RT-MAT 96-04

Automorphisms of Group Algebra of Some Metacyclic Groups

Sônia P. Coelho, Eric Jespers
C. Polcino Milies

Março/96

Automorphisms of Group Algebras of Some Metacyclic Groups

Sônia P. Coelho

Eric Jespers

C. Polcino Milies[1]

Abstract

We study the group of automorphisms of the group algebra $\mathbf{Q}G$, where G is a metacyclic group of order $2n$ with presentation $G = \langle a, b \mid a^n = 1,\ b^2 = 1,\ ba = a^i b \rangle$.

1 Rational Group Algebras

Throughout the paper G is a metacyclic group with presentation

$$G = \langle a, b \mid a^n = 1,\ b^2 = 1,\ ba = a^i b \rangle,,$$

whith $1 \leq i \leq n-1$. In this paper we study the automorphism group of the rational group algebra $\mathbf{Q}G$. Our work persues a study begun in [2].

The unit group of the integral group ring $\mathbf{Z}G$ has been studied in [5] where a description of the rational group algebra of this group is given. In order ot state this description we need to introduce some notation and make a few observations.

Note that it follows that $i^2 \equiv 1 \ (mod\ n)$. Furthermore, if we set $d = gcd(n,\ i-1)$, then $Z(G) =< a^{\frac{n}{d}} >$, $G' =< a^{i-1} >$, and the non-central conjugacy classes of G are either of the form $a^j bG'$, $0 \leq j \leq d-1$, or of the form $\{a^r,\ a^{ri}\}$ with $a^r \notin Z(G)$. So the number of conjugacy classes of G is $[Z(\mathbf{Q}G) : \mathbf{Q}] = 2d + \frac{n-d}{2}$.

[1]The first and third authors are partially supported by research grants from CNPq., (Proc. 300371/82-9(RN) and Proc. 300243/79-0(RN) respectively) and Fapesp Proc. 95/1319-0; the second is supported in part by NSERC-grant OGP0036631.

Because of [5], $\mathbf{Q}G$ is of the form:

$$\mathbf{Q}G \cong \mathbf{Q}(G/G') \oplus \Delta(G:G') \cong \mathbf{Q}(G/G') \oplus (\oplus_{\substack{m|n \\ m \nmid d}} M_2(\mathbf{Q}_m))$$

where $\mathbf{Q}_m = \mathbf{Q}(\xi_m + \xi_m^i, \xi_m^2 + \xi_m^{2i}, \cdots)$ and ξ_m denotes a primitive root of unity of order m. Notice that, though not reflected on the notation employed, the field $\mathbf{Q}_m$ also depends on the integer i verifying $i^2 \equiv 1\ (mod\ n)$. We give a more precise description of this field below.

Lemma 1.1 *Let m and i be positive integers, such that $i^2 \equiv 1\ (mod\ m)$ but $i \not\equiv 1\ (mod\ m)$ and let ξ be a primitive root of unity of order m; set $\mathbf{Q}_m = \mathbf{Q}(\xi + \xi^i, \xi^2 + \xi^{2i}, \cdots)$, as above. Then $\mathbf{Q}_m = \mathbf{Q}(\xi + \xi^i)$ except if $\xi^i = -\xi$, in which case $\mathbf{Q}_m = \mathbf{Q}(\xi^2)$. In both cases we have that $[\mathbf{Q}(\xi) : \mathbf{Q}_m] = 2$.*

Proof. Assume first that $\xi^i \neq -\xi$. We claim that $[\mathbf{Q}(\xi) : \mathbf{Q}(\xi + \xi^i)] = 2$. To prove this assertion, it will suffice to show that the Galois group of this extension has order 2, i.e. that there exists only one non-trivial automorphism of $\mathbf{Q}(\xi)$ that fixes $\mathbf{Q}(\xi + \xi^i)$. Note that since $i \not\equiv 1(mod\ n)$, it follows that $-\xi \neq \xi^i$ and thus the Galois group has order at least 2.

