BAYREUTHER MATHEMATISCHE SCHRIFTEN

ISSN 0172-1062 Heft **33**, 1990

Schriftleitung Prof. Dr. A. Kerber, Lehrstuhl II für Mathematik
Postfach 3008 · 8580 Bayreuth, W.-Deutschland

Herausgeber dieser Schriftenreihe sind die Dozenten des Mathematischen Instituts der Universität Bayreuth. Arbeiten, die in dieser Schriftenreihe erscheinen sollen, sind über einen der Dozenten einzureichen. In der Reihe erscheint etwa vierteljährlich ein Heft. Inhaltlich handelt es sich um Originalarbeiten, Dissertationen, Habilitationsschriften und Manuskripte zu Spezialvorlesungen. Die Arbeiten werden im Zentralblatt für Mathematik, den Mathematical Reviews und dem Referativnis Journal referiert.

Einzelhefte können zur Zeit zum Preis von DM 12,00 über folgende Adresse bezogen werden:

Universitätsbibliothek Bayreuth
Geschenk- und Tauschstelle
Postfach 101251
D-8580 Bayreuth
Bundesrepublik Deutschland

BAYREUTHER MATHEMATISCHE SCHRIFTEN **33** (1990), 153-171

Large Subgroups in the Unit Group of Group Rings (a Survey)

Jürgen Ritter

1 Introduction

Looking at group rings $\mathfrak{o}G$, where $\mathfrak{o}$ is the ring of integers in a local or global field K and G is a finite group, is caused by mainly two reasons. Firstly, group rings are prominent examples of orders in semi-simple algebras, of which are found a great many in number theory and which are known to hold relevant arithmetical properties, and secondly, group rings are natural operator domains acting on distinguished objects coming along with a Galois extension L/F of number fields. So does the ring $\mathfrak{o}_L$ of integers of L, on which the action of the Galois group $G_{L/F}$ has only been determined in special cases yet [F1]. If, for example, we asssume $F = \mathbb{Q}$ and L to be an abelian tamely ramified extension of $\mathbb{Q}$, then it has been shown that $\mathfrak{o}_L \simeq \mathbb{Z}G_{L/\mathbb{Q}}$, that is to say that there exists an *integral normal basis* $\{a^\sigma : \sigma \in G_{L/\mathbb{Q}}\}$ of $L/\mathbb{Q}$ with $a \in \mathfrak{o}_L$. There arises at once the question which integral elements actually generate a normal basis. Of course, they are exactly the elements a^ε with *ε a unit in the integral group ring $\mathbb{Z}G_{L/\mathbb{Q}}$*. It should be mentioned that Everst [Ev] has given valuable information on the totality of all generators by means of properties of the series $\sum_n a_n n^{-s}$ where $a_n = \#\{\varepsilon : a^\varepsilon \text{ has norm } n\}$.

Let us next turn our attention towards another inportant example, the group E_L of units in L. Here we get from the Dirichlet unit theorem [Ha] an abstract splitting $E_L = \mu_L \times \mathbb{Z}^{r+s-1}$ with μ_L the group of roots of unity and r and s the numbers of real, respectively complex, embeddings of L, and we are once more left with providing a description of the structure of a known abelian group as a module over the integral group ring $\mathbb{Z}G_{L/F}$, which again turns out to be a subtle and difficult task [F_2,F_3].

We believe that adding information on the group ring itself, in particular on its units, may well help to ease the way to getting results in the direction of our two examples above. The last one, in turn, can also be considered a hint as to what a first approach to a description of *the unit group U of a group ring* should look like: When working with units in L it is often sufficient to only have generators of a *subgroup of finite index in E_L* rather than a full set of fundamental units; the cyclotomic units or the Ramachandra units are such generators, if L is a cyclotomic field [Wa]. Thus, in the first place, one ought to find large subgroups of U.

As for orders in general, very little is known on their units. An element $e \in A$, a semi-simple algebra over the number field F, is called a *unit*, if it is invertible in A and if both, e and e^{-1}, are integral. That amounts to the same as saying e is integral and its norm is a unit in F. On page 88 in his book [Dg] Deuring writes:

> Genaueres ist über Einheiten nicht bekannt, soweit das Nichtkommutative in Betracht kommt. Ein Gegenstück des Dirichletschen Satzes für Zahlkörper ist bisher nicht aufgestellt worden

Anyhow, Siegel has proved the unit group of an order to be finitely generated [Si].
In this article some recent results on units in an order will be introduced, in particular refering to orders being group rings $\mathfrak{o}G$.

2 Some general results on units; the abelian case

To set the tune we begin this section with a quick collection of well-known facts on units [Sg,Ka]; the heart of the matter, though, is a discussion of the abelian case. We restrict ourselves to just looking at $\mathbb{Z}G$. U denotes the group of units in $\mathbb{Z}G$, u is always an element in U.

(i) If u is central and of finite order, then, up to sign, u is a group element, $u = \pm x, \quad x \in G$.

(ii) If $u = \sum_{x\in G} \alpha_x x$, $\alpha_x \in \mathbb{Z}$, has finite order and $\alpha_{x_o} \neq 0$ for some central group element x_o, then $u = \pm x_o$.

(iii) If $u = \sum_{x\in G} \alpha_x x$ has order p^m, p a prime, then there exists an $x \in G$ with $\alpha_x \neq 0$ and $\mathrm{ord}(x) = p^m$.

