CONSTRUCTION OF UNITS IN INTEGRAL GROUP RINGS OF FINITE NILPOTENT GROUPS

JÜRGEN RITTER AND SUDARSHAN K. SEHGAL

ABSTRACT. Let U be the group of units of the integral group ring of a finite group G. We give a set of generators of a subgroup B of U. This subgroup is of finite index in U if G is an odd nilpotent group. We also give an example of a 2-group such that B is of infinite index in U.

1. INTRODUCTION

Let $U = U(\mathbb{Z}G)$ be the group of units, having augmentation one, of the integral group ring $\mathbb{Z}G$ of a finite group G, namely,

$$U = \left\{ u = \sum a_g g \in \mathbb{Z}G \,\middle|\, \sum a_g = 1 \text{ and there exists } v \in \mathbb{Z}G \text{ with } uv = 1 \right\}.$$

It is a basic question to describe constructively, for example, by giving generators, the elements of U. Bass and Milnor [2] have done this for a subgroup of finite index in U for abelian groups G. We shall do the same for nilpotent groups G with a few exceptions concerning their Sylow 2-groups.

We begin by describing units of $\mathbb{Z}\langle a \rangle$ where $a \in G$ is an element of order d. Let $|G| = n$ and $\varphi(n) = m$, where φ is the Euler function. For a natural number i, relatively prime to d and $1 < i < d$, the element

$$u = (1 + a + \cdots + a^{i-1})^m + \frac{1 - i^m}{d}\hat{a}, \qquad \hat{a} = 1 + a + \cdots + a^{d-1},$$

is integral, as $i^m \equiv 1 \pmod{d}$, and belongs to U. These units correspond to the circular units of cyclotomic fields and Bass [2] has proved that if G is *cyclic* then a subset of units of the above type obtained for all $\langle a \rangle$ gives a linear independent set of generators of a subgroup of finite index in $U(\mathbb{Z}G)$. We call the units obtained by varying $\langle a \rangle$ and i, the Bass cyclic units of $\mathbb{Z}G$.

We have other units which are attached to two elements $a, b \in G$:

$$u_{a,b} = 1 + (a - 1)b\hat{a} \quad \text{with } u_{a,b}^{-1} = 1 - (a - 1)b\hat{a}.$$

We shall call the units $\{u_{a,b} | a, b \in G\}$ the bicyclic units of $\mathbb{Z}G$. Clearly, if a and b commute then $u_{a,b} = 1$. With this notation our main result on units is:

Theorem A. *Suppose that G is a nilpotent group such that the rational group algebra $\mathbb{Q}G$ has no simple components which are 2×2 matrices over $\mathbb{Q}$ or $\mathbb{Q}(i)$ or $2^r \times 2^r$ matrices, $r > 0$ over $\mathbb{H}_k$, $k \geq 3$, the Hamilonian quaternions over $\mathbb{Q}(\zeta_{2^{k-1}} + \zeta_{2^{k-1}}^{-1})$ where $\zeta_{2^{k-1}}$ is a 2^{k-1}th primitive root of unity. Then the Bass cyclic units and the bicyclic units of $\mathbb{Z}G$ generate a subgroup of finite index in $U(\mathbb{Z}G)$.*

Obviously, the restrictions are on the Sylow 2-subgroup of G. If G is a 2-group some restrictions are necessary. For instance, if G is the group of order 16 given by

$$G = \langle a, b | a^4 = 1 = b^4, a^b = a^{-1} \rangle$$

then the group generated by the Bass cyclics and bicyclics is of infinite index. This is proved in §6.

The proof of the theorem is reduced to assertions (3.5) and (3.6) in §3; the assertions themselves are shown in §5. Their proofs depend on a canonical way of writing an absolutely irreducible representation T of a p-group G as an induced representation. Namely, depending on T we find a distinct maximal subgroup M of G together with an irreducible representation V of M inducing T such that, among other important properties, T and V have the same character field (see §4). This method also gives a new and direct proof of the next Proposition (cf. [14]). The result for p-groups, for a regular prime goes back to Schur [4, p. 158].

Proposition. *If G is a nilpotent group which does not have a homomorphic image the quaternion group of order 8 or the dihedral group of order 8, then each representation of G is realizable over the algebraic integers in its character field.*

We remark that just as in the case of cyclotomic fields, one can expect, in general, to construct U up to a finite index only, as we have done for our nilpotent groups G. While talking about units, it is appropriate to mention recent theorems of Roggenkamp and Scott [13] and Weiss [18] where they have characterized certain finite groups of units up to conjugacy.

2. NOTATIONS AND NEEDED RESULTS

We fix some notations and state some important results that we shall need. $\mathbb{Q}G$ is the rational group algebra of a finite group G and $\mathbb{Z}G$ is its integral group ring. The groups G in our paper are such that their Wedderburn components S_i,

$$\mathbb{Q}G = S_1 \oplus \cdots \oplus S_t,$$

are either matrix rings $S_i = (K_i)_{n_i \times n_i}$ over number fields K_i or $S_i = \mathbb{H}_k$, the Hamilton quaternion field over the real field $\mathbb{Q}(\zeta_{2^{k-1}} + \zeta_{2^{k-1}}^{-1})$ for some $k \geq 3$, where ζ_l, for $l \in \mathbb{N}$, is a primitive lth root of unity; see §7. π_i denotes the projection of $\mathbb{Q}G$ onto S_i. Let $\mathscr{O}_i$ be the ring of algebraic integers in the field K_i. Then $(\mathscr{O}_i)_{n_i \times n_i}$ is a maximal order in $S_i = (K_i)_{n_i \times n_i}$. We

denote by GL_i or $GL(n_i, \mathscr{O}_i)$ the group of units of $(\mathscr{O}_i)_{n_i \times n_i}$ and by SL_i or $SL(n_i, \mathscr{O}_i)$ the subgroup of determinant one. In §4 we shall show the projection $\pi_i \colon \mathbb{Q}G \to S_i = (K_i)_{n_i \times n_i}$ actually maps $\mathbb{Z}G$ into $(\mathscr{O}_i)_{n_i \times n_i}$. Let Δ_k be some maximal order in $\mathbb{H}_k$, then $SL_1(\Delta_k)$, the group of units of Δ_k of reduced norm one, is finite [11, p. 216].

For an ideal $\mathscr{Q}$ of $\mathscr{O}_i$ we denote by $E(\mathscr{Q})$ the subgroup of SL_i generated by all $\mathscr{Q}$-elementary matrices, $I + qe_{lm}$, $q \in \mathscr{Q}$, $l \neq m$, e_{lm} a matrix unit and by $\widetilde{E}(\mathscr{Q})$ its normal closure in SL_i. It is well known that if $n \geq 3$ then the normal subgroup of $E(\mathscr{O}_i)$ generated by $E(\mathscr{Q})$ is normal in SL_i and hence coincides with $\widetilde{E}(\mathscr{Q})$. With this notation, the congruence theorems of Bass-Milnor-Serre [3] and Serre [15] read as follows. See also [1].

Lemma 2.1. *Assume that either $n_i \geq 3$ or $n_i = 2$ and S_i is not a 2×2 matrix ring over the rational field or an imaginary quadratic field. Then*

(1) *$[SL_i : \widetilde{E}(\mathscr{Q})]$ is finite for any nonzero ideal $\mathscr{Q}$ of $\mathscr{O}_i$.*

(2) *Every noncentral subgroup of SL_i normalized by a subgroup of finite index contains $\widetilde{E}(\mathscr{Q})$ for some nonzero ideal $\mathscr{Q}$ of $\mathscr{O}_i$.*

We shall also need the following result due to Vaserstein [16, 17], compare also [9].