Let ψ be a non-trivial automorphism. Then, $\psi(\xi) = \xi^r$, for some positive integer r such that $gcd(m, r) = 1$. Then:

$$\xi + \xi^i = \psi(\xi + \xi^i) = \xi^r + \xi^{ri}.$$

We may assume that $arg(\xi) = \frac{2\pi}{m}$ and $arg(\xi^i) = i\frac{2\pi}{m}$. Since $|\xi| = |\xi^i| = 1$ it is easy to see, from elementary geometric considerations, that:

$$|\xi + \xi^i| = 2\left|cos\left(\frac{i-1}{2}\right).\frac{2\pi}{m}\right|,$$

$$arg(\xi + \xi^i) = \frac{i+1}{2}.\frac{2\pi}{m}.$$

In a similar way we obtain:

$$|\xi^r + \xi^{ri}| = 2\left|cos\left(\frac{r(i-1)}{2}\right).\frac{2\pi}{m}\right|,$$

$$arg(\xi^r + \xi^{ri}) = \frac{r(i+1)}{2}.\frac{2\pi}{m}.$$

Hence:

$$m \mid (r \pm 1)(i-1),$$
$$m \mid (r-1)(i+1).$$

So, we are left with two possible cases:

$$(i)\begin{cases} m \mid (r-1)(i+1) \\ m \mid (r-1)(i-1) \end{cases} \qquad (ii)\begin{cases} m \mid (r-1)(i+1) \\ m \mid (r+1)(i-1) \end{cases}$$

We discuss case (ii) first. Subtracting, we obtain that $m \mid 2(r-i)$, which implies that either $\xi^r = \xi^i$ or $\xi^r = -\xi^{-i}$. The second possibility leads to a contradiction since if we have that $\xi^{r-i} = -1$ then $2|m$ and it follows that $2 \mid (i-1)(i+1)$ so i is odd. Hence $\xi + \xi^i = \psi(\xi + \xi^i) = -\xi^i + (-1)^i\xi^{i^2} = -(\xi^i + \xi)$ and thus $2(\xi + \xi^i) = 0$ implying that $\xi = -\xi^i$, against the initial assumption. So we obtain that $\psi(\xi) = \xi^i$. Since ψ is also a $\mathbf{Q}_m$-automorphism of $\mathbf{Q}(\xi)$ and $\mathbf{Q}(\xi + \xi^i) \subset \mathbf{Q}_m \subset \mathbf{Q}(\xi)$ but $\mathbf{Q}_m \neq \mathbf{Q}(\xi)$, it follows that $\mathbf{Q}(\xi + \xi^i) = \mathbf{Q}_m$ and $[\mathbf{Q}(\xi) : \mathbf{Q}_m] = 2$.

Case (i) readily gives, also by subtraction, that $m \mid 2(r-1)$ and again either $\xi^r = \xi$ or $\xi^r = -\xi$. If ξ^{r-1}, then $2 \mid m$ and, as above, we obtain a contradiction. Therefore, we must have that $\psi(\xi) = \xi$, which is a contradiction, since ψ is not trivial.

It follows easily that $\mathbf{Q}_m = \mathbf{Q}(\xi^2)$. Furthermore, $\mathbf{Q}(\xi) \neq \mathbf{Q}(\xi^2)$ for, otherwise, we would have $\xi = \xi^{2l}$ for some l, and thus $m \mid (2l-1)$. However, $\xi^i = -\xi$ implies that m is even, so $m \nmid (2l-1)$. Thus $[\mathbf{Q}(\xi) : \mathbf{Q}_m] = [\mathbf{Q}(\xi) : \mathbf{Q}(\xi^i)] = 2$.

□

We need some technical results. We begin with the following easy lemma.

Lemma 1.2 *Let ξ, θ be roots of unity such that $o(\theta)$ is even and $\mathbf{Q}(\xi) \subset \mathbf{Q}(\theta)$. Then $[\mathbf{Q}(\theta) : \mathbf{Q}(\xi)] = 2$ if and only if one of the following conditions holds:*

(i) $o(\xi)$ is even and either $o(\theta) = 2o(\xi)$ or $o(\theta) = 3o(\xi)$ and $3 \nmid o(\xi)$.

(ii) $o(\xi)$ is odd and either $o(\theta) = 4o(\xi)$ or $o(\theta) = 6o(\xi)$ and $3 \nmid o(\xi)$.

Proof. Since $\xi \in \mathbf{Q}(\theta)$ and $o(\theta)$ is even, we have that $\xi = \theta^j$, for some positive integer j, and hence $o(\xi) \mid o(\theta)$. We write $o(\xi)$ and $o(\theta)$ as products of different prime divisors:

$$o(\xi) = p_1^{a_1} \dots p_t^{a_t},$$
$$o(\theta) = p_1^{b_1} \dots p_t^{b_t} q_1^{c_1} \dots q_s^{c_s}$$

with $1 \leq a_i \leq b_i$, $1 \leq i \leq t$.

