JOURNAL OF NUMBER THEORY **30**, 375–381 (1988)

Units in Regular Abelian p-Group Rings

K. HOECHSMANN

University of British Columbia, Vancouver, British Columbia, Canada V6T 1W5

AND

S. K. SEHGAL

University of Alberta, Edmonton, Alberta, Canada T6G 2E1

Communicated by H. Zassenhaus

Received May 20, 1987

0. INTRODUCTION

An element of the group ring $R[A]$, of some finite abelian group A of odd order over a commutative ring R, will be called *symmetric*, if it is left fixed by the involution on $R[A]$ induced by $a \to a^{-1}$ $(a \in A)$. One of the basic facts about units in $\mathbb{Z}[A]$ is that $U_1\mathbb{Z}[A] = AU_*\mathbb{Z}[A]$ and $U_*\mathbb{Z}[A]$ is torsion-free (cf. [2, Lemma 2.6]), where generally U_1 denotes the units of augmentation one, and U_* the subgroup of symmetric elements therein.

In this note, we investigate the images of three natural maps for abelian p-groups, A (p *odd*):

(1) $U_*\mathbb{Z}[A] \to U_*\mathbb{Z}_p[A]$, where $\mathbb{Z}_p$ denotes p-adic integers,

(2) $\prod_C U_*\mathbb{Z}[C] \to U_*\mathbb{Z}[A]$, where C runs over cyclic subgroups, and Π is direct,

(3) $U_*\mathbb{Z}[A_1] \to U_*\mathbb{Z}[A_2]$, where $A_1 \to A_2$ is surjective.

We shall make heavy use of the main result of [5], which we restate below as Lemma 0. It studies the p-adic counterparts to (2) and (3), restricted to the group $U'_*\mathbb{Z}_p[A]$ of those units whose Galois norm is 1 in each Wedderburn component. (Note that the scarcity of rational units makes $U_*\mathbb{Z}[A] = U'_*\mathbb{Z}[A]$.)

LEMMA 0. (a) *$\prod_C U'_*\mathbb{Z}_p[C] \to U'_*\mathbb{Z}_p[A]$ is surjective.*

(b) *If $A_1 \to A_2$ is surjective, so is $U'_*\mathbb{Z}_p[A_1] \to U'_*\mathbb{Z}_p[A_2]$.*

0022-314X/88 $3.00

The globalization of these statements does not have much hope unless p is a *regular* prime, which means that p does not divide the class number of the pth roots of unity, so our Theorems 1, 2, and 3 depend on that assumption.

In Section 1, we study the analogue of (1) for cyclotomic fields. Section 2 deals with (1) and (3) for cyclic p-groups, and Section 3 contains the theorems.

1. Cyclotomic Fields

For an odd prime number p and an abelian group X (written additively), let $\bar{X}$ denote the group X/pX and $\hat{X}$ the $\mathbb{Z}_p$-module $X \otimes \mathbb{Z}_p$, the tensor product being over $\mathbb{Z}$. Our first task is to show that the inclusion $\mathbb{Z} \to \mathbb{Z}_p$ induces an injection $\bar{U}(\mathbb{Z}[\zeta]) \to \bar{U}(\mathbb{Z}_p[\zeta])$, if p is regular, and ζ is a p^mth root of 1. For $m=1$, this is a special case of Kummer's Lemma (cf. [1, V.6, Theorem 3]).[1] The following two lemmas are variations on well-known themes: the first one is due to Iwasawa [6], the second sometimes appears in class field theoretic proofs of Kummer's Lemma (cf. [8, pp. 80–81]).

For brevity we shall use the word *p-extension* to mean a finite Galois field-extension K/k of p-power degree, and call a number field K *p-ample*, if it has an unramified p-extension. By class field theory, which we wish to avoid, this is equivalent to saying that p divides the class number of K; we shall ignore this connection, in order to situate our arguments in as elementary a context as possible.

