Canad. Math. Bull. Vol. **30** (1), 1987

INTEGRAL GROUP RINGS WITHOUT PROPER UNITS

BY
K. HOECHSMANN AND S.K. SEHGAL

ABSTRACT. If A is an elementary abelian p-group and C one of its cyclic subgroups, the integral group rings ZA contains, of course, the ring ZC. It will be shown below, for A of rank 2 and p a *regular* prime, that every unit of ZA is a product of units of ZC, as C ranges over all cyclic subgroups.

1. **Introduction**. If A is an elementary abelian p-group and C one of its cyclic subgroups, the integral group ring $\mathbf{Z}A$ contains, of course, the ring $\mathbf{Z}C$. It will be shown below, for A of rank 2 and p a *regular* prime, that every unit of $\mathbf{Z}A$ is a product of units of $\mathbf{Z}C$, as C ranges over all cyclic subgroups. It is in this sense that $\mathbf{Z}A$ has no units of its own, i.e. no *proper* units. We shall provide some evidence that this state of affairs persists for A of higher rank than 2, and we believe that the restriction to regular primes is also just a feature of our method of proof rather than a necessary condition. We may assume without loss of generality that $p > 3$ [9, p. 57].

To be more precise, let $\dot{U}(A)$ denote the group of units of $\mathbf{Z}A$ modulo torsion, and consider the natural maps

$$\coprod_C \dot{U}(C) \xrightarrow{\alpha} \dot{U}(A) \xrightarrow{\beta} \prod_K \dot{U}(K)$$

where C and K run over the cyclic subgroups and factor-groups of A, respectively, and where the products are free abelian. The composite $\gamma = \beta \circ \alpha$ is an injection of lattices (free abelian $\mathbf{Z}$-modules), whose index is a known power of p; in fact, $\log_p \operatorname{ind}(\gamma) = (n/2)R$, where $n + 1$ is the rank (over $\boldsymbol{F}_p$) of A, and R is the rank (over $\mathbf{Z}$) of any of the three lattices involved, namely

$$R = \frac{1}{2}(p - 3)(1 + p + \ldots + p^n),$$

by Dirichlet's Unit Theorem (cf. [5]).

Another fact known about γ is the number of cyclic factors of its cokernel, i.e. the corank of $\bar{\gamma} = \gamma \otimes_{\mathbf{Z}} \boldsymbol{F}_p$ (the unit groups written additively); it equals $R - \Sigma_r h(n, r)$, where R and n are as above, r runs over all even numbers between 1 and $p - 2$, and $h(n, r)$ denotes the number of monomials of degree r in $n + 1$ indeterminates (cf. [6]).

Received by the editors March 20, 1985.
This work is supported by NSERC Grant A-5300.
AMS Subject Classification (1980): Primary 20C05; Secondary 16A25, 16A18.

So far, not much seems to be known about α or β. As indicated at the outset, we suspect that α is surjective (hence bijective), i.e. that γ and β have the same index. The main result of this paper is that $\bar{\gamma}$ and $\bar{\beta}$ have the same rank, provided that p satisfies a condition which is (only ?) formally weaker than regularity. Since the cokernel of β is at least as large as that of $\bar{\beta}$, this does provide an improved upper bound on the index of α, but only for $n = 1$ does it force surjectivity. These matters are taken up in paragraph 3 below.

Paragraph 4 makes the connection between regularity of p and the condition actually used in the proof of the main result, namely that the kernel of

$$\pi : U_1 ZC \to U_1 F_p C$$

should consist entirely of p^{th} powers, where U_1 denotes 1-units and π comes from reducing coefficients: $Z \to F_p$; C again stands for a cyclic group of order p.

In paragraph 2, we recall some fairly standard facts about the action of $G = \mathrm{Aut}(C) = F_p^{\times}$ on $\dot{U}(C)/\dot{U}(C)^p$ and on the augmentation ideal of F_pA. As in [6], much of our information comes from counting the multiplicities of G-characters.