Lemma 2.2. *(1) If $n_i \geq 3$, then $\widetilde{E}(\mathscr{Q}^2) \subseteq E(\mathscr{Q})$; in particular, $[SL_i : E(\mathscr{Q})] < \infty$.*

(2) If $n_i = 2$ and K_i is not rational or imaginary quadratic, then

$$[SL_i : E(\mathscr{Q})] < \infty.$$

We shall denote by B_1 and B_2, respectively, the subgroups of $U = U(\mathbb{Z}G)$ generated by the Bass cyclic units and the bicyclic units of $\mathbb{Z}G$ whereas we shall denote by B the group generated by B_1 and B_2. We note that generators of B_2 are of the form $1 + \alpha$, $\alpha^2 = 0$ and thus $\pi_i(B_2)$ has determinant one if $n_i > 1$, however, if $n_i = 1$ or $S_i = \mathbb{H}_k$, $\pi_i(B_2) = 1$. Finally, Z will be the center of U.

3. REDUCTIONS AND PLAN OF PROOF

We shall need the following result.

Lemma 3.1. *The images of the Bass cyclic units of $\mathbb{Z}G$ under the natural map $j \colon U(\mathbb{Z}G) \to K_1(\mathbb{Z}\mathbb{G})$ generate a subgroup of finite index.*

Proof. See Bass [2].

Lemma 3.2. *In order to prove our theorem it suffices to prove*

(3.3)   *B_2 contains a subgroup $F = \prod_{i=1}^{t} F_i$ with a subgroup F_i of finite index in SL_i for $n_i > 1$ and $F_i = 1$ elsewhere.*

Proof. Let $z \in Z$, the center of U. Then by (3.1) there exists an integer m, independent of z, such that $j(z^m b^{-1}) = 1$ for some $b \in B_1$. This means that a suitable matrix

$$\begin{pmatrix} z^m b^{-1} & & & \\ & 1 & & \\ & & \ddots & \\ & & & 1 \end{pmatrix}$$

is a commutator. Therefore, $\pi_i(z^m b^{-1})$ has determinant one if $n_i > 1$, and so, by (3.3), $\pi_i(z^{mq} b^{-q}) \in B_2$ for some q. If $n_i = 1$, $\pi_i(z^m b^{-1}) = 1$, and if S_i is a definite quaternion algebra, then $nr(\pi_i(z^m b^{-1})) = 1$ and $\pi_i(z^{ml} b^{-l}) = 1$, for a suitable l [11, p. 216]. We have proved that $z^{mql} b^{-mql} \in B_2$. Thus $z^{mql} \in B$ and B contains a subgroup of finite index in Z. Now, since $[GL_i : SL_i \mathscr{O}_i^\times] < \infty$, we conclude that $[U : B] < \infty$.

Lemma 3.4. *In order to prove* (3.3) *and hence our theorem it suffices to prove*
   (3.5) $[SL_i : \pi_i(B_2)] < \infty$ *for all* $n_i > 1$; *and*
   (3.6) *for all* $i \neq j$, $n_i, n_j > 1$, *there is an element* $b \in B_2$ *such that* $\pi_i(b) = 1$, $\pi_j(b)$ *is noncentral.*

Proof. First, recall that $\pi_i(B_2) = 1$ for all $n_i = 1$. Now, given $n_l > 1$, we shall produce a subgroup F_l of finite index in SL_l such that B_2 contains $(1, \ldots, 1, F_l, 1, \ldots)$. We know by (3.6) that given $i \neq j$ with $n_i, n_j > 1$, B_2 contains an element $(\ldots, 1, \ldots, \varepsilon, \ldots)$ with 1 in the ith place and a noncentral matrix ε in the jth place. Then B_2 contains

$$(\ldots, 1, \ldots, \varepsilon, \ldots)^{B_2} = (\ldots, 1, \ldots, \varepsilon^{B_2}, \ldots) = (\ldots, 1, \ldots, \varepsilon^{\pi_j(B_2)}, \ldots).$$

The group $\varepsilon^{\pi_j(B_2)}$ is normalized by $\pi_j(B_2)$ which is of finite index in SL_j by (3.5). This group intersects SL_j noncentrally and is normalized by $\pi_j(B_2) \cap SL_j$, which is of finite index in SL_j. Thus by (2.1), $\varepsilon^{\pi_j(B_2)}$ contains a group F_j of finite index in SL_j. Suppose, we have proved by induction that B_2 contains

$$(\ldots, \overbrace{1, 1, \ldots, 1}^{r}, \ldots, F_j, \ldots)$$

where there are r 1's and F_j is of finite index in jth place. Since the 1's are allowed to appear any place, we also have in B_2 a group

$$(\ldots, \overbrace{1, 1, \ldots, 1}^{(r-1)}, \ldots, F_j', 1, \ldots)$$

with F_j' of finite index. Taking commutators, with $N_j = F_j \cap F_j'$, B_2 contains

$$(\ldots, \overbrace{1, 1, \ldots, 1}^{r}, \ldots, \ldots [N_j, N_j], 1, \ldots).$$

Now N_j is of finite index and $[N_j, N_j] \triangleleft N_j < SL_j$. It follows as above that B_2 contains a group with $(r+1)$ 1's and jth component of finite index. By induction B_2 contains groups with a subgroup of finite index in one component and one elsewhere. This completes the proof of the lemma.

Remark. For p-groups we shall even show (see (5.2)):

(3.6)$'$ b can be chosen to be of the form $b = 1 + (x-1)f\hat{x}$ with $x \in G$, $f \in \mathbb{Z}G$.

Once we have proved (3.3) for the groups of our theorem we would also have proved the following theorem.

Theorem A$'$. $\langle Z, B_2 \rangle$ *is of finite index in* U.

4. THE MAIN PROPOSITIONS

We introduce the following notation:

For a square matrix Y having entries in a field $|Y|_1$ is the multiplicity of 1 as eigenvalue of Y.

$Q_{2^k} = \langle a, b : a^{2^{k-1}} = 1, a^{2^{k-2}} = b^2, a^b = a^{-1} \rangle$ is the generalized quaternion group of order 2^k, $k \geq 3$.

$D_{2^k} = \langle a, b : a^{2^{k-1}} = 1 = b^2, a^b = a^{-1} \rangle$ is the dihedral group of order 2^k, $k \geq 3$.

$D_{2^{k+1}}^\varepsilon = \langle a, b : a^{2^k} = 1 = b^2, a^b = a^{\varepsilon \cdot 1 + 2^{k-1}} \rangle$ with $\varepsilon = +$ or $-$; these groups have order 2^{k+1}, $k \geq 3$.

Our first lemma is well-known.

Lemma 4.1. *The only nonabelian p-groups, p being any prime, in which every abelian normal subgroup is cyclic, are* Q_{2^k}, D_{2^k}, $D_{2^{k+1}}^-$.

Namely, from [7, p. 304] we get at once that $p = 2$ and the groups in question have a cyclic normal subgroup of index 2. By applying [6, p. 187] we are left with finding a noncyclic abelian normal subgroup in $D_{2^{k+1}}^+$, as, for example, $\langle a^{2^{k-1}}, b \rangle$.

Now we are in the position to state our main result.

Proposition A. *Assume that G is a p-group different from* Q_{2^k}, D_{2^k}, $D_{2^{k+1}}^-$. *Let T be an absolutely irreducible faithful representation of G of degree p^n, $n \geq 1$. Then there exists 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* $T = \operatorname{ind}_M^G V$, $V(a) = 1$, $|V(a^b)|_1 = 0$ ($\forall b \notin M$).

Before going into the proof of Proposition A we would like to deduce two important corollaries.

Corollary 1. *In the situation of Proposition* A *the character fields belonging to the representations T and V coincide.*

In order to see this we first denote by χ and ψ the characters of the representations and then recall that $\chi = \mathrm{ind}_M^G \psi$. Thus $\mathbb{Q}(\chi) \subset \mathbb{Q}(\psi)$. If the containment was proper, we would have a nontrivial automorphism $\alpha \in \mathrm{Gal}(\mathbb{Q}(\psi)/\mathbb{Q}(\chi))$, and consequently χ would lie above both, ψ and $\psi^\alpha \neq \psi$. As a result $\psi^\alpha = \psi^b$ for some $b \in G \backslash M$. Plugging in the element a from the proposition then gives the desired contradiction.