Since $[\mathbf{Q}(\theta) : (\mathbf{Q}(\xi)] = 2$ we readily see that $\phi(o(\theta)) = 2\phi(o(\xi))$, where ϕ denotes Euler's Totient function. Thus:

$$2 = p_1^{b_1 - a_1} \dots p_t^{b_t - a_t} q_1^{c_1 - 1} \dots q_s^{c_s - 1}(q_1 - 1) \dots (q_s - 1).$$

If $o(\xi)$ is even, we may assume that $p_1 = 2$ and we have two possibilities: either $b_1 = a_1 + 1$, with $b_i = a_i$, $2 \leq i \leq t$ and $s = 0$ or $b_i = a_i$, $1 \leq i \leq t$ and $s = 1$ with $q_1 = 3$ and $c_1 = 1$ so, we obtain (i). The converse is trivial.

If $o(\xi)$ is odd, since $o(\theta)$ is even, we may assume that $q_1 = 2$ and again we have two possibilities: either $q_1 = 2$ with $c_1 = 2$ or $q_1 = 2$, $q_2 = 3$ with $c_1 = c_2 = 1$. In both cases, we have that $a_i = b_i$, $1 \leq i \leq t$ and $s = 1$ or 2. Notice also that, in the last case, we have that $3 \nmid o(\xi)$. The converse is again trivial. □

Lemma 1.3 *Let $m < k$ be positive integers and let i be an integer such that $i^2 \equiv 1 \ (mod\ m)$ and $i^2 \equiv 1 \ (mod\ k)$ but $i \not\equiv 1 \ (mod\ m)$, $i \not\equiv 1 \ (mod\ k)$. If $\mathbf{Q}_m = \mathbf{Q}_k$ then, one of the following conditions holds:*

(i) $gcd(6, m) = 1$ and $k = 2m$.

(ii) $gcd(6, m) = 2$ and $k = \frac{3}{2}m$, where $4 \mid m$.

(iii) $gcd(6, m) = 3$ and either $k = 2m$ or $k = \frac{4}{3}m$.

Proof. Let θ be a primitive root of unity of order $lcm(m, k)$; then $\mathbf{Q}(\theta) = \mathbf{Q}(\xi_m, \xi_k)$. Since Lemma 1.1 shows that $[\mathbf{Q}(\xi_k) : \mathbf{Q}_k] = [\mathbf{Q}(\xi_m) : \mathbf{Q}_m] = 2$, it follows that $[\mathbf{Q}(\theta) : \mathbf{Q}(\xi_m)] = [\mathbf{Q}(\theta) : \mathbf{Q}(\xi_k)] \leq 2$.

If $[\mathbf{Q}(\theta) : \mathbf{Q}(\xi_m)] = 1$, then we have that $\mathbf{Q}(\xi_m) = \mathbf{Q}(\xi_k)$ and [7, III.2.14] shows that $k = 2m$ and m is odd.

So, assume that $[\mathbf{Q}(\theta) : \mathbf{Q}(\xi_m)] = 2$, set $d_0 = gcd(m, k)$ and write $m = m'd_0$, $k = k'd_0$. Then, $o(\theta) = lcm(m, k) = k'm = m'k$. If m and k are both even, then Lemma 1.2 shows that m', $k' \in \{2, 3\}$ and we obtain that $m = 2d_0$, $k = 3d_0$ so $k = \frac{3}{2}m$. Notice that this implies also that d_0 must be even, so $4 \mid m$.

If m is even and k odd, then Lemma 1.2 shows that $k' = 3$ and also that $m' = 4$ or 6, contradicting the fact that $m < k$. If m is odd and k is even it follows that $m = 3d_0$, $k = 4d_0$ so $k = \frac{4}{3}m$.

Finally, Lemma 1.2 shows that the case where m and k are both odd cannot occur.

We are now ready to complete our discussion.

If $gcd(6, m) = 1$ it is easily seen that $\mathbf{Q}_m = \mathbf{Q}_k$ can only happen if $\mathbf{Q}(\xi_m) = \mathbf{Q}(\xi_k)$ and hence $k = 2m$ and m is odd.

If $gcd(6, m) = 2$ then, clearly, $k = \frac{3}{2}m$ and $3 \nmid m$.

