \mathcal{U}\mathbb{F}_q[\zeta], \end{array} \tag{9.3}$$

which works for all cases. Its lower left hand corner reflects the important fact that $\mathcal{U}_2^\oplus(C) = \mathcal{Y}(C) = \mathcal{W}(C)$ for any C of prime order. The pull-back also makes $\ker\big[\mathcal{U}_2^\oplus(A) \to \mathcal{U}^\oplus(\xi)\big]$, which we denote by $\mathcal{U}_2^\oplus(A|p,q)$, a direct product:

$$\mathcal{U}_2^\oplus(A|p,q) \;\simeq\; \ker\big[\mathcal{W}(A_q) \to \mathcal{U}\mathbb{F}_p[\eta]\big] \times \ker\big[\mathcal{W}(A_p) \to \mathcal{U}\mathbb{F}_q[\zeta]\big]\,. \tag{9.4}$$

The notation $\mathcal{U}(A|\ldots)$ is supposed to indicate which of the characters $\psi_n : x \mapsto \xi$, $\psi_q : x \mapsto \eta$, and $\psi_p : x \mapsto \zeta$ can be non-trivial on the units in question. In these terms, the subgroups of $\mathcal{U}_2^\oplus(A)$ corresponding to the two kernels shown in (9.4) are just $\mathcal{U}_2^\oplus(A|q)$ and $\mathcal{U}_2^\oplus(A|p)$, respectively. Thus we have the direct product $\mathcal{U}_2^\oplus(A|p,q) = \mathcal{U}_2^\oplus(A|p) \times \mathcal{U}_2^\oplus(A|q)$. Putting $\mathcal{L}(\xi) = \mathrm{im}\big[\mathcal{U}_2^\oplus(A) \longrightarrow \mathcal{U}^\oplus(\xi)\big]$, where $\mathcal{L}$

again means "liftable", we obtain the short exact sequence

$$1 \longrightarrow \mathcal{U}_2^{\oplus}(A|p) \times \mathcal{U}_2^{\oplus}(A|q) \longrightarrow \mathcal{U}_2^{\oplus}(A) \longrightarrow \mathcal{L}(\xi) \longrightarrow 1\,. \tag{9.5}$$

Unfortunately, the functor $\mathcal{Y}$ does not preserve the pull-back property. So, when we restrict the map $x \mapsto \xi$ to the constructible units $\mathcal{Y}(A)$, the kernel $\mathcal{Y}(A|p,q)$ does not in general split as conveniently. However, it obviously contains the product $\mathcal{Y}(A|p)\mathcal{Y}(A|q)$, which is direct because $\mathcal{U}_2^{\oplus}(A|p)$ does not intersect $\mathcal{U}_2^{\oplus}(A|q)$. Hence we wind up with the exact sequence

$$1 \to \frac{\mathcal{Y}(A|p,q)}{\mathcal{Y}(A|p)\mathcal{Y}(A|q)} \to \frac{\mathcal{U}_2^{\oplus}(A|p)}{\mathcal{Y}(A|p)} \times \frac{\mathcal{U}_2^{\oplus}(A|q)}{\mathcal{Y}(A|q)} \to \frac{\mathcal{U}_2^{\oplus}(A)}{\mathcal{Y}(A)} \to \frac{\mathcal{L}(\xi)}{\mathcal{Y}(\xi)} \to 1\,. \tag{9.6}$$

Our aim is to study $\mathcal{U}_2^{\oplus}(A)/\mathcal{Y}(A)$ by analysing the other terms of this sequence. The central object of attention will be the map

$$\Xi_n : \quad \frac{\mathcal{U}_2^{\oplus}(A|p)}{\mathcal{Y}(A|p)} \times \frac{\mathcal{U}_2^{\oplus}(A|q)}{\mathcal{Y}(A|q)} \quad \longrightarrow \quad \frac{\mathcal{U}_2^{\oplus}(A)}{\mathcal{Y}(A)}\,. \tag{9.7}$$

We shall see, among other things, that Ξ_n is bijective whenever $(p-1, q-1) \leq 2$ and that, in general, its kernel and cokernel tend to be comparatively small.

9.2 Even order

As one would expect, the case $q = 2$ requires special treatment, which in this instance is particularly easy. We shall use this subsection to get it out of the way, and at the same time gather some experience for later.