LEMMA 1. *Let K/k be an abelian p-extension of number fields. Suppose that a single prime divisor v of k ramifies in K, and is totally ramified. Then, K is p-ample if and only if k is.*

Proof. Let L/K be an unramified Galois extension of degree p. Its Galois closure M over k is a p-extension unramified over K. Since $G = \mathrm{Gal}(M/k)$ is a p-group and $G_0 = \mathrm{Gal}(M/K)$ is normal in G, G_0 has a subgroup H of index p which is normal in G and such that G/H is still abelian.

The fixed field E of H is an abelian p-extension of k. Therefore, the prime divisors of v in E all have the ame inertia group T in $\mathrm{Gal}(E/k)$. If w is the prime under v in k, its ramification index in E is $[K:k]$, because E/K is unramified. Hence $|T| = [K:k]$ and $[F:k] = p$, if F is the fixed field of T. F/k is unramified, because no prime other than w ramifies in E/k. The converse is obvious.

[1] Kummer's Lemma says that the composite $\bar{U}\mathbb{Z}[\zeta] \to \bar{U}\mathbb{Z}_p[\zeta] \to \mathbb{F}_p[\zeta]^{\times}$ is injective, where $\mathbb{F}_p[\zeta]$ denotes the artinian ring $\mathbb{Z}[\zeta]/p\mathbb{Z}[\zeta] = \mathbb{F}_p[x]/(1 + x + \cdots + x^{p-1})$.

LEMMA 2. *Let K be a number field containing the pth roots of unity and such that $K_p = \mathbb{Q}_p \otimes_{\mathbb{Q}} K$ is a field. Consider the inclusion $U_K \to U_{K_p}$ of units (in the respective rings of integers).*

(a) *If $\bar{U}_K \to \bar{U}_{K_p}$ is not injective then K is p-ample.*

(b) *Conversely, if p is prime to the class number of K and $\bar{U}_K \to \bar{U}_{K_p}$ is injective, K is not p-ample.*

Proof. (a) Let $\varepsilon \in U_K \backslash U_K^p$ become a pth power in U_{K_p}. Then $f(x) = x^p - \varepsilon$ splits into p factors in K_p, and the prime divisor of p in K splits completely in $E = K(\eta)$, where $\eta^p = \varepsilon$. The different of E/K divides $p\eta^{p-1}$, hence no other finite prime of K can be ramified in E. The infinite primes are already complex. Hence E/K is an unramified p-extension.

(b) Let E/K be an unramified Galois extension of degree p. By Kummer Theory, $E = K[\theta]$, where $\theta^p = t \in K$. For every discrete valuation v_E of E we have $v_E(t) = v_K(t) = p v_E(\theta)$; i.e., $v_K(t)$ is always divisible by p, and the principal divisor (t) is a pth power. Since p does not divide the class number, this means that (t) is a pth power of a principal divisor (s), i.e., $t = \varepsilon s^p$, with $\varepsilon \in U_K \backslash U_K^p$. Now $E = K[\eta]$, where $\eta^p = \varepsilon$. The prime divisor above p in K cannot remain inert in E, since $x^p - \varepsilon$ would generate a purely inseparable extension on the residue class field. Hence it splits in E, i.e., $x^p - \varepsilon$ splits in K_p, and ε becomes a pth power there; $\bar{U}_K \to \bar{U}_{K_p}$ is not injective.

Remark. Part (b) replaces a reference to the Hilbert class field, which would render it utterly trivial.

PROPOSITION 1. *If ζ denotes a p^mth root of* 1, *$\bar{U}(\mathbb{Z}[\zeta]) \to \bar{U}(\mathbb{Z}_p[\zeta])$ is injective, provided that p is regular.*

Proof. If not, $\mathbb{Q}[\zeta]$ would be p-ample by Lemma 2(a). Then, by Lemma 1, so would be the field of pth roots of unity. By Lemma 2(b), this would contradict Kummer's Lemma.