If $gcd(6, m) = 3$ either $\mathbf{Q}(\xi_m) = \mathbf{Q}(\xi_k)$ and then $k = 2m$ or $k = \frac{4}{3}m$. Notice that $gcd(6, m) = 6$ is impossible since this implies that m and k are both even and $m = 2d_0$, $k = 3d_0$, so $o(\theta) = 3m$ is even and Lemma 1.2 shows that $3 \nmid m$, a contradiciton. □

Lemma 1.4 *Let ξ, θ be roots of unity of orders $k = 3d_0$ and $l = 6d_0$ respectively, where d_0 is an even number, and let i be a positive integer such that $i^2 \equiv 1 \ (mod\ l)$ and $k \nmid gcd(l, i-1)$. Set $\mathbf{Q}_k = \mathbf{Q}(\xi + \xi^i, \ldots)$; then:*

(i) $[\mathbf{Q}(\theta) : \mathbf{Q}(\xi)] = 2$.

(ii) $Gal(\mathbf{Q}(\theta) : \mathbf{Q}_k) = \{h_0, h_1, h_2, h_3\}$, *where* $h_0(\theta) = \theta$, $h_1(\theta) = \theta^i$, $h_2(\theta) = \theta^{k+1}$, $h_3(\theta) = \theta^{k+i}$ *and the fixed field of* $\mathbf{Q}(\theta)$ *under this Galois group is* $\mathbf{Q}_k$.

Proof. Since $o(\theta) = 6d_0 = l$ we have that $\mathbf{Q}(\xi) = \mathbf{Q}(\theta^2)$, so $[\mathbf{Q}(\theta) : \mathbf{Q}(\xi)] \leq 2$. The order of the group of torsion units of $\mathbf{Q}(\xi)$ is $|TU(\mathbf{Q}(\xi))| = m$, so $\theta \notin \mathbf{Q}(\xi)$ and thus $[\mathbf{Q}(\theta) : \mathbf{Q}(\xi)] = 2$. Since $k \nmid (i-1)$, Lemma 1.1 shows that $[\mathbf{Q}(\theta), \mathbf{Q}_k)] = 4$.

Direct computations show that the mappings of the statement are well-defined $\mathbf{Q}_k$-automorphisms of $\mathbf{Q}(\theta)$ which are pairwise different. Since $|Gal(\mathbf{Q}(\theta), \mathbf{Q}_k)| \leq [\mathbf{Q}(\theta), \mathbf{Q}_k)] = 4$, the proof is complete. □

Theorem 1.5 *Let $m < k$ be positive integers, set $l = lcm(m, k)$ and let i be a positive integer such that $i^2 \equiv 1 \ (mod\ l)$ and such that both m and k do not divide $gcd(l, i-1)$. Set $\mathbf{Q}_m = \mathbf{Q}(\xi + \xi^i, \ldots)$; then $\mathbf{Q}_m = \mathbf{Q}_k$ if and only if one of the following conditions holds:*

(i) m is odd and either $k = 2m$ or $3 \mid m$, $3^2 \nmid m$, $\frac{2m}{3} \mid (i-1)$ and $k = \frac{4}{3}m$.

(ii) m *and* $\frac{m}{2}$ *are both even,* $3 \nmid m$, $\frac{m}{2} \mid (i-1)$ *and* $k = \frac{3}{2}m$.

Proof. Assume that $\mathbf{Q}_m = \mathbf{Q}_k$. We shall use the results of Lemma 1.3.

If $gcd(6, m) = 1$ then condition (i) holds. If $gcd(6, m) = 2$ then $k = \frac{3}{2}m$, where $4 \mid m$. Writing $m = 2d_0$ and $k = 3d_0$, we have that d_0 is even and $l = 6d_o$. Setting $\theta = \xi_l$ and $\xi = \xi_k$ we may apply Lemma 1.4. Since $o(\xi_m) = 2d_0 = o(\theta^3)$, we may assume that $\xi_m = \theta^3$.