Corollary 2. *A simple Wedderburn component S of the rational group algebra $\mathbb{Q}G$ of a p-group is a matrix ring either over $\mathbb{Q}(\chi)$ the character field of an absolutely irreducible representation, or over $\mathbb{H}_k$, the Hamilton field over $\mathbb{Q}(\zeta_{2^{k-1}} + \zeta_{2^{k-1}}^{-1})$. In the former case, the representation is realizable over $\mathscr{O}_\chi$, the ring of integers in $\mathbb{Q}(\chi)$.*

Proof. We first observe that

$$\mathbb{Q}D_{2^k} = \begin{cases} \mathbb{Q}D_{2^{k-1}} \oplus K_{2\times 2}, & k \geq 4, \qquad K = \mathbb{Q}(\zeta_{2^{k-1}} + \zeta_{2^{k-1}}^{-1}), \\ 4\mathbb{Q} \oplus K_{2\times 2}, & k = 3, \qquad K = \mathbb{Q}, \end{cases}$$

$$\mathbb{Q}D_{2^{k+1}}^- = \mathbb{Q}D_{2^k} \oplus K_{2\times 2}, \qquad K = \mathbb{Q}(\zeta_{2^k} + \zeta_{2^k}^{-1}),$$

$$\mathbb{Q}Q_{2^k} = \begin{cases} \mathbb{Q}D_{2^{k-1}} \oplus \mathbb{H}_k, & k \geq 4, \\ 4\mathbb{Q} \oplus \mathbb{H}, & k = 3, \ \mathbb{H}_3 = \mathbb{H}. \end{cases}$$

Therefore, we may suppose that G is not one of these groups. Let T be an absolutely irreducible representation belonging to S. We may assume that T is faithful. Then by the Proposition, $T = \mathrm{ind}_M^G V$. By induction, V is realizable over $\mathbb{Q}(\psi)$ and in fact over $\mathscr{O}_\psi$ or belongs to $(\mathbb{H}_k)_{r\times r}$. In the first case, T is realizable over $\mathbb{Q}(\psi) = \mathbb{Q}(\chi)$ and thus over $\mathscr{O}_\chi$. In the second case, it is readily seen that T belongs to $(\mathbb{H}_k)_{2r\times 2r}$.

An immediate consequence of this corollary is a theorem of Roquette [14] which states that the Schur index with respect to a number field F of an absolutely irreducible representation of a p-group is 1 if either p is odd or if $p = 2$ and F contains the 4th roots of unity.

In fact, the argument shows more, namely, each absolutely irreducible representation of a nilpotent group G is realizable over the ring of integers in its character field, provided G does not have D_8 or Q_8 as a homomorphic image. This has also been stated as a proposition in the introduction. For the proof observe:

Since G is the direct product of its Sylow subgroups, and since an absolutely irreducible representation T of G can be written as the tensor product of absolutely irreducible representations T_i of the Sylow subgroups P_i [7, p. 516], and as, moreover, the ring $\mathscr{O}$ of integers in the character field of T is the composite of the rings of integers in the character fields of the corresponding T_i [8, p. 75], we may assume that G is a p-group. The result follows from Corollary 1; T can be assumed to be a faithful representation. We simply note that the exceptional groups in Lemma 4.1 all map homomorphically onto Q_8 or D_8.

After a long detour we return to our proper topic.

Proof of Proposition A. In due sequence we are going to show the following.

(A1) Given an absolutely irreducible representation T' of our group G, there is a maximal abelian normal subgroup A of G, a subgroup S of G containing A, and an abelian character σ of S such that $T' = \mathrm{ind}_S^G(\sigma)$, $\ker\sigma \cap A \neq 1$.

(A2) Let $W = \{x \in \ker\sigma \cap A, x^p = 1\}$. Then $W \neq 1$ and, if $T' = T$, W is of index p in $A_p = \{x \in A, x^p = 1\}$. Hence when looking at A_p as an $\mathbb{F}_p$-vector space of dimension m, say, W is a hyperplane in A_p. There is a basis $v_1, \ldots, v_m$ of A_p such that the natural action of G on the normal subgroup A_p induces a homomorphism

$$G \to G_m = \left\{ \begin{pmatrix} 1 & & \alpha_{ij} \\ & \ddots & \\ & & 1 \end{pmatrix} : \alpha_{ij} \in \mathbb{F}_p, \ 1 \le i < j \le m \right\}.$$

In terms of this basis W is given as

$$\left\{ \sum_{i=1}^m \alpha_i v_i : \alpha_i \in \mathbb{F}_p, \ \sum_{i=1}^m \gamma_i \alpha_i = 0 \right\}$$

for a fixed vector $(\gamma_1, \ldots, \gamma_m)$ with entries in $\mathbb{F}_p$. We have $\gamma_1 \neq 0$.

(A3) For $x \in W$ define $M_x = \{s \in G_m : sx \in W\}$. There is a $0 \neq a \in W$ such that M_a is a maximal subgroup in G_m.

(A4) If $x \in W$, then $|T'(x)|_1 = \#M(x)/|S|$ where $M(x) = \{y \in G : x^{y^{-1}} \in W\}$.

The sets $M(x)$ have the properties

$$1 \in M(x);$$
$$y \in M(x) \& s \in S \Rightarrow sy \in M(x);$$
$$y \in M(x) \& z \in Z_G(A_p) \Rightarrow yz, zy \in M(x).$$

We then choose a as in (A3) and see that $M = M(a)$ is a maximal subgroup of G. Observe that $M(a)$ is the preimage of M_a in G and thus is maximal in G or all of G. In the latter case we would have $a \in \bigcap_{y \in G} W^y$, and thus $T(a) = 1$ contrary to our assumption that T is faithful. Because of (A1) and (A4), $A \le S \le M$. Thus, if we define $V = \mathrm{ind}_S^M(\sigma)$, (A1) implies $\mathrm{ind}_M^G V = T$. Moreover, in view of (A4),

$$|T(a)|_1 = |V(a)|_1 = p^{n-1} = \dim V,$$

forcing $V(a) = 1$ as well as $|V(a^b)|_1 = 0$ for $b \notin M$. Since $a \in A \le S$, A is an abelian normal subgroup of G, and as $V = \mathrm{ind}_S^M \sigma$, and $T = \mathrm{ind}_S^G \sigma$, we get diagonal forms for both, $V(a)$ and $T(a)$. Regarding the proof of Proposition A we are left with showing (A1) to (A4).

Proof of (A1). This is well known. For the convenience of the reader we repeat the argument. Choose a maximal abelian normal subgroup A of G and restrict T' to A. Let w be a constituent of $\text{res}_A^G T'$ and S_w be the stabilizer group of w in G. From Clifford's theory [7, V17] we get an irreducible representation T_w of S_w that induces T' and whose restriction to A is $p^r w$ with $p^r = \dim T_w$. Since p-groups are monomial, $T_w = \text{ind}_S^{S_w}(\sigma)$ for some $S \le S_w$ and some abelian character σ of S. In particular, $T' = \text{ind}_S^G \sigma$. We restrict to A and use Mackey's formula [7, p. 558]:

$$p^r w = \text{res}_A^{S_w} \text{ind}_S^{S_w}(\sigma) = \sum_y \text{ind}_{S^y \cap A}^A \text{res}_{S^y \cap A}^{S^y}(\sigma^{y^{-1}}),$$

where the sum is taken over a set of representatives of SA in S_w. If $S^y \cap A$ was a proper subgroup of A, then we would have at least two different characters of A occurring in $\text{ind}_{S^y \cap A}^A(\text{res}_{S^y \cap A}^{S^y} \sigma^{y^{-1}})$. Hence $S^y \cap A = A$, or, what amounts to the same, $A \subset S$. Assume next that $\ker \sigma \cap A = 1$. So A, being a subgroup of $S/\ker \sigma$, is cyclic. Since we can do all this by choosing any maximal abelian normal subgroup A in G, we are left with the possibility that all the A are cyclic. But this contradicts Lemma 4.1.