We now shift to the subfields $\mathbb{Q}[\zeta]_*$ and $\mathbb{Q}_p[\zeta]_*$ left fixed by the automorphism $\zeta \to \zeta^{-1}$. Their units will be denoted by subscript asterisks. If $n = [\mathbb{Q}[\zeta]_* : \mathbb{Q}]$, Dirichlet's Unit Theorem implies that $U_*(\mathbb{Z}[\zeta])$ is a free $\mathbb{Z}$-module of rank $n-1$. By an analogous local result (cf. [3, II.15.5]), $U_*(\mathbb{Z}_p[\zeta])$ is a free $\mathbb{Z}_p$-module of rank n. The inclusion $U_*(\mathbb{Z}[\zeta]) \to U_*(\mathbb{Z}_p[\zeta])$ takes $U_*(\mathbb{Z}[\zeta])$ into the group $U'_*(\mathbb{Z}_p[\zeta])$ of units of Galois-norm 1. We claim that the image is dense.

PROPOSITION 2. *If p is regular, the map λ: $\hat{U}_*(\mathbb{Z}[\zeta]) \to U'_*(\mathbb{Z}_p[\zeta])$ is an isomorphism.*

Proof. By Proposition 1, $\bar{U}_*(\mathbb{Z}_p[\zeta]) \to \bar{U}'_*(\mathbb{Z}_p[\zeta])$ is injective and hence an isomorphism, since both are vector spaces of dimension $n-1$ over $\mathbb{F}_p$, the field of p elements. Nakayama's Lemma now implies that λ is surjective. Since we are dealing with free $\mathbb{Z}_p$-modules of equal rank, it is also injective.

2. Cyclic Groups

Let C be a cyclic group of order p^m $(m>0)$, and consider the fibre product

$$\begin{array}{ccc} U_*\mathbb{Z}[C] & \longrightarrow & U_*\mathbb{Z}[\zeta] \\ {\scriptstyle\pi}\downarrow & & \downarrow{\scriptstyle\rho} \\ U_*\mathbb{Z}[C/C_p] & \longrightarrow & U_*\mathbb{F}_p[C/C_p] \end{array}$$

in which ζ is a p^mth root of 1, $C_p = \{c \in C \mid c^p = 1\}$, π comes from the canonical map $C \to C/C_p$, and ρ means reduction modulo $\zeta^{p^{m-1}} - 1$. This is easily derived from the corresponding diagram for the respective rings, which is easily seen to be a fibre product (cf. [7, Section 1]). We record its properties in the exact sequence

$$1 \to U_*\mathbb{Z}[C] \to U_*\mathbb{Z}[C/C_p] \times U_*\mathbb{Z}[\zeta] \to U_*\mathbb{F}_p[C/C_p],$$

in which the last arrow is the quotient of π and ρ. Note that the last term is a finite p-group. In particular, it is a natural $\mathbb{Z}_p$-module, and the other terms can be tensored with $\mathbb{Z}_p$ (being free over $\mathbb{Z}$) without changing the exactness. An entirely analogous fibre product and sequence exists for $U'_*\mathbb{Z}_p[-]$ and can even be restricted to elements whose norm under $G = \mathrm{Aut}(C)$ is 1.

Thus we obtain a map of exact sequences

$$\begin{array}{ccccccc} 1 & \longrightarrow & \hat{U}_*\mathbb{Z}[C] & \longrightarrow & \hat{U}_*\mathbb{Z}[C/C_p] \times \hat{U}_*\mathbb{Z}[\zeta] & \longrightarrow & U_*\mathbb{F}_p[C/C_p] \\ & & \downarrow & & \downarrow & & \downarrow \\ 1 & \longrightarrow & U'_*\mathbb{Z}_p[C] & \longrightarrow & U'_*\mathbb{Z}_p[C/C_p] \times U'_*\mathbb{Z}_p[\zeta] & \longrightarrow & U_*\mathbb{F}_p[C/C_p] \end{array}$$

in which one of the components of the middle arrow is an isomorphism by Proposition 2, if p is regular. Induction yields our next result.