2. **Preliminaries**. Continuing in the notation of the introduction, we put $\bar{U}(A) = \dot{U}(A)/\dot{U}(A)^p$. In additive notation, this would be $\dot{U}(A) \otimes_Z F_p$. The natural action of G on A makes it into a semi-simple G-module, whose G-structure depends entirely on the multiplicity with which the various characters $\bar{\chi}_r : G \to F_p^{\times}$, $r = 1, \ldots, p-1$, occur in it. Explicitly $\bar{\chi}_r$ is given by $\bar{\chi}_r(g) = g^r$. This is because $|G| = p - 1$ and F_p is a splitting field of G (cf. [3] p. 213–14).

LEMMA 1. *If r is an even number between 1 and $p-2$, the multiplicity of $\bar{\chi}_r$ in $\bar{U}(C)$ is 1. Otherwise it is 0.*

PROOF. This is essentially an F_p-version of Minkowski's Unit Theorem, which makes the analogous assertion about $\dot{U}(C) \otimes_Z C$ and the characters $\chi_r(g) = \mu^r \in C^{\times}$, where μ is a primitive $(p-1)^{\text{st}}$ root of 1 and g is a generator of G. Actually, Minkowski's theorem (cf. [4], Anhang, p. 271) describes the Galois action on the units of $Q[\epsilon + \epsilon^{-1}]$, ϵ a p^{th} root of unity.

Indeed, the integral representation of G on $\dot{U}(C)$ has a character χ whose (rational integral) values $\chi(g^s)$ can be written as $\Sigma_r m_r \mu^{sr}$ in $Z[\mu]$, where m_r is the multiplicity of χ_r (i.e. 0 or 1). Applying the homomorphism $Z[\mu] \to F_p$ which sends μ to g, we see that the reduced version $\bar{\chi}$ of this character has the values $\bar{\chi}(g^s) = \Sigma_r m_r g^{sr}$, with the same multiplicities.

Our second lemma deals with the augmentation ideal $\Delta_p(A)$ of F_pA, again as a G-module. This ideal is generated by elements of the form $(a-1)$ with $a \in A$. On these, $g \in G$ acts by $(a-1) \to a^g - 1 = (1 + [a-1])^g - 1 = g(a-1) + \binom{g}{2}(a-1)^2 + \ldots$, which proves the following statement.

LEMMA 2. *G acts on $\Delta_p(A)^r/\Delta_p(A)^{r+1}$ via the character $\bar{\chi}_r$.*

The point of this observation is to deduce the proposition stated at the end of this

https://doi.org/10.4153/CMB-1987-005-6 Published online by Cambridge University Press

paragraph. Before we get to it, we need to recall something about logarithms.

In the ring $\boldsymbol{Q}[[x, y]]$ of formal power-series, we have the identity

$$\log (1 + x + y + xy) = \log (1 + x) + \log (1 + y).$$

If we work modulo the p^{th} power of the maximal ideal (x, y), this identity can be written with coefficients in the p-adic integers $\boldsymbol{Z}_p$, since $(x + y + xy)^p = x^p = y^p = 0$. The same identity is thus valid in the truncated polynomial ring $\boldsymbol{F}_p[x, y]/(x, y)^p$. It therefore allows us to define a homomorphism

$$\log : U_1 R(A) \to I(A)$$

from the 1-units of the artinian local ring $R(A) = \boldsymbol{F}_p A/\Delta_p(A)^p$ to its maximal ideal $I(A) = \Delta_p(A)/\Delta_p(A)^p$. We remark in passing that, for $A = C$ cyclic, $\Delta_p(C)^p = 0$ anyway, and hence $R(C) = \boldsymbol{F}_p C$.

Since G acts as ring automorphisms on $R(A)$ and $\log (1 + t)$ is a polynomial in $t \in I(A)$, the logarithm is a G-map. In paragraph 3 the following statement will be useful.

PROPOSITION. *The multiplicity of $\bar{\chi}_r$ in $I(A)$ is $h(n, r)$, for $r = 1, \ldots, p - 1$.*

PROOF. If $a_0, \ldots, a_n$ are generators of A, $t_i = a_i - 1$ generate the ideal $\Delta_p(A)$, and $\boldsymbol{F}_p A$ is the polynomial ring $\boldsymbol{F}[t_0, \ldots, t_n]$ subject to the relations $t_i^p = 0$. For $1 \leq r < p$, $I(A)^r/I(A)^{r+1} \simeq \Delta_p(A)^r/\Delta_p(A)^{r+1}$ is isomorphic, as an $\boldsymbol{F}_p$-space, to the space of homogeneous polynomials of degree r.

