BOL. SOC. BRAS. MAT., VOL. 16 Nº 2 (1985), 1-9

INTEGRAL GROUP RINGS WHOSE GROUP OF UNITS IS SOLVABLE AN ELEMENTARY PROOF

Jairo Z. Gonçalves (*)

1. Introduction. Let $\mathbb{Z}G$ be the group ring of a finite group G over the ring of rational integers $\mathbb{Z}$, and let $U(\mathbb{Z}G)$ be its unit group. The characterization of the groups G such that $U(\mathbb{Z}G)$ is solvable was obtained by Hartley and Pickel [1], and independently by Sehgal [2], using arguments involving free groups and orders with solvable unit groups. We felt that an elementary proof could be approached, and this is the objective of the present note. Finally, we want to mention that we followed closely the arguments of Hartley and Pickel [1], Theorem 2. We are indebted to the referee for many useful comments and for his short proof of Proposition 2.3

2. Some lemmas

We denote by $\mathbb{Q}$ the field of rational numbers, and by $GL(n,D)$ the $n\times n$ general linear group over the division ring D. If H is a subgroup of G we represent by $[G:H]$ the index of H in G.

The Lemma below is taken from Hartley and Pickel [1].

(*) This work was done while the author was visiting the University of Alberta, and was supported by Conselho Nacional de Desenvolvimento Científico e Tecnológico - CNPq.

Recebido em 20/06/85.

Lemma 2.1 - *Let G be a finite group and let e be a central idempotent of $\mathbb{Q}G$. Then $[U(\mathbb{Z}Ge): U(\mathbb{Z}G)e] < \infty$.*

Proof - Let m be a positive integer such that $me \in \mathbb{Z}G$. Then, since $\mathbb{Z}Ge/m\mathbb{Z}Ge \cong (\mathbb{Z}/m\mathbb{Z})Ge$, the quotient ring $\mathbb{Z}Ge/m\mathbb{Z}Ge$ is finite. Now, if we restrict the canonical epimorphism

$$\mathbb{Z}Ge \twoheadrightarrow \mathbb{Z}Ge/m\mathbb{Z}Ge$$

to the group of units of $\mathbb{Z}Ge$, we obtain the multiplicative epimorphism

$$\omega: U(\mathbb{Z}Ge) \twoheadrightarrow L,$$

where $L = \omega U(\mathbb{Z}Ge)$ is a subgroup of the finite group $U(\mathbb{Z}Ge/m\mathbb{Z}Ge)$. Therefore

$$H = \ker \omega = \{x \in U(\mathbb{Z}Ge) \mid x \equiv e \mod m\mathbb{Z}Ge\}$$

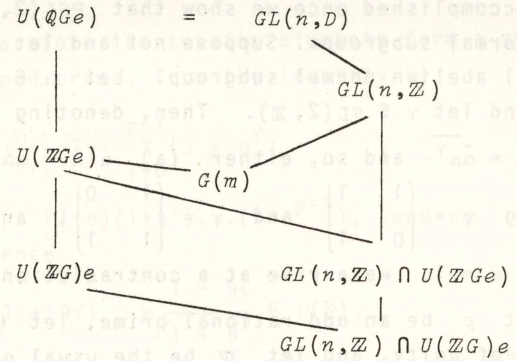
is a normal subgroup of finite index of $U(\mathbb{Z}Ge)$. We claim that $U(\mathbb{Z}G)e$ contains H. Indeed, let $x \in H$ and let us consider the element $\alpha = 1-e+ex \in \mathbb{Q}G$. We have by definition that $x = e + mye$, for some $y \in \mathbb{Z}G$, and hence

$$\alpha = 1-e+ex = 1-e+e(e+mye) = 1+mye \in \mathbb{Z}G.$$

By the same reason $\beta = 1-e+ex^{-1} \in \mathbb{Z}G$, and observing that $\beta = \alpha^{-1}$ and $\alpha e = ex = x$, the conclusion follows. □