Now, the elements of $Gal(\mathbf{Q}(\theta) : \mathbf{Q}_k)$ fix $\mathbf{Q}_m = \mathbf{Q}_k$. Then, the element $\xi_m + \xi_m^i = \theta^3 + \theta^{3i} \in \mathbf{Q}_m$ must be fixed by $h_3 \in Gal(\mathbf{Q}(\theta) : \mathbf{Q}_k)$, so we have:

$$\theta^3 + \theta^{3i} = h_3(\theta^3 + \theta^{3i}) = \theta^{3(k+i)} + \theta^{3i(k+i)}.$$

Since $\theta^{3k} = \theta^{9d_0}$ which has order 2, we conclude that $\theta^{3k} = -1$. Hence:

$$\theta^3 + \theta^{3i} = -\theta^{3i} - \theta^3.$$

Consequently $\theta^{3i} = -\theta^3$, which implies that $\frac{m}{2} = d_0$ divides $i - 1$. Thus, condition (ii) holds.

Now, we consider the case where $gcd(6, m) = 3$. Then, either $k = 2m$ or $k = \frac{4}{3}m$. If $k = 2m$ we obtain condition (i), so assume that $k = \frac{4}{3}m$. Writing $m = 3d_0$ and $k = 4d_0$, we have that d_0 is odd.

Notice that being d_0 odd, we have that $o(-\xi_m) = 6d_0$ and thus, since i is odd, we obtain that $\mathbf{Q}_{6d_0} = \mathbf{Q}_{3d_0}$; hence $\mathbf{Q}_{6d_0} = \mathbf{Q}_k = \mathbf{Q}_{4d_0}$. Also notice that since Lemma 1.3 shows that $gcd(6, m) \neq 6$ it follows that $gcd(6, 4d_0) = 2$ and thus $3 \nmid d_0$. Set $m_1 = 4d_0$ and $k_1 = 6d_0$; then $\mathbf{Q}_{m_1} = \mathbf{Q}_{k_1}$ and condition (ii) of the statement shows that $\frac{m_1}{2} = 2d_0 = \frac{2m}{3}$ divides $(i-1)$.

To prove the converse, we begin by assuming that condition (ii) holds. Write $m = 2d_0$, where d_0 is even and $3 \nmid d_0$, $k = 3d_0$, $l = 6d_0$ and $d_0 \mid (i-1)$. Set $\theta = \xi_l$ and $\theta^3 = \xi_m$. Then, Lemmas 1.1 and 1.2 show that:

$$[\mathbf{Q}(\theta) : \mathbf{Q}_m] = [\mathbf{Q}(\theta) : \mathbf{Q}(\xi_m)][\mathbf{Q}(\xi_m) : \mathbf{Q}_m] = 4.$$

Furthermore, since Lemma 1.4 shows that $|Gal((\mathbf{Q}(\theta) : \mathbf{Q}_k]| = 4$, in order to prove that $\mathbf{Q}_m = \mathbf{Q}_k$ it will suffice to show that $Gal(\mathbf{Q}(\theta) : \mathbf{Q}_k) \subset Gal(\mathbf{Q}(\theta) : \mathbf{Q}_m)$.

Since $\xi_m^i = \theta^{3i}$ and $o(\theta^{3d_0}) = 2$, writing $i = d_0 q + 1$, we obtain that $\xi_m^i = \theta^{3i} = (-1)^q \theta^3 = (-1)^q \xi_m$. If q is even then $m = 2d_0$ divides $i - 1$, a contradiction. Thus, q must be odd and then $\xi_m^i = -\xi_m$. Therefore, Lemma 1.1 shows that $\mathbf{Q}_m = \mathbf{Q}(\xi_m^2) = \mathbf{Q}(\theta^6)$.

Now, a simple calculation shows that θ^6 is fixed by the elements of $Gal(\mathbf{Q}(\theta) : \mathbf{Q}_k)$ described in Lemma 1.4. Hence $Gal(\mathbf{Q}(\theta), \mathbf{Q}_k) \subset Gal(\mathbf{Q}(\theta), \mathbf{Q}_m)$.

Assume now that condition (i) holds. If $k = 2m$ we can take $\xi_k = -\xi_m$, so that $\mathbf{Q}(\xi_m) = \mathbf{Q}(\xi_k)$ and $\mathbf{Q}_m = \mathbf{Q}_k$.