Lemma 9.1. *For $n = 2p$, the map Ξ_n is bijective.*

Proof. Since $\mathcal{Y}(A|q) = \{1\}$ and $\mathcal{Y}(A|p,q) = \mathcal{Y}(A|p)$, the kernel of Ξ_n as shown in the sequence (9.6) is trivial. Now let us find $\mathcal{L}(\xi)$. Since $\xi = -\zeta$, we have

$$1 - \xi = \frac{1-\zeta^2}{1-\zeta} = (1-\zeta)^{\tau_2 - 1}\,, \tag{9.8}$$

where $\tau_2 \in G_p$ is the automorphism $\zeta \mapsto \zeta^2$. In other words, every element of $\mathcal{U}^{\oplus}(\xi)$ has the form $\xi^a(1-\zeta)^\delta$ with $\delta \in \Delta(G_p)$. To show that $\mathcal{L}(\xi) = \mathcal{Y}(\xi)$, it suffices to prove that such a unit cannot be lifted to $\mathcal{U}_2^{\oplus}(A)$ unless $\delta \in \Delta^2(G_p)$.

Indeed, if there is a $v(x) \in \mathcal{U}_2^{\oplus}(A)$ such that $v(\xi) = \xi^a(1-\zeta)^\delta$, we also have $v(x^2) = \zeta^{2a}(1-\zeta^2)^\delta$. This means that $\zeta^{2a}(1-\zeta^2)^\delta$ is liftable to $\mathcal{U}_2^{\oplus}(A_p)$, whence $\delta \in \Delta^2(G_p)$ — cf. Lemma 3.1. □

We thus have an isomorphism between $\mathcal{U}_2^{\oplus}(A)/\mathcal{Y}(A)$ and $\mathcal{U}_2^{\oplus}(A|p)/\mathcal{Y}(A|p)$. For any q, we have already seen that the projection $A \to A_p$ identifies $\mathcal{U}_2^{\oplus}(A|p)$ with $\ker_q \mathcal{W}(A_p)$, the kernel of the natural map $\mathcal{W}(A_p) \to \mathcal{U}_1 \mathbb{F}_q A_p \simeq \mathcal{U}\mathbb{F}_q[\zeta]$. The question is what happens to $\mathcal{Y}(A|p)$ under that identification. If $(q-1, p-1) \leq$

2, the answer is that it goes to $\mathcal{W}(A_p)^{\tau_q - q}$, which is obviously a subgroup of $\ker_q \mathcal{W}(A_p)$ since the automorphism $\tau_q : z \to z^q$ is just the q-th power in $\mathbb{F}_q A_p$. We prove this now for $q = 2$.

Lemma 9.2. *If $n = 2p$, the projection $A \to A_p$ maps $\mathcal{Y}(A|p)$ onto $\mathcal{W}(A_p)^{\tau_2 - 2}$.*

Proof. Any element of $\mathcal{Y}(A)$ is of the form $u(x) = w_\alpha(x) w_\gamma(x^2)$. A glance at Proposition 2.3 shows that the relation (9.8) immediately implies

$$w_\alpha(\xi) = w_\alpha(\zeta)^{\tau_2 - 1} \tag{9.9}$$

for any $\alpha \in \Delta^2(H_n)$. To get $u(x) \in \mathcal{Y}(A|p)$, i.e., $u(\xi) = 1$, we must have $1 = w_\alpha(\xi) w_\gamma(\zeta^2) = w_\alpha(\zeta)^{\tau_2 - 1} w_\gamma(\zeta)^{\tau_2}$. Since ζ is a p-th root of unity, it follows that $\gamma\tau_2 = \alpha(1 - \tau_2)$ in $\Delta^2(H_p)$; in particular, $w_\gamma(z)^{\tau_2} = w_\alpha(z)^{1 - \tau_2}$.

Now let $x \mapsto z$ be the map $A \to A_p$ mentioned in the lemma. Then the image of $u(x)$ is just $u(z) = w_\alpha(z) w_\gamma(z)^{\tau_2} = w_\alpha(z)^{2 - \tau_2}$. □

At this point, $c(A)$ is seen to equal the index $\big[\ker_2 \mathcal{W}(A_p) : \mathcal{W}(A_p)^{\tau_2 - 2}\big]$, which remains to be computed. Since the required calculation is the same for any q, we shall state the general result.