Lemma 2.2 - *Let G be a finite group and let e be a central idempotent of $\mathbb{Q}G$ such that $U(\mathbb{Q}Ge) = GL(n,D)$, $n > 1$. Then $[GL(n,\mathbb{Z}): GL(n,\mathbb{Z}) \cap U(\mathbb{Z}G)e] < \infty$.*

Proof: We have the following Hasse diagram



Let e_{ij}, $1 \leq i,j \leq n$, be the element of $\mathbb{Q}Ge$ corresponding to the matrix of $M(n,D)$ that has 1 at the position i,j and 0 elsewhere, and let m be a positive integer such that $me_{ij} \in \mathbb{Z}Ge$ for every i and j. Thus $\mathbb{Z}Ge$ contains every $n\times n$ matrix over $\mathbb{Z}$ which is congruent to 1 modulo m, and hence $U(\mathbb{Z}Ge)$ contains $G(m)$, the principal congruence subgroup of $GL(n,\mathbb{Z})$. By Lemma 2.1 $[U(\mathbb{Z}Ge): U(\mathbb{Z}G)e] < \infty$ and so $[GL(n,\mathbb{Z}) \cap U(\mathbb{Z}Ge): GL(n,\mathbb{Z}) \cap U(\mathbb{Z}G)e] < \infty$, and the conclusion follows. □

Proposition 2.3 - *Let G be a group with center Z, and suppose that G/Z is an infinite group which contains no nontrivial abelian normal subgroups. Then G is not solvable-by-finite.*

Proof - If G/Z has a normal solvable subgroup H/Z of finite index, then the last nontrivial term of the derived series of H/Z is a normal abelian subgroup of G/Z. □

Lemma 2.4 - *$GL(n,\mathbb{Z})$, $n > 1$, is not solvable-by-finite.*

Proof - The property of being solvable-by-finite is inherited by subgroups and by homomorphic images. So, it is enough to show that $PSL(2,\mathbb{Z}) = SL(2,\mathbb{Z})/\{\pm I\}$, where $SL(2,\mathbb{Z}) = \{\alpha \in GL(2,\mathbb{Z}) \mid \det\alpha = 1\}$ and $I = \begin{pmatrix} 1 & 0 \\ 0 & 1 \end{pmatrix}$, is not solvable-by-finite. By Proposition 2.3

this is accomplished once we show that $PSL(2,\mathbb{Z})$ has no nontrivial abelian normal subgroups. Suppose not and let $\bar{N} \triangleleft PSL(2,\mathbb{Z})$ be a nontrivial abelian normal subgroup. Let $\alpha \in N$ be such that $\bar{\alpha} \neq 1$, and let $\gamma \in SL(2,\mathbb{Z})$. Then, denoting $\gamma^{-1}\alpha\gamma$ by α^γ, we have $\overline{\alpha^\gamma\alpha} = \overline{\alpha\alpha^\gamma}$ and so, either (a) $\alpha^\gamma\alpha = \alpha\alpha^\gamma$ or (b) $\alpha^\gamma\alpha = -\alpha\alpha^\gamma$. Now taking $\gamma = \begin{pmatrix} 1 & 1 \\ 0 & 1 \end{pmatrix}$ and $\gamma = \begin{pmatrix} 1 & 0 \\ 1 & 1 \end{pmatrix}$, and taking into account that $\det \alpha = 1$, we arrive at a contradiction.

Let p be an odd rational prime, let θ be a primitive p-th root of unity, and let $\mathbb{H}$ be the usual quaternion algebra over the rationals, i.e.,

$$\mathbb{H} = \{x + yi + zj + wk \mid i^2 = j^2 = -1,\ ij = -ji = k,\ x,y,z,w \in \mathbb{Q}\}.$$

Let $\mathbb{H}_\theta = \mathbb{Q}(\theta) \otimes_{\mathbb{Q}} \mathbb{H}$, and inside this $\mathbb{Q}$-algebra let us consider the subring

$$R = \{x + yi + zj + wk \mid x,y,z,w \in \mathbb{Z}[\theta]\}.$$

A few observations are now in order now.