Proof of (A2). Because we are dealing with p-groups, $W \ne 1$. Moreover, as A_p/W turns out to be a subgroup of $S/\ker \sigma$, it is cyclic and thus already of order 1 or p, since A_p has exponent p. $A_p = W$ would force W to be normal in G and hence to lie in the kernel of T, which is trivial. In particular, $m \ge 2$. The natural action of G on A_p induces a homomorphism $G \to \text{Aut}_{\mathbb{F}_p}(A_p)$, the image of which is a p-subgroup of $\text{Aut}_{\mathbb{F}_p}(A_p)$. By choosing a basis of A_p we identify $\text{Aut}_{\mathbb{F}_p} A_p = GL_m(\mathbb{F}_p)$, the Sylow p-groups of which are $tG_m t^{-1}$ for $t \in GL_m(\mathbb{F}_p)$ [7, p. 185]. Hence by choosing the basis appropriately, we will arrive at a homomorphism $G \to G_m$. It has kernel $Z_G(A_p)$. Observe that $y \in G$ acts on A_p, $x \mapsto x^{y^{-1}}$, exactly as its image s in G_m does, $x \mapsto sx$.

　　If we think of the hyperplane W in A_p as being given by a linear form $f: A_p \to \mathbb{F}_p$, then our vector $(\gamma_1, \dots, \gamma_m)$ is just $(f(v_1), \dots, f(v_m))$ with the basis $v_1, \dots, v_m$ of A_p from above. Assume $\gamma_1 = 0$. Then $v_1 \in W$. As $sv_1 = v_1$ for all $s \in G_m$, we have $v_1^{y^{-1}} = v_1$ for all $y \in G$, which implies v_1 to be central and thus to lie in the kernel of T, a contradiction.

Proof of (A3). We first suppose that $\gamma_2 \ne 0$. Solve $\gamma_1 + \gamma_2 \alpha = 0$, i.e. $\alpha = -\gamma_1/\gamma_2 \ne 0$, and set $a = v_1 + \alpha v_2$. Then $s \in M_a$ means that the $(1, 2)$-entry α_{12} of the matrix s is zero. Thus M_a is the subgroup $\widetilde{G}_m$ in G_m defined by $\alpha_{12} = 0$ and so maximal.

　　Next let $\gamma_2 = 0$. Then $v_2 \in W$ and so $sv_2 \in W$ as long as $s \in \widetilde{G}_m$. Thus again $M_a = \widetilde{G}_m$ is maximal, if $a = v_2$.

Proof of (A4). From the definition of the scalar product of characters we get

$$|T'(x)|_1 = (\mathrm{res}^G_{\langle x \rangle} \mathrm{ind}^G_S(\sigma), 1)_{\langle x \rangle}.$$

Thus by applying Mackey's formula as well as Frobenius reciprocity [7, p. 555 and 558] we deduce

$$|T'(x)|_1 = \sum_y (\mathrm{ind}^{\langle x \rangle}_{\langle x \rangle \cap S^y} \mathrm{res}^{S^y}_{\langle x \rangle \cap S^y} \sigma^{y^{-1}}, 1)_{\langle x \rangle}$$

$$= \sum_y (\mathrm{res}^{S^y}_{\langle x \rangle \cap S^y} \sigma^{y^{-1}}, 1)_{\langle x \rangle \cap S^y},$$

the summation running over all y from a coset representative set of S in G. Recall that $x \in A \le S$ and $A \triangleleft G$, and so $Sy\langle x \rangle = S\langle x^{y^{-1}} \rangle y = Sy$. It follows that

$$|T'(x)|_1 = \#\{y \bmod S : \langle x \rangle \cap S^y \le \ker \sigma^{y^{-1}}\}$$

$$= \#\{y \bmod S : \langle x^{y-1} \rangle \cap S \le \ker \sigma\}.$$

Since $x \in W$, this last number evidently equals $\#M(x)/|S|$. The stated properties of $M(x)$ are obvious because $W \triangleleft S$.

Proposition B. *Assume that in addition to the representation T of Proposition A we are given a second absolutely irreducible representation T' of G. Then we can arrange to get the data in Proposition A so that there is an irreducible representation V' of M inducing T' provided that $0 \ne |T'(a)|_1 \ne \dim T'$.*

Proof. As has been carried out in (A1), with respect to T' we have a subgroup R in G containing our A and an abelian character ρ of R such that $T' = \mathrm{ind}^G_R \rho$; along with ρ there is the subgroup $W' = \ker \rho \cap A_p$. As $0 \ne |T'(a)|_1 \ne \dim T'$, after passing from (R, ρ) to a conjugate pair $(R^y, \rho^{y^{-1}})$ if need be, we shall have $a \in V$ but $a \notin \bigcap_{y \in G} W'^y$. In particular, V is a hyperplane in A_p. Let W' be given in terms of the linear form $g = (\lambda_1, \ldots, \lambda_m)$; recall that W belongs to $(\gamma_1, \ldots, \gamma_m)$, $\gamma_1 \ne 0$. We again distinguish two cases. First suppose that $\gamma_2 \ne 0$. Then $a = v_1 + \alpha v_2$ by (A3). If λ_1 was zero, then λ_2 would have to be zero as well as a is in V. Consequently, $a^{y^{-1}} = \beta_1 v_1 + \beta_2 v_2$ (for some $\beta_1, \beta_2 \in \mathbb{F}_p$) would belong to W' for every $y \in G$; observe here that we have computed $a^{y^{-1}}$ by letting y correspond to the appropriate matrix in G_m. Since $a \notin \bigcap_{y \in G} V^y$, λ_1 cannot be zero. Thus switching over from g to $\gamma_1/\lambda_1 \cdot g$ yields $\lambda_1 = \gamma_1$ and hence $\lambda_2 = \gamma_2$, as $a \in W' \cap W$. A striking consequence of this is the following:

$$y \in M \Leftrightarrow a^{y^{-1}} \in W \Leftrightarrow a^{y^{-1}} \in W',$$

from which we deduce $R \le M$. As $W' \triangleleft R$, this implies the assertion of Proposition B.

There is still the case $\gamma_2 = 0$. Then $a = v_2$ by (A3). We know that the maximal subgroup M is the preimage of $\widetilde{G}_m$ and so there is an element $y \in G$ corresponding to a matrix s in G_m which is not in $\widetilde{G}_m$. Using this y we pass from W' to $W^{y^{-1}}$, from W to $(W')^{y^{-1}}$, and from a to $a^{y^{-1}}$. Observe now that the linear form determining $W^{y^{-1}}$ is $(\gamma_1, 0, \gamma_3, \ldots, \gamma_m) \cdot s^{-1} = (\gamma_1, -\gamma_1\beta, \ldots)$ with $\beta \neq 0$ being in the $(1, 2)$-position of s. It follows that we are back to the case that has already been dealt with.

5. THE PROOFS OF PROPERTIES (3.5) AND (3.6) FOR p ODD

Proposition 5.1. *If G is a p-group with p odd, and if T is a nonabelian absolutely irreducible representation of G, then property (3.5) holds for the component of $\mathbb{Q}G$ that belongs to T.*