Lemma 9.3. *Let K be a group of odd prime order p, and q be a prime distinct from p. Moreover, let $\mathrm{im}_q \mathcal{W}(K)$ denote the image of the natural map $\mathcal{W}(K) \to \mathcal{U}\mathbb{F}_q K$. Then*

$$(q-1)\big[\ker_q \mathcal{W}(K) : \mathcal{W}(K)^{\tau_q - q}\big] = \big[\mathcal{U}_1^+ \mathbb{F}_q K : \mathrm{im}_q \mathcal{W}(K)\big] \ .$$

Proof. Since $\mathrm{im}_q \mathcal{W}(K) \simeq \mathcal{W}(K)/\ker_q \mathcal{W}(K)$, the lemma amounts to saying

$$(q-1)\big[\mathcal{W}(K) : \mathcal{W}(K)^{\tau_q - q}\big] = |\mathcal{U}_1^+ \mathbb{F}_q K| \, . \tag{9.10}$$

Let f be the order of $\tau_q \in H = H_p$, and define g by $fg = |H|$. We shall prove the lemma by showing that each side of (9.10) is equal to $(q^f - 1)^g$.

For the left side, recall that $\mathcal{W}(K) \simeq \mathbb{Z}H/\mathcal{N}(H)$, where $\mathcal{N}(H) \in \mathbb{Z}H$ is the ideal generated by $\Sigma(H)$. By analysing the cokernels of the endomorphism $\tau_q - q$ acting on the sequence $\mathcal{N}(H) \to \mathbb{Z}H \to \mathcal{W}(K)$, one finds that the maps

$$\mathcal{W}(K) \xrightarrow{\tau_q - q} \mathcal{W}(K) \qquad \text{and} \qquad \frac{\mathcal{N}(H)}{(1-q)\mathcal{N}(H)} \longrightarrow \frac{\mathbb{Z}H}{(\tau_q - q)\mathbb{Z}H} \tag{9.11}$$

have isomorphic cokernels — whence it follows that

$$(q-1)\big[\mathcal{W}(K) : \mathcal{W}(K)^{\tau_q - q}\big] = \big[\mathbb{Z}H : (\tau_q - q)\mathbb{Z}H\big] \, . \tag{9.12}$$

The right hand side of this equality is just the determinant of the operator $(q - \tau_q)$ on $\mathbb{Z}H$, i.e., the characteristic polynomial of τ_q evaluated at q. But 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_q.

The second equality comes from the decomposition of q in the Dedekind ring $\mathbb{Z}[\theta]$, where $\theta = \zeta + \zeta^{-1}$. Its Galois group is H, its Frobenius automorphism given by $\tau_q : \zeta \mapsto \zeta^q$, and its degree of inertia is therefore f. Now $\mathbb{F}_q K \simeq \mathbb{F}_q \oplus \mathbb{F}_q[\zeta]$ implies $\mathcal{U}_1^+ \mathbb{F}_q K \simeq \mathcal{U}\mathbb{F}_q[\theta]$, and hence $\left|\mathcal{U}_1^+ \mathbb{F}_q K\right| = (q^f - 1)^g$, because g is the number of simple components of the semi-simple ring $\mathbb{F}_q[\theta]$. □

Remark. Obviously, $\left[\mathcal{U}_1^+ \mathbb{F}_q K : \mathrm{im}_q \mathcal{W}(K)\right]$ can also be computed in $\mathbb{F}_q[\zeta]$, namely as $\left[\mathcal{U}\mathbb{F}_q[\theta] : \mathrm{im}_q \mathcal{W}(\zeta)\right]$. Remembering that

$$\mathcal{U}^{\oplus}(\zeta) = (\zeta^{-1} - \zeta)^{\Delta(G_p)} \quad \text{and} \quad \mathcal{W}(\zeta) = (\zeta^{-1} - \zeta)^{\Delta^2(G_p)}\,, \tag{9.13}$$

we obtain

$$\mathrm{im}_q \mathcal{U}^{\oplus}(\zeta)^{q-1} = \mathrm{im}_q \mathcal{U}^{\oplus}(\zeta)^{\tau_q - 1} \subseteq \mathrm{im}_q \mathcal{W}(\zeta)\,, \tag{9.14}$$

because the q-th power is the automorphism τ_q in $\mathbb{F}_q[\zeta]$. For $q - 1 = 1$, this is even simpler, giving $\mathrm{im}_2 \mathcal{W}(\zeta) = \mathrm{im}_2 \mathcal{U}^{\oplus}(\zeta)$.