LEMMA 3. *If C is a cyclic p-group for regular p, $\hat{U}_*\mathbb{Z}[C] \to U'_*\mathbb{Z}_p[C]$ is an isomorphism.*

Together with Lemma 0(b), this yields another proof of Theorem 1.3 in [7].

COROLLARY. *If p is regular, a surjection $C_1 \to C_2$ of cyclic p-groups induces a surjection $U_*\mathbb{Z}[C_1] \to U_*\mathbb{Z}[C_2]$.*

Proof. By induction it suffices to show this for $C \to C/C_p$. The cokernel of $\pi: U_*\mathbb{Z}[C] \to U_*\mathbb{Z}[C/C_p]$ is a subgroup of $U_*\mathbb{F}_p[C/C_p]$, a finite p-group. If π were not surjective, neither would $\hat{\pi}$ be. By Lemma 3 this would contradict Lemma 0(b).

5. ABELIAN GROUPS

Now let A be a finite p-group, and consider the commutative square

$$\begin{array}{ccc} \prod_C \hat{U}_*\mathbb{Z}[C] & \longrightarrow & \hat{U}_*\mathbb{Z}[C] \\ \downarrow & & \downarrow \\ \prod_C U'_*\mathbb{Z}_p[C] & \twoheadrightarrow & U'_*\mathbb{Z}_p[A] \end{array}$$

Here C runs over all cyclic subgroups of A, and U'_* denotes units of G-norm 1, where $G = (\mathbb{Z}/p^m\mathbb{Z})^\times$ for m large enough to make $A^{p^m} = \{1\}$. Since $U_*\mathbb{Z}_p[-]$ has no $\mathbb{Z}_p$-torsion (cf., for instance, [5] or [3, II.15.5]) it does not matter if m is taken too large. The bottom arrow is surjective by Lemma 0.

THEOREM 1. *If p is regular, $\hat{U}_*\mathbb{Z}[A] \to U'_*\mathbb{Z}_p[A]$ is an isomorphism.*

Proof. The surjectivity is immediately obvious from Lemmas 0 and 3, and the commutative square above. The injectivity is again due to equality of ranks, which can be seen as follows.

The Wedderburn decompositions of $\mathbb{Q}[A]$and $\mathbb{Q}_p[A]$ are completely parallel, involving cyclotomic fields $\mathbb{Q}[\zeta_\varphi]$ and $\mathbb{Q}_p[\zeta_\varphi]$ corresponding to rational characters φ of A. The ranks of $U_*\mathbb{Z}[A]$ and $U_*\mathbb{Z}_p[A]$ are equal to those of the units in the maximal orders of $\mathbb{Q}[A]_*$ and $\mathbb{Q}_p[A]_*$, respectively. For each non-trivial φ, $U_*\mathbb{Z}[\zeta_\varphi]$ has rank one less than $U_*\mathbb{Z}_p[\zeta_\varphi]$, i.e., equal to that of $U'_*\mathbb{Z}_p[\zeta_\varphi]$, the kernel of the Galois norm. In the composite inclusion

$$U_*\mathbb{Z}[A] \to U'_*\mathbb{Z}_p[A] \to \prod_{\varphi \neq 1} U'_*\mathbb{Z}_p[\zeta_\varphi]$$

the two end-terms have therefore equal rank.

THEOREM 2. *If p is regular, the cokernel of $\prod_C U_*\mathbb{Z}[C] \to U_*\mathbb{Z}[A]$, as C runs over all cyclic subgroups of A, has no p-primary component.*

Proof. Such a component would survive the tensoring with $\mathbb{Z}_p$ and therefore show up in the $\hat{U}_*$-context, which is impossible by Lemas 0 and 3, again because of our commutative square.

We can now globalize Lemma 0(b). For its proof we need to consider the group $U^1(A)$ consisting of certain units in the maximal order of $\mathbb{Q}A$, namely those which are $\equiv 1$ modulo the ideal generated by the augmentation ideal $\Delta\mathbb{Z}A$.