3. **The Main Result**. We shall produce a diagram

$$\begin{array}{ccccc} \prod_C \bar{U}(C) & \xrightarrow{\bar{\alpha}} & \bar{U}(A) & \xrightarrow{\bar{\beta}} & \prod_K \bar{U}(K) \\ \downarrow & & \downarrow \rho_A & & \downarrow \\ \prod_C V(C) & \xrightarrow{\alpha^+} & V(A) & \xrightarrow{\beta^+} & \prod_K V(K) \end{array}$$

in which the arrows represent linear maps of $\boldsymbol{F}_p$-spaces, the vertical ones being surjections. For the coranks of the horizontal ones, we therefore have the inequalities

$$\operatorname{cork} \bar{\gamma} \geq \operatorname{cork} \bar{\beta} \geq \operatorname{cork} \beta^+,$$

and we now shall prove, for certain primes p, that $\operatorname{cork} \beta^+ \geq \operatorname{cork} \bar{\gamma}$, which implies the equality of all these coranks. This will work for primes which fit the following description.

DEFINITION. *A prime p will be called* quasi-regular, *if the kernel of the map*

$$\pi : U_1 \boldsymbol{Z} C \to U_1 \boldsymbol{F}_p C,$$

as described in the introduction, consists entirely of p^{th} powers.

https://doi.org/10.4153/CMB-1987-005-6 Published online by Cambridge University Press

As we shall see in paragraph 4, regularity implies this condition, and the two notions actually coincide modulo the so called Vandiver conjecture.

Our main result can now be stated.

THEOREM. *If p is quasi-regular, the maps $\bar{\beta}$ and $\bar{\beta} \circ \bar{\alpha}$ have the same rank.*

For the unreduced map α, this has a relatively modest consquence.

COROLLARY 1. $\log_p \operatorname{ind} \alpha \leq ((n-2)/2)R + \Sigma_r\, h(n,r)$ *where r runs over the even numbers between* 1 and $p-2$.

PROOF. Immediate from the values for $\log_p \operatorname{ind} \gamma$ and $\operatorname{cork} \bar{\gamma}$ quoted in the introduction.

If A is of rank 2, i.e. $n = 1$, we have

$$R = \frac{p-3}{2}(p+1), \qquad \sum_r h(n,r) = \sum_r (n+1) = \frac{p-3}{2}\frac{p+1}{2},$$

and therefore $\log_p \operatorname{ind} \alpha \leq 0$. We state this formally.

COROLLARY 2. *If A has rank 2 and p is quasi-regular, $\dot{U}(A)$ is the free abelian product $\Pi_C\, \dot{U}(C)$, where C runs over the cyclic subgroups of A.*

The first candidates for elementary abelian groups whose group rings *might* have proper units are those of order 5^3 and order 37^2, both large enough to discourage naive computational verifications.

For the proof of the theorem, it is convenient to work with a subgroup $U_*(A)$ of $U_1\boldsymbol{Z}A = U(1+\Delta(A))$, namely those units of $1+\Delta(A)^2$ which are fixed under the involution of $\boldsymbol{Z}A$ taking every group element to its inverse. This is "the" torsion-free subgroup of $U\boldsymbol{Z}A$; it is isomorphic to $\dot{U}(A)$ (cf [2], Lemma 2.6) in a manner obviously compatible with the action of G.

In particular, we may identify $\bar{U}(A)$ with $U_*(A)/U_*(A)^p$, from where we have a G-map

$$\bar{\pi}_A : \bar{U}(A) \to U_1\boldsymbol{F}_pA$$

induced by π_A (reduction of coefficients $\boldsymbol{Z} \to \boldsymbol{F}_p$), because every element of $U_1\boldsymbol{F}_pA$ is of order p. In fact, we shall take this map a little farther, into $U_1R(A)$, which entitles us to follow it with the logarithm, as explained in paragraph 2. All in all, we now have a G-map $\rho_A = \log \bar{\pi}_A$:

$$\bar{U}(A) \xrightarrow{\bar{\pi}_A} U_1R(A) \xrightarrow{\log} I(A).$$

We let $V(A)$ be its image and have thereby produced the diagram promised at the beginning of this paragraph.