For $q = 2$, we therefore have $c(A)$ equal to the "defect" $d_2(\zeta)$, which measures by how much the circular units $\mathcal{U}^{\oplus}(\zeta)$ in $\mathbb{Z}[\zeta]$ fall short of generating $\mathcal{U}\mathbb{F}_2[\theta]$. To calculate it, choose an integer c such that $\zeta \mapsto \zeta^c$ generates H_p, and consider the unit $v_c(\zeta) = \zeta^{(1-c)/2}(1 + \zeta + \ldots + \zeta^{c-1})$, together with its H_p-conjugates, all read in $\mathbb{F}_2[\zeta]$. The question is how much of $\mathcal{U}\mathbb{F}_2[\theta]$ these units generate. For $p < 100$, this turns out to be all of $\mathcal{U}\mathbb{F}_2[\theta]$, except when $p = 37$, 73, and 97 — where the shortfall is $d_2(\zeta) = 3$, 7, and 7, respectively.

9.3 Odd order

The case of odd order $n = pq$ has been thoroughly dealt with in [H9]. Instead of reproducing detailed proofs, we shall take this opportunity to outline the main results, and give a rough idea of how they come about. We shall encounter the same questions as in the last paragraph — kernel and cokernel of Ξ_n, as well as the index $\left[\mathcal{U}_2^{\oplus}(A|p) : \mathcal{Y}(A|p)\right]$ and its relation to the defect $d_q(\zeta_p)$ — but we now approach them in more or less the opposite order.

The cheapest and most of obtrusive of the numerical invariants in this story is the greatest common divisor m of $|H_p| = (p-1)/2$ and $|H_q| = (q-1)/2$. It turns out that, for $m = 1$, everything happens as before: Ξ_n is an isomorphism, and $\left[\mathcal{U}_2^{\oplus}(A|p) : \mathcal{Y}(A|p)\right]$ equals the defect $d_q(\zeta_p)$. In the notation of the proof of Lemma 9.3, the latter is the index between the first two of the following unit groups

$$\acute{\mathcal{U}}\mathbb{F}_q[\theta] \supseteq \mathrm{im}_q \acute{\mathcal{U}}^{\oplus}(\zeta) \supseteq \mathrm{im}_q \mathcal{W}(\zeta)\,, \tag{9.15}$$

where the acute accent means restriction to elements with trivial H_p-norm. Since this norm maps $\mathcal{U}\mathbb{F}_q[\theta]$ onto $\mathbb{F}_q^{\times}$, restriction to its kernel gets rid of the factor

$(q-1)$ in Lemma 9.3, and produces the formula

$$\big[\ker_q \mathcal{W}(K) : \mathcal{W}(K)^{\tau_q - q}\big] = d_q(\zeta) e_q(\zeta)\,, \tag{9.16}$$

where $e_q(\zeta)$ is the index between the last two groups in the filtration (9.15).

Lemma 9.4. $\mathrm{im}_q \acute{\mathcal{U}}^{\oplus}(\zeta)/\mathrm{im}_q \mathcal{W}(\zeta)$ *is a cyclic group whose order* $e_q(\zeta)$ *divides* m.

Proof. Since the cyclic group $\Delta(G_p)/\Delta^2(G_p)$ is annihilated by $(p-1)$, so are its homomorphic images $\mathcal{U}^{\oplus}(\zeta)/\mathcal{W}(\zeta)$ and $\mathrm{im}_q \mathcal{U}^{\oplus}(\zeta)/\mathrm{im}_q \mathcal{W}(\zeta)$. In view of (9.14), the latter is also killed by $(q-1)$, hence by $(p-1, q-1) = 2m$. But $\mathrm{im}_q \acute{\mathcal{U}}^{\oplus}(\zeta)$ is of index 2 in the group $\mathrm{im}_q \mathcal{U}^{\oplus}(\zeta)$, which is mapped onto $\{\pm 1\}$ by the H_p-norm. □

The next problem is to connect the left hand side of (9.16) to the index $\big[\mathcal{U}_2^{\oplus}(A|p) : \mathcal{Y}(A|p)\big]$. Of course, the projection $A \to A_p$ always maps $\mathcal{U}_2^{\oplus}(A|p)$ to $\ker_q \mathcal{W}(A_p)$, by virtue of the pull-back (9.3), but what does it do to $\mathcal{Y}(A|p)$? Again the answer involves m.