(iv) Equivalent are

- the torsion part of U consists only of the elements $\pm x, \quad x \in G$
- $\mathbb{Z}G$ does not contain nilpotent elements $\neq 0$
- G is either abelian or a direct product $A_2 \times Q_8$ of a 2-elementary abelian group A_2 and the quaternion group Q_8 of order 8

Moreover, U itself is exhausted by $\pm G$, if, and only if, either G is abelian and its exponent divides 4 or 6, or $G = A_2 \times Q_8$ as above.

A recent result in the same direction is [RS_1]

(v) Precisely if G satisfies

"for any natural j prime to $|G|$, x^j is conjugate to x or to x^{-1}, where x runs through G",

there are only finitely many central units in $\mathbb{Z}G$.

(vi) Let G be abelian. Then U splits into

$U = \pm G \times \mathbb{Z}^n, \quad n = 1/2(|G| + 1 + n_2 - 2n_c)$ with $n_2 =$ number of cyclic subgroups of order 2 and $n_c =$ number of all cyclic subgroups of G.

The result (vi) goes back to Higman; it is a translation of the Dirichlet unit theorem into the group ring language. Below we shall be concerned with finding large subgroups of U in the abelian case.

(vii) Until around 1980 U was explicitly known for $G =$

S_3 [HP]
A_4 [AH]
D_4, the dihedral group of order 8 [PM]
D_{2p}, the dihedral group of order $2p$, p a prime [PS]
$p \rtimes q$, the semidirect product of two cyclic groups of prime orders p and $q | p-1$ [GRU]
P, an extraspecial p-group, p odd [RS$_2$].

It should be pointed out that for the last three infinite series the determination of U rests on the fact that the integral group ring appears as a pull-back of the group ring $\mathbb{Z}G/[G,G]$ and the image of $\mathbb{Z}G$ in *the* nonabelian Wedderburn component of the rational group algebra $\mathbb{Q}G$.

The abelian case: We assume G to be an abelian p-group with p odd. The rational group algebra $\mathbb{Q}G$ splits into cyclotomic fields $\mathbb{Q}(\zeta)$ with ζ running through a certain set of roots of unity of p-power order. Recall that

$$C_\zeta = \langle -1, \zeta^{(1-a)/2}\frac{1-\zeta^a}{1-\zeta} : 1 < a < \frac{\operatorname{ord}\zeta}{2},\ p \nmid a \rangle$$

is the group of *cyclotomic units* in $\mathbb{Q}(\zeta)^+ = \mathbb{Q}(\zeta + \zeta^{-1})$. It has finite index h^+ in the whole unit group of $\mathbb{Q}(\zeta)^+$, which according to Vandiver's conjecture is prime to p [Wa].

Define then a subgroup Ω of U_1, the group of units having augmentation one, by requiring that Ω is stable under the isomorphism $x \mapsto x^{-1}$ of G and that it collects the u which *appear circular* in each field $\mathbb{Q}(\zeta)$, that is to say, their projections into $\mathbb{Q}(\zeta)$ fall into C_ζ.

There is a distinguished subgroup Λ of Ω, the group of *constructible units*, namely

$$\Lambda = \prod W(C),$$

the product being taken over all cyclic subgroups C of G. Here $W(C)$ is the intersection of Ω with the group spanned by all *Bass-Milnor units*

$$w_i(x) = (1 + x + \ldots + x^{i-1})^m + \frac{1-i^m}{\operatorname{ord}(x)}\hat{x},\ \hat{x} := 1 + x + \ldots + x^{\operatorname{ord}(x)-1},$$

where $x \in C$, $1 < i < \mathrm{ord}(x)$, $(i, \mathrm{ord}(x)) = 1$, $m = \varphi(|C|)$, φ the Euler φ-function.
Notice that $w_i(x)$ projects into C_ζ.

With these notations (or rather with a slight modification of the W, the precise definition of which shall be omitted) it is proved in [HR,Ho]

- $|U : \Lambda| < \infty$
- Λ and Ω have the same Wedderburn projectons
- $|\Omega : \Lambda|$ is a p-power and is closely related to the order of the kernel subgroup $D(\mathbb{Z}G)$. Recall that $D(\mathbb{Z}G)$ is that part of the class group of the locally free $\mathbb{Z}G$-modules that vanishes under the embedding of $\mathbb{Z}G$ into the maximal order of $\mathbb{Q}G$ [Ty]. As a special case, $|\Omega : \Lambda| = 1$ when p is a regular prime.
- $|U_1^+ : \Omega|$ is p-prime provided Vandiver's conjecture holds. Here U_1^+ denotes the subgroup of U that consists of all units having augmentation one and being invariant under the automorphism $x \mapsto x^{-1}$ of G.

Thus, without exaggerating, one can say that, even for numerical purposes, in the case of an abelian p-group G the unit group of its integral group ring is as much in our hands as are the units of the cyclotomic fields $\mathbb{Q}(\zeta)$ themselves.

As for the proof, there are essentially three ingredients to be stressed. One is Borevic's description [Bv] of the Galois module structure of the group of 1–units in a p-adic field that does not contain a primitive p-th root of unity ζ_p, which, in the present context, applies to the structure of the 1–units of $K = \mathbb{Q}_p(\zeta_{p^n} + \zeta_{p^n}^{-1})$ as a $\mathbb{Z}_p G_{K/\mathbb{Q}_p}$-module. Another one is Fröhlich's exact sequence relating the kernel subgroup D to global and local unit groups [F4]. A third one, finally, is the discussion of the embedding $\mathbb{Z}G \subset \mathbb{Z}_p G$.