Proof. From Corollary 2 to Proposition A we know that T is realizable over the integers of $\mathbb{Q}(\chi)$ and so T itself serves as a projection onto the component in question. Denote by $\overline{T}$ the faithful representation of $\overline{G} = G/\ker T$ given by T. Then $T(u_{a,b}) = T(1 + (a-1)b\hat{a}) = \overline{T}(1 + (\overline{a}-1)\overline{b}(r\hat{\overline{a}})) = \overline{T}(u_{\overline{a},\overline{b}})^r$ with $r = \operatorname{ord}(a)/\operatorname{ord}(\overline{a})$. So r is a divisor of q, the order of G. Thus, if we only can show that $\langle \overline{T}(u_{\overline{a},\overline{b}})^q : \overline{a}, \overline{b} \in \overline{G}\rangle$ is of finite index in $SL_{p^n}(\mathcal{O})$, where $p^n = \dim T = \dim \overline{T}$ and $\mathcal{O}$ is the ring of integers in $\mathbb{Q}(\chi) = \mathbb{Q}(\overline{\chi})$, then

$$\langle T(u_{a,b}) : a, b \in G\rangle \geq \langle \overline{T}(u_{\overline{a},\overline{b}})^q : \overline{a}, \overline{b} \in \overline{G}\rangle$$

is of finite index as well. We therefore now suppose that T is faithful and, as a consequence, we are in the situation of Proposition A. Choose $a \in A \leq M$ and V, ψ as before and fix some element $b \notin M$. With respect to the coset representatives $1, b, \ldots, b^{p-1}$ of M in G we may write

$$T(a) = \begin{pmatrix} 1 & & & & & \\ & \ddots & & & & \\ & & 1 & & & \\ & & & w_e & & \\ & & & & \ddots & \\ & & & & & w_{p^n} \end{pmatrix},$$

$$T(bm) = \begin{pmatrix} 0 & V(m) & & & \\ & & V(m^b) & & \\ & & & \ddots & \\ & & & & V(m^{b^{p-2}}) \\ V(b^p m^{b^{p-1}}) & 0 & & \cdots & 0 \end{pmatrix},$$

where $e = p^{n-1} + 1$, $w_i^p = 1$, but $w_i \neq 1$, and $m \in M$. Recall at this stage that $T = \operatorname{ind}_S^G \sigma$, $a \in A \leq S \leq M$, $A \triangleleft G$. We compute $T(q \cdot (u_{a,bm} - 1))$ for $m \in M$.

$T(q(a-1)bm\widehat{a})$

$$= q \begin{pmatrix} 0 & & & \\ & \ddots & & \\ & & 0 & \\ & & & \pi_e \\ & & & & \pi_{p^n} \end{pmatrix} T(bm) \begin{pmatrix} p & & & & \\ & \ddots & & & \\ & & p & & \\ & & & 0 & \\ & & & & \ddots \\ & & & & & 0 \end{pmatrix}$$

$$= \begin{pmatrix} & 0 \\ * & \end{pmatrix} \quad \text{with } * = qp \begin{pmatrix} \pi_g & & \\ & \ddots & \\ & & \pi_{p^n} \end{pmatrix} V(b^p m^{b^{p-1}})$$

and $\pi_i = w_i - 1$, $g = p^n - p^{n-1} + 1$.

Since $(1 + q(a - 1)bm\widehat{a})^{-1} = 1 - q(a - 1)bm\widehat{a}$, $(1 + q(a - 1)bm_1\widehat{a})$
$\times(1+q(a-1)bm_2\widehat{a}) = 1+q(a-1)b(m_1+m_2)\widehat{a}$, and as $\{b^p m^{b^{p-1}} : m \in M\} = M$,
we conclude

$$\langle T(1 + q(a - 1)bm\widehat{a}): m \in M \rangle = \begin{pmatrix} 1 & & \\ & \ddots & \\ X & & 1 \end{pmatrix}$$

$$\text{with } X = qp \begin{pmatrix} \pi_g & & \\ & \ddots & \\ & & \pi_{p^n} \end{pmatrix} V(\mathbb{Z}M).$$

This now is a full lattice in the V-component $\mathbb{Q}(\psi)_{p^{n-1} \times p^{n-1}}$ of the group algebra $\mathbb{Q}M$, since q, p, and π_i all are invertible in $\mathbb{Q}(\psi)$. Therefore, for some suitable natural number N, $N\mathscr{O}e_{rs} \subset X$ for all r, s that is

$$(N \cdot \mathscr{O})_{p^{n-1} \times p^{n-1}} \subset X.$$

Working with $q(a - 1)b^i m\widehat{a}$ for $2 \le i \le p - 1$, and with $q(a^{b^j} - 1)b^i m^{b^j} \cdot \widehat{a^{b_j}}$
for $1 \le j \le p - 1$, makes it possible to move the X around and thus yields

$$I + Ne_{ij} \in \langle T(u_{a,b})^q : a, b \in G \rangle$$

for all those $i \ne j$ that do not "correspond to a diagonal block", that is, i, j are not allowed to belong both to any of the sets $\{1 + \nu p^{n-1}, 2 + \nu p^{n-1}, \ldots, p^{n-1} + \nu p^{n-1}\}$ for $0 \le \nu \le p - 1$. In order to get hold of these exceptional pairs i, j as well, we are going to show that given $i \ne j$, there exists an $x \in G$ with $1 + N\mathscr{O}e_{ij} \in \langle T(u_{x,y})^q : y \in G \rangle$ for some natural number N.

Our arguments given so far, together with the equality $\mathbb{Q}(\chi) = \mathbb{Q}(\psi)$, imply this property to be true for T if only we can assure it for the exceptional pairs i, j.

By induction we may assume that we have already proved the respective property for the representation V. Thus given $\gamma \in \mathcal{O}$ and $i \neq j$ between 1 and p^{n-1} we find an element $x \in M$ such that

$$1 + N\gamma e_{ij} = \prod_y V(u_{x,y})^{\pm q};$$

the product being taken over suitable elements $y \in M$. We get

$$1 + pN\gamma e_{ij} = \prod_{\nu=0}^{p-1} \prod_y V(u_{x,a^\nu y})^{\pm q},$$

as $V(a) = 1$.

Since, for each $1 \leq k \leq p - 1$ the matrix $V(a^{b^k})$ is diagonal with primitive pth roots of unity as diagonal entries, we conclude

$$\prod_{\nu=0}^{p-1} \prod_y V(u_{x^{b^k},(a^{b^k})^\nu y^{b^k}})^{\pm q}$$

$$= \prod_y V\left(1 + (x^{b^k} - 1)\left(\sum_{\nu=0}^{p-1} a^{b^k \nu}\right) y^{b^k} \widehat{x^{b^k}}\right)^{\pm q}$$

$$= \prod_y \left(1 + V(x^{b^k} - 1)V\left(\sum_{\nu=0}^{p-1} a^{b^k \nu}\right) V(y^{b^k} \widehat{x^{b^k}})\right)^{\pm q}$$

$$= \prod_y (1 + V(x^{b^k} - 1) \cdot 0 \cdot V(y^{b^k} \widehat{x^{b^k}}))^{\pm q} = 1.$$

So, in fact, using $T = \operatorname{ind}_M^G V$, we arrive at

$$\prod_{\nu=0}^{p-1} \prod_y T(u_{x,a^\nu y})^q = 1 + pN\gamma e_{ij}.$$

For a pair i, j in a set $\{1+\nu p^{n-1}, \ldots, p^{n-1}+\nu p^{n-1}\}$ with $\nu > 0$ the argument is similar. Because of Corollary 1 to Proposition A we know that $\mathbb{Q}(\chi) = \mathbb{Q}(\psi)$ and thus we can apply Lemma 2.2. to complete the proof.

Proposition 5.2. *Let T and T' be two nonabelian absolutely irreducible representations of the p-group G, where p is odd. Then there is an element $u \in B_2$ with $T(u) = 1 + Ne_{ij}$ for some natural number N and $T'(u) = 1$ provided T and T' are not Galois conjugate over $\mathbb{Q}$. Thus (3.6) is valid. Moreover, u can be chosen to be of the form $u = 1 + (x - 1)f\hat{x}$, where $x \in G$, $f \in \mathbb{Z}G$.*

Proof. We show first that we may assume T to be faithful, so that we can apply Proposition B. In fact, if $|T'(a)|_1$ happens to be zero or $\dim T'$, then we need not do much, since then we have $T'(u_{a,b}) = 1$ with the a and b from the last proof. Namely, in this case, $T'(\hat{a}) = 0$, respectively, $T'(a - 1) = 0$. But $T(u_{a,b})$ is noncentral, as has been shown above.