Lemma 9.5. *The projection* $A \to A_p$ *maps* $\mathcal{Y}(A|p)$ *bijectively onto the* w*-image of* $\Delta^2(G_p) \cap (\tau_q - q)\Delta(G_p)$ *in* $\mathcal{W}(A_p)$. *This group contains* $\mathcal{W}(A_p)^{\tau_q - q}$ *as a subgroup of index* m *with cyclic factor group.*

The proof of this result occupies Section 4 of [H9]. By way of illustration, we shall describe a typical element of the group in question. Let $\tau_c : \zeta \mapsto \zeta^c$ have order $2m$ in G_p, and put $\gamma = (\tau_c - 1)(q - \tau_q) \in \Delta(G_p)$. Since $2m \mid q-1$, we clearly have $\gamma = (\tau_c - 1)\big[(q-1) + (1-\tau_q)\big]$ in $\Delta^2(G_p)$, and hence get $w_\gamma(z) \in \mathcal{W}(A_p)$. Defining $v_c(\zeta)$ as at the end of the last subsection, we can write $w_\gamma(\zeta) = v_c(\zeta)^{q-\tau_q}$, which shows that $w_\gamma(z)$ is in $\ker_q \mathcal{W}(A_p)$.

If $\varepsilon \in \Delta(H_p)$ denotes the image of $m(\tau_c - 1)$, we actually have $\varepsilon \in \Delta^2(H_p)$, because in H_p the order of τ_c is only m. With γ read in $\Delta^2(H_p)$, we therefore get the equation $m\gamma = (q - \tau_q)\varepsilon$, which implies $w_\gamma(z)^m = w_\varepsilon(z)^{q-\tau_q}$. In fact, it can be shown that $w_\gamma(z)$ generates the group mentioned in the lemma, modulo $\mathcal{W}(A_p)^{\tau_q - q}$.

Note that Lemma 9.5 refers *not* to H_p but to G_p, and necessarily so. Indeed, if 4 divides $p-1$ but not $q-1$, the w-image of $\Delta^2(H_p) \cap (\tau_q - q)\Delta(H_p)$ is twice too big. To see this, take τ_c of order $4m$ and define γ as above, but read everything in $\Delta(H_p)$. Then $\gamma \in \Delta^2(H_p)$ and $w_\gamma(z) \in \mathcal{W}(A_p)$.

The reason for this status of G_p is that it occurs as a subgroup of H_n while H_p does not. Remember that $G_n = G_p \times G_q$ and that $H_n = G_n/\langle\star\rangle$. 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. Hence we have

$$G_n = G_q \times G_p \quad \text{and} \quad H_n = \tilde{G}_q \cdot \tilde{G}_p \tag{9.17}$$

with $\tilde{G}_q \cap \tilde{G}_p$ of order 2. Of course, G_n acts on $x = yz$ and $\xi = \eta\zeta$ via this factorisation, and H_n acts on $\mathcal{U}^+(A)$ and $\mathcal{U}^+(\xi)$ in the same way.

The odd order analogue of the relation (9.8) is the *basic G_q-norm relation*

$$(\xi-1)^{s(q)} = (\zeta-1)^{\tau_q-1}\,, \tag{9.18}$$

where $s(q) \in \mathbb{Z}G_n$ denotes the sum over the elements of G_q, and $\tau_q \in G_p$ the obvious automorphism. This relation could equally well be written in terms of $\xi^{-1}-\xi$ and $\zeta^{-1}-\zeta$. For $v_a(\xi) = \xi^{(1-a)/2}(1+\xi+\cdots+\xi^{a-1})$ it translates to

$$v_a(\xi)^{s(q)} = w_\gamma(\zeta) \quad \text{with} \quad \gamma = (\tau_a-1)(\tau_q-1)\,, \tag{9.19}$$

which constitutes a sharpened analogue of (9.9). The main idea in the proof of Lemma 9.5 is to show, using this relation, that every element of $\mathcal{Y}(A|p)$ has the form $w_\alpha(x)w_\gamma(x^q)$, where $\alpha \in \Delta^2(H_n)$ and $\gamma \in \Delta^2(Hp)$ are derived from a single $\delta \in \Delta(\tilde{G}_p)$ by $\alpha = s(q)\delta$ and $\gamma = (\tau_q^{-1}-1)\delta$.