(i) If L is the subfield of $\mathbb{H}_\theta$ generated by θ and i, then $\mathbb{H}_\theta = L \oplus Lj$ as a left vector space over L, and the right regular representation of $\mathbb{H}_\theta$ gives us the embedding

$$\psi\colon \mathbb{H}_\theta \to M(2,L)$$

$$a \longrightarrow \psi_a = \begin{pmatrix} x+yi & z+wi \\ -z+wi & x-yi \end{pmatrix}$$

where $a = x + yi + zj + wk$. The determinant of $M(2,L)$ gives us a multiplicative function

$$N(a) = x^2 + y^2 + z^2 + w^2$$

(ii) The center of $U(R)$, which we will denote by $\zeta U(R)$, is $U(\mathbb{Z}[\theta])$ and $U(R)/\zeta U(R)$ is infinite. Only the last assertion deserves a proof. Suppose that this is note true. Then $U(R)$ is

an FC-group, and therefore its torsion elements form a subgroup. Now since p is an odd prime, from the identity

$$X^p + 1 = \prod_{i=0}^{p-1} (X + \theta^i),$$

we conclude that $1 = (1+\theta)(1+\theta^2)\ldots(1+\theta^{p-1})$, and so $1+\theta^2 \in U(\mathbb{Z}[\theta])$. Hence

$$(1+\theta i)^{-1} = \frac{1-\theta i}{1+\theta^2} \in U(R),$$

and we claim that the product of the torsion units $\left(\frac{1-\theta i}{1+\theta^2}\right)j(1+\theta i)$ and $-j$ has infinite order. Indeed,

$$\left(\frac{1-\theta i}{1+\theta^2}\right)j(1+\theta i)(-j) = \frac{(1-\theta i)^2}{1+\theta^2}$$

is a complex number, and if this number is a root of unity then its absolute value is 1. Therefore $|1-\theta i|^2 = |1+\theta^2|$. Let us calculate both sides of the equality above. Let $\theta = \cos\frac{2\pi}{p} + i\sin\frac{2\pi}{p}$ and $\bar\theta = \cos\frac{2\pi}{p} - i\sin\frac{2\pi}{p}$. Then

$$|1-\theta i|^2 = (1-\theta i)(1+\bar\theta i) = 2\left[1+\sin\frac{2\pi}{p}\right]$$

and, on the other hand

$$|1+\theta^2| = \left|1+\cos\frac{4\pi}{p} + i\sin\frac{4\pi}{p}\right| = \sqrt{\left(1+\cos\frac{4\pi}{p}\right)^2 + \sin^2\frac{4\pi}{p}}$$

$$= \sqrt{4\cos^2\frac{2\pi}{p}} = 2\left|\cos\frac{2\pi}{p}\right|.$$

Since $p \geqq 3$, the angle $\frac{2\pi}{p}$ belongs either to the first or to the second quadrant, and therefore $1+\sin\frac{2\pi}{p} > 1$ and $\left|\cos\frac{2\pi}{p}\right| < 1$, a contradiction.

We are in position to prove the Lemma that is the crux of the matter.

Lemma 2.5 - $U(R)$ *is not solvable-by-finite.*

Proof - In view of Proposition 2.3 and observation (ii) it is enough to show that $U(R)/\zeta U(R)$ contains no nontrivial abelian normal subgroups. Suppose not and let $\bar{A} \lhd U(R)/\zeta U(R)$ be an abelian subgroup. Let $\alpha \in A$ be such that $\bar{\alpha} \neq \bar{1}$, and let $\gamma \in U(R)$. Then

$$\overline{\alpha^{\gamma}}\,\bar{\alpha} = \bar{\alpha}\,\overline{\alpha^{\gamma}}, \quad \text{i.e.,} \quad \alpha\alpha^{\gamma} = \alpha^{\gamma}\alpha\delta, \quad \text{where } \delta \in U(\mathbb{Z}[\theta]).$$