If $\ker T \cap \ker T \neq 1$, we divide it out. If $\ker T \neq 1$, there is a central element z of order p in $\ker T$. So $z \notin \ker T'$. As in the last proof, we find elements $\overline{a}, \overline{b} \in \overline{G} = G/\ker T$ with

$$\overline{T}(u_{\overline{a}, \overline{b}}) = \begin{pmatrix} 1 & & \\ & \ddots & \\ * & & 1 \end{pmatrix}, \qquad * \neq 0;$$

a product of these elements with fixed $\overline{a}$ giving an elementary matrix. Then also $T(u_{a,b}) = \overline{T}(u_{\overline{a}, \overline{b}})^r$ is noncentral, where a and b are preimages of $\overline{a}, \overline{b}$, respectively. Replace b by bz^i. Because $z \in \ker T$, we get a product

$$\prod T\left(\prod_{i=0}^{p-1} u_{a,bz^i}\right) = \prod T(u_{a,b})^p = \text{elementary.}$$

On the other hand,

$$\prod T'\left(\prod_{i=0}^{p-1} u_{a,bz^i}\right) = \prod T'\left(1 + \sum_{i=0}^{p-1}(a-1)bz^i\widehat{a}\right)$$

$$= \prod T'\left(1 + (a-1)b\widehat{a} \cdot \sum_{i=0}^{p-1} z^i\right)$$

$$= T'(1),$$

namely on account of $T'(z) = \text{diag}(\zeta)$ with ζ being a primitive pth root of unity. We are now in the position to apply Proposition B. Of course, V' and V cannot be Galois conjugate over $\mathbb{Q}$, since they induce T' and T, respectively, and these two are assumed not to be Galois conjugate over $\mathbb{Q}$. We will therefore find an element $\mu \in \mathbb{Q}M$ with $V(\mu) = 1$ or e_{12} depending on V being abelian or not, but $V'(\mu) = 0$. Hence there is also an element $\mu \in \mathbb{Z}M$ having the property $V(\mu) = N$ or Ne_{12} for some $N \in \mathbb{N}$ and $V'(\mu) = 0$. Since with m the elements $b^p m^{b^{p-1}}$ run through all of M, μ can be written as an integral linear combination of certain $b^p m^{b^{p-1}}$. Hence we shall get the wanted unit u by simply recalling that combining the elements $b^p m^{b^{p-1}}$ linearly in $\mathbb{Z}M$ amounts to multiplying the corresponding units $u_{a,bm}$ in $\mathbb{Z}G$ as in the proof of (5.1).

6. The case $p = 2$

All groups in this section are 2-groups. Here is where we actually needed p to be odd in our discussion before.

Firstly, we have applied Proposition A which does not hold for $G \in \{Q_{2^k}, D_{2^k}, D_{2^{k+1}}^-\}$. Since we have always reduced our situation to working with faithful irreducible representations, we can carry over the given argument at most to groups G that do not have a homomorphic image in this set. However, the

quaternion group Q_8 of order 8 can be ruled out, because the only nonabelian component of $\mathbb{Q}Q_8$ is $\mathbb{H}$ in which there are only finitely many units. Since, for $k \geq 3$, $Q_{2^{k+1}}$, D_{2^k} and $D_{2^{k+1}}^-$ all map homomorphically onto D_8, we define our first exceptional list E_1 to just consist of the group D_8.

Secondly, we have employed the fact that the matrix sizes of the simple components of the group algebra are at least 3 in order to be able to apply Lemma 2.2. Since in dimension 2 the lemma need not be true when the center is $\mathbb{Q}$ or imaginary quadratic, we better exclude the groups fitting into this situation as well. Thus define E_2 to consist of all groups having a faithful absolutely irreducible representation of dimension 2, Schur index 1, and character field $\mathbb{Q}$ or an imaginary quadratic extension of $\mathbb{Q}$, but which do not project onto D_8.

Thirdly, we have only been dealing with representations that are realizable over their character fields. This need no longer be true for 2-group-representations. Hence we collect in a list E_3 all groups that have a faithful absolutely irreducible representation of dimension 2^{r+1}, $r \geq 1$, and Schur index 2; the corresponding component of the group algebra is $(\mathbb{H}_k)_{2^r \times 2^r}$ due to Corollary 2 of Proposition A. Observe that if a component is just $\mathbb{H}_k$ itself, that is, the representation in question is of dimension 2 and Schur index 2, we have, modulo central units, only finitely many units in this component [11, p. 216] and thus we need not exclude this case.

Putting things together we have arrived at the observation that for 2-groups not having a homomorphic image in E_1, E_2, E_3 the index $[U : B]$ is still finite. We state this in terms of representations in the following proposition.

Proposition 6.1. *Let G be either a dihedral 2-group or such that its rational group algebra does not have a simple component of the following types:*

$$K_{2 \times 2} \quad \text{with } K = \mathbb{Q} \text{ or } \mathbb{Q}(i), \qquad (\mathbb{H}_k)_{2^r \times 2^r} \quad \text{with } k \geq 3, \ r \geq 1.$$

Then $[U(\mathbb{Z}G) : B]$ is finite.

With respect to the dihedral groups we refer to [12]. Regarding the character fields we observe that according to the fact that our groups are monomial these fields are subfields of $\mathbb{Q}(\zeta)$ with ζ being a 2-power root of unity. In here $\mathbb{Q}(i)$ and $\mathbb{Q}(\sqrt{-2})$ are the only imaginary quadratic subfields. The following lemma implies that we need not account for $\mathbb{Q}(\sqrt{-2})$.

Lemma 6.2. $E_2 = \{D_{16}^+, \langle a, b, c : a^2 = 1 = b^2, c^4 = 1, c \text{ central}, a^b = c^2 a \rangle\}$.

Proof. Since by definition G has an absolutely irreducible faithful representation T of dimension 2 and Schur index 1 and since G does not project onto D_8, G and T satisfy the assumptions of Proposition A. Hence $T = \text{ind}_M^G V$ with $[G : M] = 2$ and V abelian. In particular, $M' \subset \ker V$, so $M' \subset \ker T$ as well, as $M' \lhd G$; here M' is the commutator subgroup of M. Thus M is abelian and contains the centre $Z(G)$ of G. Define $R = \ker V$. We claim that $\mathbb{Q}(\chi) = \mathbb{Q}(i)$. As T is faithful, for a fixed $x \in G \backslash M$, $R \cap R^x = 1$. Hence R^x being a subgroup of the cyclic group M/R is cyclic. Thus R is also cyclic. As

$\mathbb{Q}(\psi) = \mathbb{Q}(\chi) = \mathbb{Q}$ or imaginary quadratic, that is $\mathbb{Q}(\psi) = \mathbb{Q}$ or $\mathbb{Q}(i)$ because ψ is abelian, R is of order 2 or 4.

Since $Z(G)$ turns out to be a subgroup of M/R, it is cyclic of order 2 or 4 as well. Summing up we get: If $\mathbb{Q}(\chi) = \mathbb{Q}$, then $|Z(G)| = 2 = |R|$ and so for order reasons already, $G = D_8$ which is not allowed. Consequently, $\mathbb{Q}(\chi) = \mathbb{Q}(i)$. We have

$$R = \langle b \rangle, \qquad |R| = 2 \text{ or } 4, \qquad |M/R| = 4, \qquad |G/M| = 2.$$

First, suppose that $|R| = 4$. Then $c = bb^x$ is a central element of order 4 as $R \cap R^x = 1$. Consequently, $b^x \equiv b^{-1} \not\equiv b \bmod Z(G)$ and G has D_8 as a homomorphic image, which is not allowed. Thus we have $|R| = 2$, $M \supset R$, M is noncyclic of order 8. As M/R is cyclic of order 4, we find an element c of order 4 in M that modulo R generates M/R. After suitable renaming, if necessary, we get $c^x = c$, thereby proving $M = R \times Z(G)$. Namely, if $c^x \neq c$ then $c^x = c^3$ or cb or $c^3 b$. If $c^x = c^3$, replace c by cb and obtain $(cb)^x = c^3 b^x \neq (cb)^3 = c^3 b$. Hence we are left with $c^x = cb$ or $c^3 b$. Then either $c = c^{x^2} = (cb)^x = c^x b^x = cbb^x$ yielding $bb^x = 1$, contrary to $R \cap R^x = 1$ or $c = c^{x^2} = (c^3 b)^x = (c^3 b)^3 b^x = cbb^x$ which is again a contradiction. We write

$$R = \langle b \rangle, \qquad b^2 = 1, \qquad M = R \times Z(G), \qquad Z(G) = \langle c \rangle, \qquad c^4 = 1.$$

Then $b^x b$ being central is c^2 and we have $b^x = bc^2$. The possibilities $x^2 = b, bc, bc^2, bc^3$ lead to the contradiction $c^2 = 1$. Thus for example, if $x^2 = b$ then $b^x = bc^2 = x^2 c^2$, $x^{-1} b = xc^2$, $x^2 = bc^2$, $c^2 = 1$. We are left with $x^2 = 1, c, c^2, c^3$. If $x^2 = 1$ (or c^2) we have

$$G = \langle b, c, x | b^2 = 1 = x^2 = c^4, b^x = bc^2, c \text{ central} \rangle.$$

If $x^2 = c$ (or c^3) we get D_{16}^+. This completes the proof of the lemma.