As a consequence of Lemma 9.5, the index $\big[\ker_q\mathcal{W}(K) : \mathcal{W}(K)^{\tau_q-q}\big]$ equals $m\cdot\big[\mathcal{U}_2^{\oplus}(A|p) : \mathcal{Y}(A|p)\big]$, and hence

$$\frac{m}{e_q(\zeta_p)}\cdot\big[\mathcal{U}_2^{\oplus}(A|p) : \mathcal{Y}(A|p)\big] = d_q(\zeta_p)\,. \tag{9.20}$$

Of course, we have an analogous formula with p and q interchanged. Multiplying the two yields an expression for the order of the domain of Ξ_n.

We must now look at its kernel and cokernel. It turns out that, in both of them, the greatest common divisor m'' of the indices $\big[H_p : \langle\tau_q\rangle\big]$ and $\big[H_q : \langle\tau_p\rangle\big]$ plays a role. Obviously m'' is 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.

Lemma 9.6. *The kernel of the map Ξ_n is cyclic of order m''.*

The proof of this fact takes up most of Sections 3 and 5 of [H9]. It analyses the image of an injection

$$\frac{\mathcal{Y}(A|p,q)}{\mathcal{Y}(A|p)\times\mathcal{Y}(A|q)} \quad\longrightarrow\quad \frac{\Delta(H_n)}{s(q)\Delta(\tilde{G}_p)\oplus s(p)\Delta(\tilde{G}_q)}\,, \tag{9.21}$$

induced by mapping the typical element $u(x) = w_\alpha(x)w_\beta(x^p)w_\gamma(x^q)$ of $\mathcal{Y}(A|p,q)$ to its first factor $w_\alpha(x) \in \mathcal{W}(A) \simeq \Delta^2(H_n)$. In view of (9.6), the domain of this morphism is just the kernel of Ξ_n. In the abstract context of Section 3 (*loc. cit.*), the torsion subgroup of the right hand side of (9.21) is shown to be generated by

$$\delta_0 = \frac{|H_p|}{m}s(q) - \frac{|H_q|}{m}s(p)\,, \tag{9.22}$$

and the rest of the argument turns on finding the smallest integer $t>0$ for which $t\delta_0$ lies in the image of the map (9.21). It turns out that $t = m/m''$.

In Section 7 of [H9], the cokernel $\mathcal{L}(\xi)/\mathcal{Y}(\xi)$ of Ξ_n is studied via a filtration

$$\mathcal{L}(\xi) \supseteq \mathcal{L}^\circ(\xi) \supseteq \mathcal{L}^*(\xi) \supseteq \mathcal{Y}(\xi) \tag{9.23}$$

to be defined presently. Since $\mathcal{Y}(\xi)$ consists of units like $w_\alpha(\xi)w_\beta(\eta)w_\gamma(\zeta)$ with $\alpha \in \Delta^2(H_n)$, $\beta \in \Delta^2(H_q)$, and $\gamma \in \Delta^2(H_p)$, any coset of $\mathcal{U}^\oplus(\xi)$ modulo $\mathcal{Y}(\xi)$ has the form

$$(\xi^{-1} - \xi)^{2t} v_a(\xi)v_b(\eta)v_c(\zeta) \cdot \mathcal{Y}(\xi)\,, \tag{9.24}$$

where $v_a(\xi)$ is as described above — cf. (9.19) — with $v_b(\eta)$, $v_c(\zeta)$ built similarly, and $t \geq 0$ an integer. Note that $v_a(\xi) = (\xi^{-1/2} - \xi^{1/2})^{\tau_a - 1}$, etc. The exponent on the first factor in (9.24) is even because of $\star$-symmetry.