Applying the function N defined in (i) to both sides of the last equality, we conclude that $N(\delta) = \delta^2 = 1$, and so $\delta = \pm 1$. Therefore we have shown that if $\gamma \in U(R)$, either (a) $\alpha\alpha^{\gamma} = \alpha^{\gamma}\alpha$ or (b) $\alpha\alpha^{\gamma} = -\alpha^{\gamma}\alpha$ hold. Let $\alpha = x+yi+zj+wk$ and $\gamma = i$. If (a) holds then, from $\alpha\alpha^{i} = \alpha^{i}\alpha$ we obtain

$$(x + yi)(zj+wk) = (zj+wk)(x+yi) \quad \text{or}$$

$$\begin{cases} jw = 0 \\ jz = 0 \end{cases}$$

If $y \neq 0$ then $w = z = 0$ and α has two nonzero elements in its support, at most. So, let us assume that $y = 0$. Conjugating α by j we obtain either:

(a1) $\alpha\alpha^{j} = \alpha^{j}\alpha$ or (b1) $\alpha\alpha^{j} = -\alpha^{j}\alpha$.

Let us assume (a1). Then we obtain $(x+zj)wk = wk(x+zj)$ or $wz=0$, and so either $z = 0$ or $w = 0$. On the other hand, if we assume (b1) we have

$$(x+zj)^2 = (wk)^2 \quad \text{or,} \quad zx = 0 \quad \text{and} \quad x^2+w^2 = z^2$$

and from the first equation we obtain that either $x = 0$ or $z = 0$. Hence, we have that α has one of the following forms:

(A) $\alpha = x + wk$, (B) $\alpha = x + zj$, (C) $\alpha = zj + wk$.

Let us assume (A) and let $\gamma = 1+\theta i$. Then $\gamma^{-1} = \dfrac{1-\theta i}{1+\theta^2}$ and so, either

(a2) $\alpha\alpha^{\gamma} = \alpha^{\gamma}\alpha$ or (b2) $\alpha\alpha^{\gamma} = -\alpha^{\gamma}\alpha$.

Let us assume (a2). Then we have

$$(1+\theta^2)\alpha^{\gamma}\alpha = [(1+\theta^2)x^2 - w^2(1-\theta^2)] + 2\theta w^2 i + 2\theta wxj + 2wxk, \quad \text{and}$$

$$(1+\theta^2)\alpha\alpha^{\gamma} = [(1+\theta^2)x^2 - w^2(1-\theta^2)] - 2\theta w^2 i + 2\theta xwj + 2wxk.$$

Hence, from the equality of the coefficients of i in both expressions above, we conclude that $4\theta w^2 = 0$, and so $w = 0$. Therefore $\alpha = x \in \zeta U(R)$, a contradicton.

Let us assume (b2). Then, from the equality of the coefficients of 1 and k we obtain

$$4wx = 0 \quad \text{and} \quad (1+\theta^2)x^2 = w^2(1-\theta^2).$$

Thus, $w = x = 0$, and α is not a unit; a contradiction is reached.

We can get rid of (B) in a way similar to the case (A). So, let us assume (C) and let $\gamma = 1+\theta i$. Let us assume (a2). Then we have

$$(1+\theta^2)\alpha^{\gamma}\alpha = (\theta^2-1)(z^2+w^2) + 2\theta(z^2+w^2)i \quad \text{and}$$

$$(1+\theta^2)\alpha\alpha^{\gamma} = (\theta^2-1)(z^2+w^2) - 2\theta(z^2+w^2)i.$$

So, from the equality of the coefficients of i, we obtain that $w^2 + z^2 = 0$. If $w \neq 0$, then $(\frac{z}{w})^2 = -1$, and $\sqrt{-1} \in \mathbb{Q}(\theta)$ and hence $\sqrt{-1} \in \mathbb{Z}[\theta]$; a contradiction is reached. Therefore $w=z=0$; a contradiction again.