Proposition 6.3. *Let G be a 2-group mapping homomorphically onto D_8. Then $[U(\mathbb{Z}G) : B]$ is infinite, if the composite map $G \to D_8 \to D_8/\langle a \rangle$ does not split.*

Corollary. 1. *If $G = \langle a, b : a^4 = 1 = b^4, a^b = a^{-1} \rangle$, then $[U(\mathbb{Z}G) : B] = \infty$.*
  2. *If $G = Q_{16}$, then $[U(\mathbb{Z}G) : B] = \infty$.*

Namely, the first group is the semidirect product $\langle a \rangle \rtimes \langle b \rangle$ in which the only elements of order 2 are a^2 and $a^2 b^2$. Modulo the central element b^2 they are sent to a^2 in D_8 and so to 1 in $D_8/\langle a \rangle$. Hence there is no splitting. Also the second group maps onto D_8; the only element of order 2 in Q_{16} is b^2 which goes to 1 in $D_8/\langle a \rangle$.

Proof of the proposition.

We are given $G \to \overline{G} = D_8 = \langle a, b \mid a^4 = 1 = b^2, a^b = a^{-1} \rangle$ such that there is no element of order 2 in G which is mapped to $b \bmod \langle a \rangle$. Let T be the representation of G corresponding to the faithful representation $\overline{T}$ of $\overline{G}$. Observe that for $x, y \in G$, $\overline{\widehat{x}} = r\widehat{\overline{x}}$ with $r = \operatorname{ord}(x)/\operatorname{ord}(\overline{x})$ and thus

$$T(u_{x,y}) = \overline{T}(\overline{u}_{x,y}) = \overline{T}(1 + r(\overline{x} - 1)\overline{y}\widehat{\overline{x}}) = \overline{T}(u_{\overline{x},\overline{y}})^r.$$

If $\overline{x}$ does not have order 2 then $u_{\overline{x},\overline{y}} = 1$ and if $\overline{x}$ has order 2 then $T(u_{x,y}) = \overline{T}(u_{\overline{x},\overline{y}})^r$ with $2 \mid r$. We have seen that $T(B_2) \le \overline{T}(B_2(\overline{G}))^2$. By the last term is meant the group generated by all 2nd powers. We now compute $\overline{T}(B_2(D_8))$:

$$\overline{T}(a) = \begin{pmatrix} 0 & 1 \\ -1 & 0 \end{pmatrix}, \qquad \overline{T}(b) = \begin{pmatrix} 1 & 0 \\ 0 & -1 \end{pmatrix}.$$

The relation

$$(a^j b - 1)a^i b(a^j b + 1) = (a^j b - 1)a^{i-j}a^j b(1 + a^j b) = (a^j b - 1)a^{i-j}(1 + a^j b)$$

implies that we only have to consider $\overline{T}(u_{\alpha,\alpha^i})$, $\alpha \in D_8$, $i = 1, 3$, so, in fact, only $i = 1$ since $\overline{T}(a^2) = -1$. We get

$$\overline{T}(B_2(D_8)) = \left\langle \begin{pmatrix} 1 & 0 \\ 4 & 1 \end{pmatrix}, \begin{pmatrix} 1 & 4 \\ 0 & 1 \end{pmatrix}, \begin{pmatrix} 3 & -2 \\ 2 & -1 \end{pmatrix}, \begin{pmatrix} -1 & -2 \\ 2 & 3 \end{pmatrix} \right\rangle,$$

where we have computed in due sequence $u_{b,a}$, $u_{a^2 b,a}^{-1}$, $u_{ab,a}$, $u_{a^3 b,a}$. The other possibilities lead to the same elements or their inverses. Referring to our original representations we see that

$$T(B_2) \le P = \left\langle \begin{pmatrix} 1 & 0 \\ 8 & 1 \end{pmatrix}, \begin{pmatrix} 1 & 8 \\ 0 & 1 \end{pmatrix}, \begin{pmatrix} 3 & -2 \\ 2 & -1 \end{pmatrix}^2 \right.$$

$$\left. = \begin{pmatrix} 5 & -4 \\ 4 & -3 \end{pmatrix}, \begin{pmatrix} -1 & -2 \\ 2 & 3 \end{pmatrix}^2 = \begin{pmatrix} -3 & -4 \\ 4 & 5 \end{pmatrix} \right\rangle.$$

This, $\bmod \pm 1$, is a subgroup of $\Gamma(2)$ which is the image of the congruence subgroup $SL_2(2\mathbb{Z})$ in $PSL_2(\mathbb{Z})$. $\Gamma(2)$ is a free group on 2 generators [10, p. 149]. Now, if $T(B_2)$ was of finite index in $SL_2(\mathbb{Z})$, then $P \bmod \pm 1$ would be of finite index j, say, in $\Gamma(2)$ and thus, due to Schreier [7, p. 141], it would be free on $1 + j$ generators. That implies $j \le 3$. Since $\Gamma(2) \supset \overline{T}(B_2(D_8)) \bmod \pm 1 \supset P \bmod \pm 1$, where the strict containments are due to the fact that the groups already differ modulo $\Gamma(4)$, we arrive at a contradiction. Thus $T(B_2)$ is not of finite index.

We are left with convincing ourselves that the Bass cyclic units do not contribute at all. Namely, as is readily seen, each Bass cyclic unit in $\mathbb{Z}G$ is mapped onto 1 in $\mathbb{Z}D_8$. □

We close this section with the following remark. We do not know whether our theorem actually fails for every group having a homomorphic image in E_2 or E_3. We do not even know this for the two groups in E_2. However, it seems

very likely that analogously to the counterexamples in the corollary above we always find a group G mapping onto a given group in E_2 and such that G does not satisfy our theorem. Regarding the set E_3, an appropriate test for an absolutely irreducible faithful character χ of dimension ≥ 4 to have Schur index 2 over the rationals consists in computing $\sum_{x \in G} \chi(x^2)$. By Frobenius-Schur [5] this sum equals $-|G|$ precisely when the Schur index is 2 over the reals, which, because we have real centre fields, amounts to the same as over $\mathbb{Q}$.

7. NILPOTENT GROUPS

The groups in this section are nilpotent groups the irreducible representations of which all have Schur index 1 and which do not have a homomorphic image in one of the two sets E_1, E_2 defined in the previous section. We call such groups *E-nilpotent*. Thus a nilpotent group G is *E*-nilpotent, if its rational group algebra has no simple components $K_{2 \times 2}$ with $K = \mathbb{Q}$, $\mathbb{Q}(i)$ or $(\mathbb{H}_k)_{2^r \times 2^r}$ with $k \geq 3$, $r \geq 0$.