In these terms, $\mathcal{L}^\circ(\xi)$ consists of those units in $\mathcal{L}(\xi)$ which can be written with $t = 0$, and $\mathcal{L}^*(\xi)$ of those for which moreover $b = c = 0$ can be assumed. We say "can be" because the product (9.24) is far from unique. The norm relation (9.18), for instance, is equivalent to $(\xi^{-1} - \xi)^{s(q)} = v_q(\zeta)^{\tau_2}$. In turn, this clearly implies

$$(\xi^{-1} - \xi)^{q-1} \;\in\; \mathcal{L}^\circ(\xi)\,, \tag{9.25}$$

which, together with its $s(p)$-counterpart makes $(\xi^{-1} - \xi)^{2m}$ lie $\mathcal{L}^\circ(\xi)$. In other words, $\mathcal{L}(\xi)/\mathcal{L}^\circ(\xi)$ is a cyclic group whose order divides m. So far, we have used only the basic norm relations. When we also take into account that we are dealing with *liftable* units, the gap between $\mathcal{L}(\xi)$ and $\mathcal{L}^\circ(\xi)$ narrows still further.

Lemma 9.7. *$\mathcal{L}(\xi)/\mathcal{L}^\circ(\xi)$ is a cyclic group whose order divides m''.*

Unfortunately, this is not the kind of exact result we got for the kernel of Ξ_n, but only an upper bound. In fact, the proof uses only one aspect of liftabilty, namely that certain Galois norms must be $= 1$. Upper bounds is all we have for the other two indices of the filtration (9.23), too. There we construct explicit group epimorphisms

$$\big[\mathbb{F}_q^\times \cap \mathrm{im}_q\mathcal{U}^\oplus(\zeta)\big] \times \big[\mathbb{F}_p^\times \cap \mathrm{im}_p\mathcal{U}^\oplus(\eta)\big] \longrightarrow \mathcal{L}^\circ(\xi)/\mathcal{L}^*(\xi)$$

$$\text{and} \qquad\qquad G_q^{2e_p(\eta)} \times G_p^{2e_q(\zeta)} \longrightarrow \mathcal{L}^*(\xi)/\mathcal{Y}(\xi)\,. \tag{9.26}$$

Now, $\mathbb{F}_q^\times \cap \mathrm{im}_q\mathcal{U}^\oplus(\zeta)$ is the kernel of the endomorphism $\sigma - 1$ on $\mathrm{im}_q\mathcal{U}^\oplus(\zeta)$, where $\langle\sigma\rangle = H_p$. Hence its order equals that of the cokernel $\mathrm{im}_q\mathcal{U}^\oplus(\zeta)/\mathrm{im}_q\mathcal{W}(\zeta)$, which is $2e_q(\zeta)$ according to the definition following (9.16). On the other hand, the first map in (9.26) is defined in such a way that it kills $(\pm1, \pm1)$. Hence the order of $\mathcal{L}^\circ(\xi)/\mathcal{L}^*(\xi)$ is at most $e_q(\zeta)e_p(\eta)$, while that of $\mathcal{L}^*(\xi)/\mathcal{Y}(\xi)$ is clearly bounded (in the sense of divisibility) by $m^2/e_q(\zeta)e_p(\eta)$. Here is the result.

Lemma 9.8. *The order of the group $\mathcal{L}^\circ(\xi)/\mathcal{Y}(\xi)$ divides m^2.*

Going back to the exact sequence (9.6), and putting together all the pieces of the puzzle, we finally have

Theorem 9.9. $\left[\mathcal{U}_2^{\oplus}(A) : \mathcal{Y}(A)\right]$ *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 $\left[\mathcal{U}_2^{\oplus}(A) : \mathcal{Y}(A)\right] = d_3(\zeta_p)$. This number turns out to be 1 for all $5 \le p \le 101$, except for $p = 61$, where it is a multiple of 44, and for $p = 97$, where it equals 73. Thus $\mathcal{U}_2^{\oplus}(A)/\mathcal{Y}(A)$ is a cyclic group of order 73 when $|A| = 291$. It would be interesting to see a generator, and to check whether 73 divides $|D^+(A)|$.

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 — with the methods described in [H10] — only for $(p-1)(q-1) \le 72$. In these cases we also have $\mathcal{U}_2^{\oplus}(A) = \mathcal{U}_1^{+}(A)$, and the triviality of $c(A)$ therefore 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 $c(A)$ might be $\neq 1$. 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 $e_q(\zeta_p) = m$ for the other five choices of (q, p). By our theorem, $c(A)$ is at most m^2 for these three exceptional groups.