It remains to be seen that $\operatorname{cork} \beta^+ \geq \operatorname{cork} \bar{\gamma}$, which will be done in two steps

(1) $rk\, V(C) = rk\, \bar{U}(C)$, and
(2) $rk\, \beta^+ \leq \Sigma_r\, h(n,r)$,

https://doi.org/10.4153/CMB-1987-005-6 Published online by Cambridge University Press

r constrained as in Corollary 1.

Step (1) amounts to seeing that $\rho_C: \bar{U}(C) \to I(C)$ is injective, or—since log has its usual inverse exp—that $\bar{\pi}_C: \bar{U}(C) \to U_1 \boldsymbol{F}_p C$ is injective. This is immediate from the definition of quasi-regularity and the identification $\bar{U}(C) = U_*(C)/U_*(C)^p$.

Step (2) depends on the characters $\bar{\chi}_r: G \to \boldsymbol{F}_p^\times$. The range of β^+ can only involve such characters as can be found in $\bar{U}(C)$, namely $\bar{\chi}_r$ with $1 < r = 2s < p - 2$. By the proposition at the end of paragraph 2, the multiplicity in $I(A)$ of such a character is $h(n, r)$.

4. **Quasi-Regularity**. Since $U_1 \boldsymbol{Z} C$ consists of a cyclic group of order p and a free abelian group of rank $(p - 3)/2$, quasi-regularity means that the image of the map

$$U_1 \boldsymbol{Z} C \xrightarrow{\pi} U_1 \boldsymbol{F}_p C \xrightarrow{\log} \Delta_p(C)$$

has dimension $\geq (p - 1)/2$. Following Kervaire and Murthy [7], we shall describe an adaptation modulo p of a classical calculation [cf. [1], Ch. V, §6.3), which shows that it has dimension $\geq ((p - 1)/2) - \delta_p)$, where δ_p is the number of Bernoulli numbers $B_2, B_4, \ldots, B_{p-3}$ vanishing in $\boldsymbol{F}_p$.

Of course, δ_p is exactly what keeps p from being regular (cf. [1], Ch V, §6.4); the first irregular prime ($\delta_p \neq 0$) being 37.

Let ϵ be a p^{th} root of 1. In $\boldsymbol{Z}[\epsilon]$ consider the units

$$v_r = \frac{\epsilon^r - 1}{\epsilon - 1} = 1 + \epsilon + \ldots + \epsilon^{r-1}, \text{ for } r = 2, \ldots, \frac{p - 1}{2}.$$

If x is a generator of C, the Wedderburn map takes $1 + x + \ldots + x^{r-1}$ to a unit in the second component of $\boldsymbol{Z} \oplus \boldsymbol{Z}[\epsilon]$, but not in the first. That can be fixed by taking instead $v_r = (1 + x + \ldots + x^{r-1})^{p-1} - m_r \hat{C}$, where $\hat{C} = 1 + x + \ldots + x^{p-1}$ and $r^{p-1} = 1 + m_r p$. These v_r *are* units in $U_1 \boldsymbol{Z} C$, and we will show that the elements $\log(\pi(v_r))$, together with $\log(\pi(x))$, span a space of dimension $((p - 1)/2) - \delta_p$ in $R'(C) = \boldsymbol{F}_p C/\Delta_p(C)^{p-1}$, which is certainly all we need.

Working modulo $\Delta_p(C)^{p-1}$ is not a mere whim; it is imposed on us by two circumstances:

1) The image of v_r in $R'(C)$ is $(1 + x + \ldots + x^{r-1})^{p-1}$, since $\hat{C} \in \Delta_p(C)^{p-1}$.

2) If z is a generator of $\Delta_p(C)$, division by z is a well-defined linear map $\Delta_p(C) \to R'(C)$, but not into $\boldsymbol{F}_p C$.

Now, to carry out the long-announced calculation, we shall work with the inverses (in $R'(C)$) of the v_r:

$$u_r = \frac{1}{r}(1 + x + \ldots + x^{r-1}) = \frac{1}{r}\frac{x^r - 1}{x - 1}.$$

To see that these *are* the inverses, one has to remember that the p^{th} power is an additive homomorphism.