3 The Brauer-Zassenhaus conjecture

The conjecture asks whether a finite subgroup of $U_1 = U_1(\mathbb{Z}G)$ is, up to conjugation in the rational group algebra $\mathbb{Q}G$, already a subgroup of G. It has meanwhile been disproved by Roggenkamp and Scott [RSc₁]. The most general result in the direction of the conjecture seems to be the following one, which is due to Weiss [Ws₁,Ws₂]:

(3a) *If G is nilpotent and $H \leq U_1$ is finite, then there is an $a \in U(\mathbb{Q}G)$ such that $aHa^{-1} \leq G$.*

I'm not going to go into the history of the conjecture which, because of their fundamental papers, has also become closely related to the names of Roggenkamp and Scott [RSc₂]. However, since there is quite a large class of groups to which the conjecture applies and, at the same time, for which we can provide generators of a subgroup of finite index in the whole unit group, I'd like to at least recall some further known results. It may perhaps be interesting to view these investigations into U_1 in the light of Dirichlet's unit theorem; on the one hand, we have sort of a description of the torsion part of U and, on the other hand, as with cyclotomic units, we have a set of explicitly given elements that generate U up to a finite index.

(3b) *Let G be a cyclic by abelian group extension, $G = C \rtimes A$, with $(|C|, |A|)$ $= 1$. Let furthermore $H \leq U_1$ be a cyclic torsion subgroup. Then, up to conjugation in $\mathbb{Q}G$, H lies in G [PRS,T₁].*

(3c) *Let $G = A \rtimes X$, A, X abelian, and X acting faithfully irreducibly on A. Then each torsion unit in U_1 is rationally conjugate to a group element [SW].*

(3d) *Assume $G = A \rtimes X$ with A and X abelian and $|X| < p$ for every prime p dividing $|A|$. Suppose in addition that either $|X|$ is prime or A is cyclic. Then again each torsion unit in U_1 is rationally conjugate to a group element [MRSW].*

(3e) *Let G have class 2. Then each torsion unit $u \in U_1$ is congruent to a unique group element x modulo the Whitcomb ideal $\Delta(G)\Delta(G,G')$; moreover, u and x are rationally congruent [RS₄].*

(3f) *Let G be a p-constrained group with $O_{p'}(G) = 1$. Then any subgroup of U_1 of order $|G|$ is in $\mathbb{Q}G$ conjugate to G [RSc₃].*

It has been announced by Trama [T_2] that he has proved the Zassenhaus conjecture for the symmetric group S_5 on five letters. As to the A_5, Luthar and Passi [LP] show that each torsion unit is rationally conjugate to a group element.

Remarks:

1. For a normal subgroup N in G, $\Delta(G,N)$ is the kernel of the natural map $\mathbb{Z}G \to \mathbb{Z}G/N$; $\Delta(G) = \Delta(G,G)$.

2. The class 2-groups are so far the only ones for which one is able to explicitly construct the group element x to which the given torsion unit u is rationally conjugate. In [RS_4] it is shown that a corresponding result for the D_{10} does not hold.

3. The condition on G in *(3e)* means that G has a normal p-subgroup N such that the centralizer of N in G sits in N.

There are, roughly, three methods of proof in this context. As long as there is only one torsion unit u in question, one uses representation theory and tries to determine the matrices $T(u)$ for every irreducible representation T. Totally different is the approach given by Weiss. For the special case of a p-group G rather than an arbitrary nilpotent group he translates the conjugacy property into a beautiful theorem on permutatoin lattices [Ws_1]:

> *Let M be a $\mathbb{Z}_p[\zeta_p]G$-lattice satisfying: M/pM is a $\mathbb{F}_pG$-permutation lattice, i.e. $\simeq \oplus\mathrm{ind}_U^G(1)$, the sum ranging over certain subgroups U of G. Then M itself is a generalized permutation module, $M \simeq \oplus\mathrm{ind}_U^G\varphi$, where $\varphi : U \to \mathbb{Z}_p[\zeta_p]$ are characters. (ζ_p is a primitive p-th root of unity).*

Finally, Roggenkamp and Scott work in the Picard group of $\mathbb{Z}G$ which Fröhlich has made accessible [F_5]. They, at the same time, have obtained far-reaching results on the automorphism group of an integral group ring.

4 Large normal subgroups of the unit group

The first result in this section compares the normal span of the units arising from the cyclic subgroups with the group of all units in $\mathbb{Z}G$; it is due to Kleinert [Kl]. Though it is also valid for most groups having even order, in order to simplify matters we restrict ourselves to looking at odd order groups only.