Let us assume (b2). Then, from the equality of the coefficients of 1, we obtain $(\theta^2-1)(z^2+w^2) = 0$, and $z=w=0$, a contradiction. Finally, we observe that the case $\alpha = x+yi$, which was not considered, can be handled by conjugation by $\gamma=1+\theta j$.

We leave to the reader the verification that the same arguments work if we assume (b) at the beginning of the proof. □

3. The Hartley-Pickel, Sehgal Theorem

Theorem 3.1. - *Let* G *be a finite group. Then* $U(\mathbb{Z}G)$ *is solvable if and only if* G *is an abelian or a Hamiltonian 2-group.*

Proof - Only necessity requires a proof. Let $\mathbb{Q}G = \bigoplus_{i=1}^{r} M(n_i, D_i)$ be the decomposition of the semisimple algebra $\mathbb{Q}G$ as a direct sum of full matrix rings over division rings. Suppose that for some ℓ, $1 \leqq \ell \leqq r$, we have $n_\ell < 1$ and let e be the corresponding central idempotent in the decomposition above. Since $U(\mathbb{Z}G)$ is solvable it follows that $U(\mathbb{Z}G)e$ is solvable, and by Lemma 2.2 $GL(n_\ell, \mathbb{Z})$ is solvable-by-finite, in contradiction with Lemma 2.4 Hence, for every i, $1 \leqq i \leqq r$, $n_i = 1$ and therefore every idempotent is central. It follows that G is an abelian or a Hamiltonian group. Let us assume that $G = \langle x\rangle \times K_8$, the direct product of a cyclic group of odd prime order p by K_8, the quaternion group of order 8. Let θ be a primitive p-th root of unity. Then

$$\mathbb{Q}(\langle x\rangle \times K_8) = (\mathbb{Q}\langle x\rangle)K_8 = (\mathbb{Q} \oplus \mathbb{Q}(\theta))K_8 = \mathbb{Q}K_8 \oplus \mathbb{Q}(\theta)K_8 =$$

$$= \mathbb{Q}K_8 \oplus \left(\bigoplus_{i=1}^{4} \mathbb{Q}(\theta) \oplus \mathbb{Q}(\theta) \otimes_{\mathbb{Q}} \mathbb{H}\right).$$

Let e be the central idempotent of $\mathbb{Q}G$ corresponding to $\mathbb{H}_\theta = \mathbb{Q}(\theta) \otimes_{\mathbb{Q}} \mathbb{H}$. Then

$$\mathbb{Z}Ge = \{x + yi + zj + wk \in \mathbb{H}_\theta \mid x, y, z, w \in \mathbb{Z}[\theta]\} = R.$$

Again, since $U(\mathbb{Z}G)$ is solvable, $U(\mathbb{Z}G)e$ is solvable and by Lemma 2.1 $U(R)$ is solvable-by-finite, in contradicton with Lemma 2.5. □

4. Final Remark. Despite the elementary character of our proof, we are able to recover [1], Theorem 2. Indeed, if G is neither an abelian nor a Hamiltonian 2-group, then $U(\mathbb{Z}G)$ has a homomorphic image that is not solvable-by-finite. By Tits Theorem [3], Theorem 1, $U(\mathbb{Z}G)$ contains a free noncyclic group.

References

[1] Hartley, B. and Pickel, P.F. *Free subgroups in the unit groups of integral group rings*. Can. J. of Math. 32, 6 (1980), 1342-1352.

[2] Sehgal, S.K. *Topics in groups rings*. Marcel Dekker, New York, 1978.

[3] Tits, J. *Free subgroups in linear groups* J. of Algebra 20 (1972), 250-270.

Instituto de Matemática e Estatística
Universidade de São Paulo
Caixa Postal 20570 - Agência Iguatemi
01.000 - São Paulo-SP