THEOREM 3. *Let $\pi A_1 \twoheadrightarrow A_2$ be a surjection of abelian p-groups for regular p. Then the induced map $U_*\mathbb{Z}[A_1] \to U_*\mathbb{Z}[A_2]$ is surjective.*

Proof. Let $U_*(A)$ be the unit-group of the maximal order of $\mathbb{Q}[A]$. It is not hard to see that $U_*\mathbb{Z}[A]$ has p-power index in $U_*(A)$ (cf. Lemma 4 below). Consider the commutative square

$$\begin{array}{ccc} U_*\mathbb{Z}[A_1] & \longrightarrow & U_*^1(A_1) \\ \downarrow & & \downarrow \\ U_*\mathbb{Z}[A_2] & \longrightarrow & U_*^1(A_2) \end{array}$$

The horizontal arrows are inclusions of the p-power index. The right vertical map is a surjection. Indeed, the characters of A_2 form (via π) a subgroup of those of A_1, and the map in question is just the projection (in the Wedderburn decomposition) onto those components. It follows that $U_*\mathbb{Z}[A_1]$ has p-power index in $U_*\mathbb{Z}[A_2]$, and if that were non-trivial, then so would be the cokernel of $\hat{U}_*\mathbb{Z}[A_1] \to \hat{U}_*\mathbb{Z}[A_2]$. By Theorem 1 and Lemma 0(b), this cannot happen in p is regular.

To complete the argument we still have to establish the following general lemma.

LEMMA 4. *If p is any prime and A is a finite abelian p-group, $U_1\mathbb{Z}[A]$ has p-power index in $U^1(A)$.*

Proof. We have the containments

$$\begin{array}{ccccc} U_1\mathbb{Z}[A] & \longrightarrow & U_1\mathbb{Z}_p[A] & \longrightarrow & \prod_\varphi U^1\mathbb{Z}_p[\zeta_\varphi] \\ & & & & \uparrow \\ & & & & u \in \prod_\varphi U^1\mathbb{Z}[\zeta_\varphi] \end{array}$$

in the notation of Theorem 1. Let $u \in U^1(A)$ in the maximal order of $\mathbb{Q}[A]$.

Then, since $\prod_\varphi U_1 \mathbb{Z}_p[\zeta_\varphi]$ is a $\mathbb{Z}_p$-module (cf. [3, II.15.5]), $u^{p^m} \in \mathbb{Z}_p[A]$ for some m. Moreover, $|A| u^{p^m} \in \mathbb{Z}[A]$ as the maximal order of $\mathbb{Q}[A]$ equals $\sum_\varphi e_\varphi \mathbb{Z}[A]$, $e_\varphi^2 = e_\varphi$ and e_φ have $|A|$ as denominator. Hence $u^{p^m} \in \mathbb{Z}[A]$, proving the lemma.

References

1. Z. I. Borevich and I. R. Shafarevich, "Number Theory," Academic Press, New York, 1966.
2. G. Cliff, S. K. Sehgal, and A. Weiss, Units of integral rings of metabelian groups, *J. Algebra* **73** (1981), 167–185.
3. H. Hasse, "Zahlentheorie," Adademie Verlag, Berlin, 1963.
4. K. Hoechsmann and S. K. Sehgal, Units in regular elementary abelian group rings, *Arch. Math.* **47** (1986), 413–417.
5. K. Hoechsmann, Norms and traces in p-adic abelian group rings, *Arch. Math.*, to appear.
6. K. Iwasawa, A note on class numbers of algebraic number fields, *Abh. Sem. Hamb.* **20** (1956), 257–258.
7. M. A. Kervaire and M. P. Murthy, On the projective class group of cyclic groups of prime power order, *Com. Helvet.* **52** (1977), 415–452.
8. L. Washington, "Introduction to Cyclotomic Fields," Springer-Verlag, New York, 1982.