On the other hand, assume that m is odd, $3 \mid m$, $3^2 \nmid m$, $\frac{2m}{3} \mid (i-1)$ and $k = \frac{4}{3}m$. Also write $m = 3d_0$ and $k = 4d_0$, with $3 \nmid d_0$. Then we can conclude, as before, that $\mathbf{Q}_{3d_0} = \mathbf{Q}_{6d_0}$. If we set $m_1 = 4d_0$ and $k_1 = 6d_0$ we can apply (ii) proved above to obtain that $\mathbf{Q}_{3d_0} = \mathbf{Q}_{6d_0} = \mathbf{Q}_{4d_0}$, as desired. □

2 The Automorphism Group

In order to describe the group of automorphisms of the algebra $\mathbf{Q}G$, which we denote by $Aut(\mathbf{Q}G)$, we introduce three subgroups.

First, for each element $\mu \in U(\mathbf{Q}G)$, where $U(\mathbf{Q}G)$ stands for the set of invertible elements of $\mathbf{Q}G$, let us denote by τ_μ the inner automorphism induced by μ and set:

$$Inn(\mathbf{Q}G) = \{\tau_\mu \mid \mu \in U(\mathbf{Q}G)\},$$

which is a normal subgroup of $Aut(\mathbf{Q}G)$.

Given an index m, where $m|n, m \nmid d$, and an automorphism $\phi_m : \mathbf{Q}_m \to \mathbf{Q}_m$, we define an automorphism $\overline{\phi_m} : M_2(\mathbf{Q}_m) \to M_2(\mathbf{Q}_m)$ by:

$$\overline{\phi_m}(a_{ij}) = (\phi_m(a_{ij})) \ , \ (a_{ij}) \in M_2(\mathbf{Q}_m).$$

For each family of automorphisms $(\phi_m)_{\substack{m|n \\ m \nmid d}}$ we shall denote by $\Phi = (\overline{\phi_m})_{\substack{m|n \\ m \nmid d}}$ the automorphism of $\mathbf{Q}G$ which is the identity on $\mathbf{Q}(G/G')$ and coincides with $\overline{\phi_m}$ on $M_2(\mathbf{Q}_m)$, for each $m|n$, $m \nmid d$. We set:

$$\mathcal{M} = \{\Phi = (\overline{\phi_m})_{\substack{m|n \\ m \nmid d}} \mid \phi_m : \mathbf{Q}_m \to \mathbf{Q}_m \text{ is an automorphism } \}.$$

Also, given two integers m, k such that $\mathbf{Q}_m \cong \mathbf{Q}_k$ we notice that, since these fields are normal extensions of $\mathbf{Q}$, we actually have that $\mathbf{Q}_m = \mathbf{Q}_k$ and $\mathbf{Q}G$ contains two simple components that are isomorphic to the full matrix ring $M_2(\mathbf{Q}_m)$. Let σ_m be the automorphism of $\mathbf{Q}G$ that permutes these components and fixes all the others. We denote by $\mathcal{P}$ the subgroup

of $Aut(\mathbf{Q}G)$ generated by all such automorphisms, which will be a direct product of symmetric groups.

Finally, let Γ_1 be the set of all automorphisms γ of $\mathbf{Q}(G/G')$ which we extend to an automorphism of $\mathbf{Q}G$ by making them equal to the identity mapping on $\Delta(G:G')$ and denote by Γ_2 the set of automorphisms of $\Delta(G:G')$ which are the identity on $\mathbf{Q}(G/G')$. Then, clearly:

$$Aut(\mathbf{Q}G) = \Gamma_1 \times \Gamma_2$$

Theorem 2.1 *With the notations above, we have that:*

$$\Gamma_2 = (Inn(\mathbf{Q}G) \rtimes \mathcal{M}) \rtimes \mathcal{P}.$$

Proof. We shall prove first that $Inn(\mathbf{Q}G).\mathcal{M}$ is a semidirect product. So, assume that there exists an element $\Phi \in \mathcal{M} \cap Inn(\mathbf{Q}G)$. Since conjugations fix the centers of each direct summand, it follows immediately that $\Phi = I$.

Also, given $\Phi \in \mathcal{M}$ and $\mu \in U(\mathbf{Q}G)$, it is clear that the automorphism $\Phi^{-1} \circ \tau_\mu \circ \Phi$ gives, by restriction, an automorphism of every simple component, which fixes its center. By the Theorem of Skolem-Noether [4, Theorem 4.3.1] these restrictions are inner automorphisms on every component, so there exists an element ν such that $\Phi^{-1} \circ \tau_\mu \circ \Phi = \tau_\nu$, showing that $Inn(\mathbf{Q}G)$ is normal in $Inn(\mathbf{Q}G).\mathcal{M}$.