Theorem A. *If G is E-nilpotent, then $[U(\mathbb{Z}G) : B]$ is finite.*

Proof. We need only establish (3.5) and (3.6). To that effect let T be a non-abelian absolutely irreducible representation of G. Write T as a tensor product of absolutely irreducible representations S_i of the Sylow subgroup P_i of G [7, p. 516]. Because G is E-nilpotent, all S_i are realizable over their character fields, and thus the same applies to T itself. As T is nonabelian, there is a Sylow subgroup P_1 such that $T_1 = S_1$ is nonabelian. Let Q be the product of all Sylow subgroups $P_i \neq P_1$ and T_2 the tensor product of the corresponding S_i; then $G = P_1 \times Q$ and $T = T_1 \otimes T_2$. Define $\mathcal{O}_i$ to be the ring of integers in the character fields of T_1 and T_2, respectively, and recall that as P_1 and Q have coprime orders, their character fields, being cyclotomic fields, are linearly disjoint over $\mathbb{Q}$ and so $\mathcal{O} = \mathcal{O}_1 \otimes \mathcal{O}_2$ is the ring of integers in the character field of T [8, p. 75].

Due to Proposition 5.1, or rather to its proof, there is a natural number N_1 such that, for any given pair $1 \leq \nu \neq \mu \leq \dim T_1$ and any element $h_1 \in \mathcal{O}_1$, we have elements $a, b_1, \ldots, b_s \in P_1$ together with certain integers $\alpha_1, \ldots, \alpha_s$ satisfying

$$\prod_{i=1}^{s} T_1(1 + (a-1)b_i\hat{a})^{\alpha_i} = 1 + N_1 h_1 e_{\nu\mu}.$$

This holds also true, if P_1 happens to be a 2-group, since then we are working under the assumption that P_1 does not map onto a group in E_1, E_2, E_3. $T_2(\mathbb{Z}Q)$ is an order in the component of $\mathbb{Q}Q$ belonging to T_2 and so there is some natural number N_2 such that for given $h_2 \in \mathcal{O}_2$ and $1 \leq i, j \leq \dim T_2$ we can solve the equation

$$T_2\left(\sum_{y \in Q} \beta_y y\right) = N_2 h_2 e_{ij} \quad \text{with } \beta_y \in \mathbb{Z}.$$

Putting things together we arrive at

$$\prod_{1\le i\le s,\, y\in Q} T(1 + (a-1)b_i y\hat{a})^{\alpha_i \beta_y} = T\Big(1 + (a-1)\Big(\sum_{i=1}^{s} \alpha_i b_i\Big)\Big(\sum_{y\in Q} \beta_y y\Big)\hat{a}\Big)$$

$$= 1 + T_1\Big((a-1)\sum_{i=1}^{s}\alpha_i b_i\hat{a}\Big) \otimes T_2\Big(\sum_{y\in Q}\beta_y y\Big)$$

$$= 1 + N_1 h_1 e_{\nu\mu} \otimes N_2 h_2 e_{ij},$$

which is an elementary matrix. Remembering that i may be equal to j, if T_2 is noncommutative we reverse the role of T_1 and T_2 and produce the remaining elementary matrices also.

We next turn to (3.6). We are now given two nonabelian absolutely irreducible representations T and T' that are not rationally equivalent. As the Galois group of the character field of T is the direct product of the Galois groups of the character fields of the S_i, where again P_i runs through the set of all Sylow subgroups of G, there is a Sylow subgroup P_1 such that T_1 is not rationally equivalent to T_1'; as before we have set $G = P_1 \times Q$, $T = T_1 \otimes T_2$, $T' = T_1' \otimes T_2'$. We search for an element $u \in B$ so that $T(u)$ is noncentral but $T'(u) = 1$.

It may happen that T_1 turns out to be abelian. If so, we solve the equations

$$T_1\Big(\sum_{x\in P_1}\alpha_x x\Big) = N \quad \text{for some } N \in \mathbb{N}, \qquad T_1'\Big(\sum_{x\in P_1}\alpha_x x\Big) = 0$$

in $\mathbb{Z}P_1$. T_2, for sure, is nonabelian and therefore there is a $u_2 \in B(Q)$ with $T_2(u_2)$ being noncentral. We write

$$u_2 = \prod_{i=1}^{t}(1 + (a-1)b_i\hat{a})^{\gamma_i} \quad \text{(with } a,\, b_i \in Q,\, \gamma_i \in \mathbb{Z})$$

and define

$$u = \prod_{i=1}^{t}\prod_{x\in P_1}(1 + (a-1)b_i x\hat{a})^{\gamma_i \alpha_x}.$$

Then

$$T(u) = T\Big(1 + (a-1)\Big(\sum_{i=1}^{t}\gamma_i b_i\Big)\Big(\sum_{x\in P_1}\alpha_x x\Big)\hat{a}\Big)$$

$$= 1 + T_1\Big(\sum_{x\in P_1}\alpha_x x\Big) \otimes (T_2(u_2) - 1) = 1 + N \otimes (T_2(u_2) - 1),$$

which is noncentral, but $T'(u) = 1 + 0 \otimes (T_2'(u_2) - 1) = 1$.

Therefore we may assume that T_1 is nonabelian. From Proposition 5.2 we then get an element $u_1 \in B_2(P_1)$ with $T_1(u_1)$ being noncentral but $T_1'(u_1) = 1$.

Observe that the statement is trivially true when T_1' is abelian, since $u_1 \in B_2(P_1)$. We now simply set $u = u_1$ and obtain

$$T(u) = T_1(u_1) \otimes 1, \qquad T'(u) = T_1'(u_1) \otimes 1 = 1.$$

Added in proof. An analogue of Theorem A for $\mathbb{Z}S_n$ and $\mathbb{Z}[y]G$, G monomial has now been proved. It will appear in J. Algebra.

References

1. A. Bak, *Subgroups of the general linear group normalized by relative elementary groups*, Algebraic K-Theory, Lecture Notes in Math., vol. 967, Springer, 1980, pp. 1–22.

2. H. Bass, *the Dirichlet unit theorem, induced characters, and Whitehead groups of finite groups*, Topology **4** (1966), 391–410.

3. H. Bass, J. Milnor and J. P. Serre, *Solution of the congruence subgroup problem for SL_n ($n \geq 3$) and Sp_{2n} ($n \geq 2$)*, Publ. Math. Inst. Hautes Etudes Sci. **33** (1967), 59–137.

4. C. W. Curtis and I. Reiner, *Representation theory of finite groups and associative algebras*, Wiley, New York and London, 1962.

5. G. Frobenius and I. Schur, *Über die reellen Darstellungen der endlichen Gruppen*, Sitz. Ber. Preuss. Akad. Wiss. (1906), 209–217.

6. M. Hall, *The theory of groups*, Macmillan, New York, 1959.

7. B. Huppert, *Endliche Gruppen* 1, Springer-Verlag, Berlin and New York, 1967.

8. S. Lang, *Algebraic number theory*, Addison-Wesley, Reading, Mass., 1970.

9. B. Liehl, *On the group SL_2 over orders of arithmetic type*, Crelle J. **323** (1981), 153–171.

10. M. Newman, *Integral matrices*, Academic Press, New York and London, 1972.

11. J. Ritter and S. K. Sehgal, *Certain normal subgroups of units in group rings*, Crelle J. **381** (1987), 214–220.

12. ____, *Generators of subgroups of $U(\mathbb{Z}G)$*; preprint (submitted to Contemp. Math.).

13. K. Roggenkamp and L. Scott, *Isomorphisms of p-adic group rings*, Ann. of Math. **126** (1987), 593–647.

14. P. Roquette, *Realisierung von Darstellungen endlicher nilpotenter Gruppen*, Arch. Math. **9** (1958), 241–250.

15. J. P. Serre, *Le problème des groupes de congruence pour SL_2*, Ann. of Math. **92** (1970), 489–527.

16. L. N. Vaserstein, *On the group SL_2 over Dedekind rings of arithmetic type*, Math. USSR-Sb. **18** (1973), 321–332.

17. ____, *The structure of classic arithmetic groups of rank greater than one*, Math. USSR-Sb. **20** (1973), 465–492.

18. A. Weiss, *Rigidity of p-adic p-torsion*, Ann. of Math. **127** (1988), 317–332.

Institut für Mathematik der Universität Augsburg, D-8900 Augsburg, West Germany

Department of Mathematics, University of Alberta, Edmonton, Alberta T6G 2G1, Canada