Let $z = \log(1 + [x - 1])$ in $\boldsymbol{F}_p C$, so that $x = \exp(z)$; z is certainly a generator of $\Delta_p(C)$, and hence the identity

$$u_r = \frac{\exp(rz) - 1}{rz} \cdot \frac{z}{\exp(z) - 1}$$

is valid in $R'(C)$.

We can now go into the Bernoulli routine and show (cf. [7]) that the formula

$$\log \frac{e^z - 1}{z} = \frac{1}{2}z + \sum_{s=2}^{p-2} \frac{B_s}{s} \cdot \frac{z^s}{s!}$$

makes sense in $R'(C)$ and holds true for any z in its maximal ideal. Hence, for $r = 2, \ldots, (p-1)/2$ and $z = \log x$,

$$\log u_r = \frac{1}{2}(r-1)z + \sum_{s=2}^{p-2} \frac{r^s - 1}{s \cdot s!} B_s z^s.$$

Of course, apart from $B_1 = -1/2$, only the even values of s have a non-trivial B_s. If, for $m = (p-3)/2$, we write

$$\log u_r - \frac{1}{2}(r-1)z = \sum_{k=1}^{m} (r^{2k} - 1) \frac{B_{2k}}{2k(2k)!} z^{2k}$$

we only need to observe the invertibility of the $m \times m$ matrix $(r^{2k} - 1)$, $2 \leq r \leq m+1$, $1 \leq k \leq m$, to conclude that the elements on the left of this set of relations span an $(m - \delta_p)$-dimensional space. Setting $u_1 = x$, hence $\log u_1 = z$, the $\log u_r$ then span a space of dimension $(p-1)/2 - \delta_p$, as advertised. Thus we have proved the following statement:

PROPOSITION. *If* $\delta_p = 0$, *then* p *is quasi-regular.*

In concluding, we shall make some remarks about a possible converse. We recall that p is *regular* if and only if the class number h_p of $\boldsymbol{Q}[\epsilon]$ does not vanish modulo p and *semi-regular* if and only if the class number h_p^+ of $\boldsymbol{Q}[\epsilon + \epsilon^{-1}]$ does not so vanish. Now h_p^+, which divides h_p (it is the "second factor" of h_p), is also the index in $U\boldsymbol{Z}[\epsilon]$ of the group generated by the units v_r together with the trivial units (cf. [8], Ch. 3, §5). It is not hard to see that the units v_r plus the trivial units generate a subgroup of index $k \cdot h_p^+$ in $U\boldsymbol{Z}C$, where all the prime divisors of k divide $p-1$, and hence k is prime to p. The only way a prime can be quasi-regular is therefore that h_p^+ contains the factor p to the power δ_p, so that the short-fall δ_p can be made up as we pass from U to $\bar{U}$. However, a conjecture ascribed to Vandiver (cf. [8], Ch. 5, §4) says that h_p^+ is always prime to p. This would mean that only regular primes can be quasi-regular.

REFERENCES

1. Z. Borevich and I. Shafarewich, *Number Theory*, Academic Press, N.Y., 1966.

2. G. Cliff, S. Sehgal and A. Weiss, *Units of Integral Group Rings of Metabelian Groups*, J. Alg., **73** (1981).

3. C. Curtis and I. Reiner, *Representation theory of finite groups and associative algebras*, Interscience, N.Y., 1962.

4. H. Hasse, *Vorlesungen über Klassenkorper theorie*, Physica-Verlag, Wurzburg (1967).

5. K. Hoechsmann, S. Sehgal and A. Weiss, *Cyclotomic Units and the Unit Group of an Elementary Abelian Group Ring*, Archiv d. Math. (to appear).

6. K. Hoechsmann, *Functions on Finite Vector Spaces and Units in Abelian Group Rings*, Can. Math. Bull. (to appear).

7. M. Kervaire and M. Murthy, *On the projective class group of cyclic groups of prime power order*, Comm. Math. Helvet., **52** (1977), pp. 415−452.

8. S. Lang, *Cyclotomic Fields*, Springer-Verlag, N.Y., 1978.

9. S. Sehgal, *Topics in Group Rings*, Dekker, N.Y., 1978.

University of British Columbia
Vancouver

University of Alberta
Edmonton
Canada