(4.1) *If $|G|$ is odd, then the normal subgroup in $U = U(\mathbb{Z}G)$ generated by the unit groups of $\mathbb{Z}C$ with C ranging over all cyclic subgroups of G has finite index in U.*

The proof is based on two main ingredients. Firstly, as Bass [Ba] has shown, the images under the natural map $U(\mathbb{Z}G) \longrightarrow K_1(\mathbb{Z}G)$ of the Bass-Milnor units which have been defined in section 3 generate a subgroup of finite index in $K_1(\mathbb{Z}G)$. Secondly, a result of Margulis regarding algebraic groups is applied:

> *Let $G_1, \ldots, G_n$ be almost simple, simply connected, noncompact algebraic groups over $\mathbb{R}$ or $\mathbb{C}$ and Γ a discrete subgroup of $G_1 \times \ldots \times G_n$ having finite covolume and satisfying*
>
> - *for $J \subsetneq \{1, \ldots, n\}$, $\Gamma \cap \prod_{i \in J} G_i$ is finite*
> - *if $\mathrm{rank} G_i = 1$, then the projecton of Γ into G_i is dense.*
>
> *Then every noncentral normal subgroup of Γ has finite index in Γ (see [Ti]).*

There is another application of the theory of algebraic groups to unit groups resting on Borel's density theorem for arithmetic groups [Bo], which Hartley [Hy] has taken advantage of when proving that certain normal subgroups of the unit group of an order Λ in a semi-simple $\mathbb{Q}$-algebra A have finite index.

(4.2) *$U = U(\Lambda)$ contains a normal subgroup U_0 of finite index such that if N is almost subnormal in U, then either N contains a nonabelian free group or $N \cap U_0$ is central. Further, $U = U_0$ unless some simple component of A is a totally definite quaternion algebra.*

Here, a subgroup N of a group U is called *almost subnormal*, if there is a finite chain of subgroups

$$N = X_0 \leq X_1 \leq \ldots \leq X_n = U,$$

such that X_i is either normal or of finite index in $X_{i+1} (0 \leq i \leq n-1)$; it is called *nearly subnormal*, if $X_i \triangleleft X_{i+1}$ for $0 \leq i \leq n-1$ and $|X_n : X_{n-1}| < \infty$.

The next result [GRS] goes into the same direction.

(4.3) Every nearly subnormal subgroup of $U(\mathbb{Z}G)$ containing G contains a free group unless G is abelian or a Hamiltonian 2-group.

Recall that a group is called *Hamiltonian*, if it is nonabelian and all its subgroups are normal.

Hartley [Hy] has shown how to deduce (4.3) from (4.2); the original proof uses arguments that have to do with congruence subgroups instead.
So let us take the opportunity to remember the famous congruence theorems due to Bass-Milnor-Serre [BMS], Serre [Se], and Vaserstein [V_1,V_2]. To state those denote by $\mathfrak{o}$ the ring of integers in an algebraic number field K. For an ideal $\mathfrak{q} \neq 0$ of $\mathfrak{o}$ we define $E(\mathfrak{q})$ to be the subgroup of the special linear group $SL(n, \mathfrak{o})$ generated by all $\mathfrak{q}$-elementary matrices $1 + qe_{ij}$, $q \in \mathfrak{q}$, $i \neq j$, e_{ij} a matrix unit, and $\tilde{E}(\mathfrak{q})$ to be its normal closure in $SL(n, \mathfrak{o})$. If $n \geq 3$, then the normal subgroup of $E(\mathfrak{o})$ generated by $E(\mathfrak{q})$ is normal in $SL(n, \mathfrak{q})$ and hence coincides with $\tilde{E}(\mathfrak{q})$.

(CT) Assume that $n \geq 3$ or $n = 2$ and the field K is neither rational nor imaginary quadratic. Then

1. *$|SL(n, \mathfrak{o}) : \tilde{E}(\mathfrak{q})| < \infty$ for every nonzero ideal $\mathfrak{q}$ of $\mathfrak{o}$.*
2. *Every noncentral subgroup of $SL(n, \mathfrak{o})$ normalized by a subgroup of finite index contains $\tilde{E}(\mathfrak{q})$ for some $\mathfrak{q} \neq 0$.*
3. *If $n \geq 3$, then $\tilde{E}(\mathfrak{q}^2) \leq E(\mathfrak{q})$, in particular, $|SL(n, \mathfrak{o}) : E(\mathfrak{q})| < \infty$.*
4. *If $n = 2$, then $|SL(2, \mathfrak{o}) : E(\mathfrak{q})| < \infty$.*

In (CT) 1., 2., 3. the field K, as long as $n \geq 3$, can also be replaced by a *division algebra D having finite dimension over some number field and $\mathfrak{o}$ by a maximal order $\mathfrak{D}$ of D;* in case $n = 2$, however, D is restricted to not being a totally definite quaternion algebra or to not having $\mathbb{Q}$ or an imaginary quadratic field as its centre.

(CT) has lots of consequences on $U(\mathfrak{o}G)$. Here is a first one [RS_3].

(4.4) *Suppose that KG does not have any simple components of the following types:*

a) 2×2 matrix ring over a division algebra D which is a totally definite quaternion algebra or the centre of which is the rational field or an imaginary quadratic field

b) a noncommutative division ring other than a totally definite quaternion algebra.

Let H be a normal subgroup of some T which is a subgroup of finite index in $U = U(\mathfrak{o}G)$. If H contains G and a power of the centre of U, then H is of finite index in U.

Next we turn to *constructing* normal subgroups of finite index in $\mathbb{Z}G$.