By more carefully studying the kernel of the first map in (9.26), R. Ferguson has bounded $[\mathcal{L}^\circ(\xi) : \mathcal{L}^*(\xi)]$ by $e_q(\zeta)e_p(\eta)m''/m$, and hence $[\mathcal{L}^\circ(\xi) : \mathcal{Y}(\xi)]$ by $m''m$. For our three exceptional A, we therefore have $c(A) \mid m$. A more precise estimate is so far not available, even at this modest level of generality.

References

[AH] Artin, E., Hasse, H., Die beiden Ergänzungssätze zum Reziprozitätsgesetz der l-ten Potenzreste im Körper der l-ten Einheitswurzeln. Hamb. Abh. 6 (1928), 142 - 163

[Bo] Borevich, Z.I., The multiplicative group of a regular local field with a cyclic group of operators (Russian). Izvestia Akad. Nauk. 28 (1964), 707 - 712

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

[B1] Bass, H., The Dirichlet unit theorem, induced characters, and Whitehead groups of finite groups. Topology 4 (1966), 391 - 410

[B2] Bass, H., Algebraic K-Theory. W.A.Benjamin, N.Y. (1968)

[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

[Fra] Franz, W., Über die Torsion einer Überdeckung. J. reine u. angew. Math. 173 (1935), 245 - 254

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

[GH] Gamst, J., Hoechsmann, K., Kummer's Lemma for cyclic 2-groups. Hamb. Abh. (to appear 1995)

[Ha] Hasse, H., Zahlentheorie. Akademie-Verlag, Berlin (1963)

[Hi] Higman, G., The units of group rings. Proc. Lon. Math. Soc. (2) 46 (1940), 231 - 248

[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] — , Norms and traces in p-adic abelian group rings. Arch. d. Math. 51 (1988), 50 - 54
[H4] — , On the Bass-Milnor Index of abelian p-groups. Contemporary Math. 93 (1989), 179 - 195
[H5] — , Généralisation d'un lemme de Kummer. Can. Math. Bull. 32 (1989), 486 - 489
[H6] —, Local units and circular index in abelian p-group rings. J. Pure and Appl. Alg. 82 (1992), 253 - 272
[H7] —, Exotic units in group rings of rank p^2. Arch. d. Math. 58 (1992), 239 - 247
[H8] —, Constructing units in commutative group rings. Manuscr. Math. 75 (1992), 5 - 23
[H9] —, Units in integral group rings for order pq. Can. J. Math. 47 (1995), 113 - 131
[H10] —, Cyclotomic units over finite fields. Rendiconti Palermo II 44 (1995), 5 - 20
[HR1] —, Ritter, J., Logarithms and units in p-adic abelian group rings. Arch. d. Math. 49 (1987), 23 - 28
[HR2] —, —, Constructible units in abelian p-group rings. J. Pure and Appl. Alg. 68 (1990), 325 - 339
[HR3] —, —, The Artin-Hasse Power Series and p-adic group rings. J. Numb. Th. 39 (1991), 117 - 128
[HS1] —, Sehgal, S.K., Integral group rings without proper units. Can. Math. Bull. 30(1) (1987), 36 - 41
[HS2] —, —, Units in regular elementary abelian group rings. Arch. d. Math. 47 (1986), 413 - 417
[HS3] —, —, 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
[Iw] Iwasawa, K., A note on class numbers of algebraic number fields. Hamb. Abh. 20 (1956), 257 - 258
[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
[KM] Kervaire, M.A., Murthy, M.P., On the projective class group of cyclic groups of prime power order. Com. Helv. 52 (1977), 415 - 452
[L1] Lang, S., Algebraic Number Theory. Addison-Wesley, N.Y.(1970)
[L2] Lang, S., Cyclotomic Fields II. Springer Verlag, N.Y. (1982)
[Re] Reiner, I., Maximal Orders. Academic Press, N.Y. (1975)
[S1] Sehgal, S.K., Topics in Group Rings. Marcel Dekker, N.Y. (1978)
[S2] Sehgal, S.K., Units in integral group rings. J.Wiley, N.Y. (1993)
[Si] Sinnott, W., On the Stickelberger ideal and the circular units of a cyclotomic field. Ann. Math. 108 (1978), 107 - 134
[Ul] Ullom, S., Class groups of cyclotomic fields and group rings. J. Lon. Math. Soc. 17 (1978), 231 - 239
[Wa] Washington, L., Introduction to Cyclotomic Fields. Springer Verlag, N.Y. (1982)