(4.5) *Assume that $\mathbb{Q}G$ satisfies the assumptions made in (4.4). Then the subgroup of $U(\mathbb{Z}G)$ generated by its centre and the units of the form $1+\alpha$, $\alpha \in \mathbb{Z}G$, $\alpha^2 = 0$ is of finite index [RS₃].*

Examples of elements $\alpha \in \mathbb{Z}G$, $\alpha^2 = 0$ are $\alpha = (a-1)b\hat{a}$ with $a, b \in G$ and $\hat{a} = 1 + a + a^2 + \ldots + a^{\mathrm{ord}(a)-1}$. For the corresponding units we have [RS₅]:

(4.6) *Denote by H the subgroup of $U = U(\mathbb{Z}G)$ generated by the centre of U and all elements $u_{a,b} = 1 + (a-1)b\hat{a}$, $a, b \in G$, and by $\tilde{H}$ the normal closure of H in U. Then, provided the assumption (4.4) a) holds for $\mathbb{Q}G$ and, moreover, if there is no simple component of $\mathbb{Q}G$ which is a totally definite quaternion division algebra, then $|U : \tilde{H}| < \infty$ if, and only if, G has no nonabelian homomorphic image which is fixed point free.*

Here, a group F is said to be *fixed point free* if it has a complex irreducible representation ϱ such that for every nonidentity element $f \in F$, $\varrho(f)$ has all eigenvalues different from one. These groups were characterized by Zassenhaus [Zs]. Observe that if G maps onto such a group F, then the representation ϱ, when lifted to G, satisfies $\varrho(\hat{a}) = 0$ or $\varrho(a-1) = 0$, i.e. $\varrho(u_{a,b}) = 1$ for all $a, b \in G$.

Again, the proofs rest heavily on (CT), which in all cases, (4.4), (4.5) and (4.6), is used to verify the assertion in the components of $\mathbb{Q}G$. At a later stage we shall show that it already suffices to only look at the simple components. To turn our attention back to (4.6), the assumption that G does not have a homomorphic fixed point free group F implies for each absolutely irreducible representation T of G the existence of elements $a, b \in G$ such that $T(u_{a,b})$ is noncentral. It then can readily be seen that $T(\tilde{H}) \cap SL(n_i, \mathfrak{D}_i)$ is noncentral; here $\mathfrak{D}_i$ is a maximal order in the division algebra D_i over which the simple component of $\mathbb{Q}G$ that is not annihilated by T appears as an $n_i \times n_i$-matrix ring.

5 Explicit generators of a subgroup of finite index in the unit group

So far, though in some restricted sense, we have already achieved sort of a close approximation of the unit group $U = U(\mathbb{Z}G)$ by constructing a subgroup $\tilde{H}$ of finite index in U. This subgroup, however, we do not really know, since we cannot give explicit generators but instead only elements which generate it *together with all their comjugates in* U. The question arises whether one can actually forget about these conjugates. This turns out to be possible for a large class of groups, including the nilpotent odd order ones. For other groups, as for example monomial groups or the $SL(2, q)$, q a prime power, one has to add some more generating elements which are built in a similar way as the $u_{a,b}$.

(5.1) *Let G be a nilpotent group such that the rational group algebra $\mathbb{Q}G$ has no simple Wedderburn components which are 2×2 matrices over $\mathbb{Q}$ or $\mathbb{Q}(i)$ or $2^r \times 2^r$ matrices, $r \geq 0$, over $\mathbb{H}_k$, $k \geq 3$. Then the Bass-Milnor units and the $u_{a,b}$, $a, b \in G$, generate a subgroup of finite index in $U(\mathbb{Z}G)$. [RS6]*

Here, $\mathbb{H}_k$ denotes the Hamiltonian quaternion algebra over the real field $\mathbb{Q}(\zeta_{2^{k-1}} + \zeta_{2^{k-1}}^{-1})$, where $\zeta_{2^{k-1}}$ is a root of unity of order 2^{k-1}.
Recall that the Bass-Milnor units are the elements $(1 + a + \ldots + a^{i-1})^m + \frac{1-i^m}{d}(1 + a + \ldots + a^{d-1})$, where $a \in G$, $\mathrm{ord}(a) = d$, $i \in \mathbb{N}$ prime to d, and where $m = \varphi(|G|)$, φ being the Euler function.

For the proof we first observe that the simple components of $\mathbb{Q}G$ are matrix rings over commutative fields [Rq]. From (CT) and the already mentioned theorem of Bass [Ba], compare section 4, it follows readily that it suffices to show

- firstly, the image of $\langle u_{a,b}\rangle$ in each nonabelian Wedderburn component $K_{n\times n}$ of $\mathbb{Q}G$ contains a subgroup of finite index in $SL(n,\mathfrak{o})$, where $\mathfrak{o}$ is the ring of integers in K, and
- secondly, to any two such different components there is an element $u\in\langle u_{a,b}\rangle$ so that for the respective corresponding projections π_1 and π_2 we have $\pi_1(u)$ is noncentral, $\pi_2(u)=1$.

As to the second property, by already taking the first one for granted we deduce the existence of an $x\in G$ and a $\gamma\in \mathbb{Z}G$ with noncentral $\pi_1(1+(x-1)\gamma\hat{x})$. Let $\mu_1\in\mathbb{Q}G$ satisfy $\pi_1(\mu_1)=\pi_1(\gamma)$, $\pi_2(\mu_1)=0$ and let $r\in\mathbb{N}$ be such that $r\mu_1=\mu\in\mathbb{Z}G$. Then $\pi_1(1+(x-1)\mu\hat{x})$ is noncentral, but $\pi_2(1+(x-1)\mu\hat{x})=1$. It is now merely a technical matter to produce a subgroup of $\langle u_{a,b}\rangle$ which just lives in one given simple nonabelian component and there has finite index in the special linear group defined over the corresponding integers.

For p-groups, the first property mentioned above depends on a new and canonical way of writing an absolutely irreducible representation as an induced representation [RS$_6$]:

> *Assume that G is a p-group with p odd. Let T be an absolutely irreducible faithful representation of G of degree p^n, $n\geq 1$. Then there exist a maximal abelian normal subgroup A in G, an element $a\in A$ of order p, a maximal subgroup M of G containing A, and an irreducible representation V of M such that $T=\mathrm{ind}_M^G V$, $V(a)=1$ and $V(a^b)$, for $b\notin M$, does not have the eigenvalue 1.*

We then identify T with the projection onto the Wedderburn component belonging to T and use that element a in order to find sufficiently many elementary matrices in $T(\langle u_{a,b}\rangle)$; we may, of course, assume here our first property to already be true for the group M and the component belonging to V, thereby having an induction argument at our disposal.

There are two supplements to (5.1):

(5.2) *If G is the dihedral group of order $2n$, then the Bass-Milnor units together with all $u_{a,b}$ generate a subgroup of finite index in U [RS$_5$]*

(5.3) *If G is nilpotent and $\mathfrak{o} = \mathbb{Z}[\zeta]$ where ζ is a primitive $|G|$th root of unity, then*

$$|U(\mathfrak{o}G) : \langle B_1^{\mathfrak{o}}, B_2^{\mathfrak{o}} \rangle| < \infty \quad [RS_7]$$

Here, for an arbitrary cyclotomic order $\mathfrak{o} = \mathbb{Z}[\zeta]$,

$$B_1^{\mathfrak{o}} = \langle (1 + \varepsilon a + (\varepsilon a)^2 + \ldots + (\varepsilon a)^{i-1})^m + \frac{1-i^m}{d}\widehat{\varepsilon a} \rangle,$$

the span ranging over all $a \in G$, $\varepsilon \in \langle \zeta \rangle$, and $0 < i < d$, $(i,d) = 1$ where $d = \mathrm{ord}(a)$; m abbreviates $\varphi(|G| \cdot \mathrm{ord}(\zeta))$. Thus $B_1^{\mathbb{Z}}$ is essentially the group of Bass-Milnor units.
Moreover, $B_2^{\mathfrak{o}} = \langle 1 + (a-1)\mathfrak{o}G\hat{a} : a \in G \rangle$, so that $B_2^{\mathbb{Z}} = \langle u_{a,b} : a, b \in G \rangle$.

At this stage we take the opportunity to introduce another unit group, namely

$$B_3^{\mathfrak{o}} = \langle 1 - (\tau(h_0)h_0 - 1)\mathfrak{o}G \sum_{h \in H} \tau(h)h : h_0 \in H \leq G,\ \tau \in \mathrm{Hom}(\mathrm{H}, \mathfrak{o}^{\times}) \rangle.$$

Remark. The restrictions on G made in (5.1) are necessary. It has been shown in [RS$_6$] that for $G = \langle a, b : a^4 = 1 = b^4,\ a^b = a^{-1} \rangle$ and also for the quaternion group of order 16 the group generated by the Bass-Milnor units and the $u_{a,b}$ has infinite index in U.

Taking $B_3^{\mathfrak{o}}$ into account, we get [RS$_7$]:

(5.4) *Let S_n denote the symmetric group on n letters. Then $|U(\mathbb{Z}S_n) : \langle B_1^{\mathbb{Z}}, B_3^{\mathbb{Z}} \rangle| < \infty$.*

(5.5) *Suppose G satisfies*
For every complex irreducible representation T of G there is a subgroup H of G and a $\tau \in \mathrm{Hom}(\mathrm{H}, \mathbb{C}^{\times})$ such that τ has multiplicity 1 in the restriction of τ to H: $res_H^G(T, \tau)_H = 1$.
Then for $\mathfrak{o} = \mathbb{Z}[\zeta]$ where ζ is a primitive $|G|$th root of unity we have $|U(\mathfrak{o}G) : \langle B_1^{\mathfrak{o}}, B_3^{\mathfrak{o}} \rangle| < \infty$.

Examples of such groups are *monomial groups*, in particular *supersolvable groups*, and some extensions of these; moreover, *the groups $SL(2,q)$*, q a prime power. However, there exist solvable groups violating the condition [Ja].

Finally we have [RS$_7$]

(5.6) Let G be one of the following groups:

a) $G = \langle a\rangle \rtimes \langle x\rangle$, $\mathrm{ord}(a) = p^m$, $\mathrm{ord}(x) = q$, *p a prime not dividing q, x acting faithfully*

b) $G = \langle a\rangle \rtimes \langle x\rangle$, $\mathrm{ord}a$ *an odd prime*

c) $G = A \rtimes X$, *A, X abelian with X acting faithfully and irreducibly.*

Then the Bass-Milnor units together with all $u_{a,b}$ generate a subgroup of finite index in $U(\mathbb{Z}G)$.

The main tool for the proofs of (5.4), (5.5) and (5.6) is that we can find a basis such that

$$T(\tau^{-1}(h)h - 1) \text{ is a matrix whose first row has only zeros}$$

and

$$T(\sum_{h\in H} \tau^{-1}(h)h) \text{ has } (|H|, 0, \dots, 0) \text{ as its first row.}$$

From this it can easily be deduced that $T((\sum_{h\in H} \tau^{-1}(h)h - 1)\mathfrak{o}G(\sum_{h\in H} \tau^{-1}(h)h))$ contains all elementary matrices $m\mathfrak{o}e_{i1}$ with $i \geq 2$ and a suitable natural number m. In order to obtain the elementary matrices with nonzero entries in the other columns as well, that is all of $E(m\mathfrak{o})$, we use the subgroups xHx^{-1}.

6 Conclusion

In the previous section, *for suitable rings $\mathfrak{o}$ of cyclotomic integers* and a large class of finite groups G we have produced a set of units in $\mathfrak{o}G$ that almost generates $U(\mathfrak{o}G)$. In many cases $\mathfrak{o} = \mathbb{Z}$ is possible; for some groups G we have to assume $\zeta_{|G|} \in \mathfrak{o}$, though. What should be done next is

- firstly, to replace the special rings $\mathfrak{o}$ by arbitrary rings of algebraic integers or even by complete discrete valuation rings

- secondly, to extend the results to all finite groups.

Regarding the first task, it is certainly sensible to allow at least some restrictions on $\mathfrak{o}$ in case there are 2-dimenisonal absolutely irreducible representations of G, since the congruence subgroup theorems definitely do not apply in dimension 2 when $\mathfrak{o}$ is too small. Regarding the second task, we have already observed that the units dealt with so far, whether they belong to $B_1^{\mathbb{Z}}$, $B_2^{\mathbb{Z}}$, or to $B_3^{\mathbb{Z}}$, are of no help if G happens to be a fixed point free group: each such $B_i^{\mathbb{Z}}$ has trivial projection in at least one simple Wedderburn component of $\mathbb{Q}G$. So, new units need to be invented.
There is a third task that hasn't been tackled at all, yet. Namely, it is possible to describe the relations the given generators satisfy? Recall that in the number field situation the Dirichlet unit theorem not only provides generators – the roots of unity and the fundamental units – but also gives the structure of the unit group. Knowing all, or at least some, relations that the generating elements fulfil would of course lead to a better understanding of the group U in the noncommutative case as well. Already the determination of the torsion part of $\langle u_{a,b} : a, b \in G\rangle$ has shown to be complicated and, so far, results here have only been obtained for a very limited class of groups.

Finally, a further question has to do with determining *the index* of our constructed subgroup B, say, in U. As one sees from the proofs, B contains a group $H_1 \times \ldots \times H_r$ where r is the number of simple Wedderburn components of the group algebra and the H_i are subgroups of the special linear groups which come along with choosing bases in the components – with each H_i actually being an elementary matrix group $E_i(\mathfrak{q}_i)$. Thus, by getting the ideals $\mathfrak{q}_i$ one will also get a first estimate on the wanted index, namely from the orders of the factor groups $SL_i/E_i(\mathfrak{q}_i)$. Observe however, that this estimate only measures the distance from B to the unit group of that maximal order which depends on the choice of the basis. So it is by no means sharp, particularly when the projection of $\mathfrak{o}G$ into some component is not even contained in the component of that maximal order. At this stage we remember the problem whether an absolutely irreducible representation T that is realizable over a number field K can also be realized over the integers of K. This is true for odd nilpotent groups a follows from [Rq] or also from the induction property for p-groups stated in the last section. In general, it is wrong, though. In [RW] we have given an example of a group of order 171 and a T such that T is realizable over its character field but not over the integers thereof.

References

[AH] Allen/Hobby, *A characterization of units in* $\mathbb{Z}[A_4]$. J. of Alg. **66** (1980), 534 - 543.

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

[BMS] Bass/Milnor/Serre, *Solution of the congruence subgroup problem for* $SL_n(n \geq 3)$ *and* $SP_{2n}(n \geq 2)$. Publ. Math. Inst. Hautes Études Sci **33** (1967), 59 - 137.

[Bo] Borel, *Introduction aux groupes arithmetique.* Hermann, Paris 1969.

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

[Dg] Deuring, *Algebren.* Springer-Verlag 1968.

[Ev] Everest, *Angular distribution of units in abelian group rings - an application to Galois-module theory.* Crelle J. **375/6** (1987), 24 - 41.

[F_1] Fröhlich, *Galois module structure of algebraic integers.* Springer Verlag 1983.

[F_2] Fröhlich, *Problems in representation theory arising from Galois modules.* Proc. Symp. Pure Math. **47** (1987), 81 - 85.

[F_3] Fröhlich, *L-functions at* $s = 0$ *and Galois modules.* Séminaire de Théorie des Nombres de Bordeaux, 1986/7.

[F_4] Fröhlich, *On the classgroup of integral grouprings of finite abelian groups II.* Mathematika **29** (1972), 51 - 56.

[F_5] Fröhlich, *The Picard group of noncummutative rings, in particular, of orders.* Trans. AMS **180** (1973), 1 - 95.

[GRS] Gonçalves/Ritter/Sehgal, *Subnormal subgroups in* $U(\mathbb{Z}G)$, Proc. AMS **103** (1988), 375 -382.

[GRU] Galovich/Reiner/Ullom, *Class groups for integral representations of metacyclic groups.* Mathematika **19** (1972), 105 – 111.

[Ha] Hasse, *Zahlentheorie,* Akademie-Verlag 1963.

[Ho] Hoechsmann, *Local units and circular index in abelian p-group rings.* Preprint.

[HR] Hoechsmann/Ritter, *Constructible units in abelian p-group rings.* To appear in J. Pure and Appl. Algebra.

[HP] Hughes/Pearson, *The group of units of the integral group ring* $\mathbb{Z}S_3$. Canad. Math. Bull **15** (1972), 529 – 534.

[Hy] Hartley, *Free groups in normal subgroups of unit groups and arithmetic groups.* Contemp. Math. **93** (1989), 173 – 177.

[Ja] Janusz, *Primitive idempotents in group algebras.* Proc. AMS **17** (1966), 520 – 523.

[Ka] Karpilovsky, *Unit groups of group rings.* Longman Scientific & Technical 1989.

[Kl] Kleinert, *A theorem on units of integral group rings.* J. Pure and Appl. Algebra **49** (1987), 161 – 171.

[LP] Luthar/Passi, *Zassenhaus conjecture for* A_5. Prod. Indian Acad Sci. **99** (1989), 1 – 5.

[MRSW] Marciniak/Ritter/Sehgal/Weiss, *Torsion units in integral group rings of some metabelian groups, II.* J. of Nb. Th. **25** (1987), 340 – 352.

[PM] Polcino Milies, *The units of the integral group ring* $\mathbb{Z}D_4$. Bol. Soc. Brasil Mat. **4** (1972), 85 – 92.

[PRS] Polcino Milies/Ritter/Sehgal, *On a conjecture of Zassenhaus on torsion units in integral group rings,* II. Proc. AMS **97** (1986), 201 – 206.

[PS] Passmann/Smith, *Units in integral group rings.* J. of Alg. **69** (1981), 213 – 239.

[Rq] Roquette, *Realisierung von Darstellungen endlicher nilpotenter Gruppen.* Arch. Math. **9** (1958), 241 – 250.

[RS_1] Ritter/Sehgal, *Integral group rings with trivial central units.* To appear in Proc. AMS.

[RS_2] Ritter/Sehgal, *Integral group rings of some p-groups.* Canad. J. Math. **34** (1982), 233 – 246.

[RS_3] Ritter/Sehgal, *Certain normal subgroups of units in group rings.* Crelle J. **381** (1987), 214 – 220.

[RS_4] Ritter/Sehgal, *On a conjecture of Zassenhaus on torsion units in integral group rings.* Math. Ann. **264** (1983), 257 – 270.

[RS_5] Ritter/Sehgal, *Generators of subgroups of $U(\mathbb{Z}G)$.* Contemp. Math. **93** (1989), 331 – 347.

[RS_6] Ritter/Sehgal, *Construction of units in integral group rings of finite nilpotent groups.* To appear in Trans. AMS.

[RS_7] Ritter/Sehgal, *Construction of units in group rings of monomial and symmetric groups.* To appear in J. of Alg.

[RSc_1] Roggenkamp/Scott, *On a conjecture of Zassenhaus for finite group rings.* Preprint.

[RSc_2] Roggenkamp/Scott, *Isomorphisms of p-adic group rings.* Ann. of Math. **126** (1987), 593 – 647.

[RSc_3] Roggenkamp/Scott, *Units in group rings.* Proc. Singapore 1987.

[RW] Ritter/Weiss, *An absolutely irreducible group representation which is realizable over its character field but not integrally.* Preprint.

[Se] Serre, *Le problème des groupes de congruence pour SL_2,* Ann. of Math. **92** (1970), 489 – 527.

[Sg] Sehgal, *Topics in group rings.* Marcel Dekker Inc. 1978.

[Si] Siegel, *Discontinuous groups.* Ann. of Math. **44** (1943), 674 – 689.

[SW] Sehgal/Weiss, *Torsion units in integral group rings of some metabelian groups.* J. of Alg. **103** (1986), 490 – 499.

[T_1] Trama, *Units in certain integral group rings.* Preprint.

[T_2] Trama, *Letter dated August 21, 1989*

[Ti] Tits, *Traveaux de Margulis* ... Séminaire Bourbaki 1975/76, LNM **567** (Springer-Verlag).

[Ty] Taylor, *Classgroups of group rings.* Cambridge Univ. Press 1984.

[V_1] Vaserstein, *The structure of classic arithmetic groups of rank greater than one.* Math. USSR Sb. **20** (1973), 257 - 270.

[V_2] Vaserstein, *On the group SL_2 over Dedekind rings of an arithmetic type.* Math. USSR Sb. **18** (1973), 321 - 332.

[Wa] Washington, *Introduction to cyclotomic fields.* Springer-Verlag 1982.

[Ws_1] Weiss, *Rigitity of p-adic p-torsion.* Ann. of Math. **127** (1988), 317 - 332.

[Ws_2] Weiss, *Letter dated August 16, 1989.*

[Zs] Zassenhaus, *Über endliche Festkörper.* Hamburg. Abh. **11** (1935), 187 - 220.

Institut für Mathematik
Universität Augsburg
D - 8900 Augsburg, Germany