It is clear that $(Inn(\mathbf{Q}G) \rtimes \mathcal{M}) \cap \mathcal{P} = \{1\}$. Set now $\tau_\mu \circ \Phi \in (Inn(\mathbf{Q}G) \rtimes \mathcal{M}$ and $\sigma \in \mathcal{P}$ and compute:

$$\sigma^{-1} \circ (\tau_\mu \circ \Phi) \circ \sigma = (\sigma^{-1} \circ \tau_\mu \circ \sigma) \circ (\sigma^{-1} \circ \Phi \circ \sigma).$$

As before, $(\sigma^{-1} \circ \tau_\mu \circ \sigma)$ gives, by restriction, an automorphism of each simple component fixing its center so, it is of the form $(\sigma^{-1} \circ \tau_\mu \circ \sigma) = \tau_\nu$, for some $\nu \in U(\mathbf{Q}G)$. On the other hand, $\sigma^{-1} \circ \Phi \circ \sigma$ also gives, by restriction, an automorphism of every simple component, though it does not necessarily fix the corresponding center. Hence, on each component $M_2(\mathbf{Q}_m)$ is of the form $\tau_{\omega_m} \circ \overline{\psi_m}$, where ω_m is a unit of $M_2(\mathbf{Q}_m)$ and ψ_m is an automorphism of $\mathbf{Q}_m$ as mentioned above. Thus $\sigma^{-1} \circ \Phi \circ \sigma$ is of the form $\tau_\omega \circ \Psi$ so:

$$\sigma^{-1} \circ (\tau_\mu \circ \Phi) \circ \sigma = \tau_{\nu\omega} \circ \Psi \in Inn(\mathbf{Q}G) \rtimes \mathcal{M}.$$

Hence, $(Inn(\mathbf{Q}G) \rtimes \mathcal{M}).\mathcal{P}$ is a semidirect product.

Finally, we shall show that every element $f \in \Gamma_2$ is in $(Inn(\mathbf{Q}G) \rtimes \mathcal{M}) \rtimes \mathcal{P}$.

Note that, if $f(M_2(\mathbf{Q}_m)) = M_2(\mathbf{Q}_k)$ for some pair of indexes m, k, since the respective centers must also correspond, we have that $f(\mathbf{Q}_m) = \mathbf{Q}_k$ and, since these fields are normal extensions of $\mathbf{Q}$, actually $\mathbf{Q}_m = \mathbf{Q}_k$. Consequently, there exists an element $\sigma \in \mathcal{P}$ which permutes simple components in the same way as f so $f \circ \sigma^{-1}$ fixes every component of $\Delta(G : G')$. We denote by ϕ_m the automorphism that it defines, by restricion, on the corresponding centers and define $\Phi = (\overline{\phi_m})_{\substack{m|n \\ m \nmid d}}$.

Now, $f \circ \sigma^{-1} \circ \Phi^{-1}$ fixes every component and also its respective center so, there exists a unit $\mu \in \mathbf{Q}G$ such that $f \circ \sigma^{-1} \circ \Phi^{-1} = \tau_\mu$; hence:

$$f = \tau_\mu \circ \Phi \circ \sigma,$$

as desired. □

3 Some Examples

We conclude with a few examples, illustrating our result, where we examine closely the subgroups Γ_1 and $\mathcal{P}$.

Example 1. If n is either odd or of the form $n = 2^t$, it follows easily that $\mathcal{P} = \{1\}$.

Example 2. Let $n = 10$. Since $i^2 \equiv 1 \ (mod\ n)$, but $i \not\equiv 1 \ (mod\ n)$ it follows that $i = 9$. So $d = gcd(n, i-1) = 2$, hence $G' =< a^2 >$, $G/G' \cong C_2 \times C_2$ and thus:

$$\mathbf{Q}G \cong \mathbf{Q} \oplus \mathbf{Q} \oplus \mathbf{Q} \oplus \mathbf{Q} \oplus M_2(\mathbf{Q}_5) \oplus M_2(\mathbf{Q}_{10}).$$

Notice that $\Gamma_1 \cong S_4$ and that, according to Theorem 2.6. we have that $\mathbf{Q}_5 = \mathbf{Q}_{10}$ so, $\mathcal{P} = C_2$ and consequently:

$$Aut(\mathbf{Q}G) \cong S_4 \times ((Inn(\mathbf{Q}G) \rtimes \mathcal{M}) \rtimes C_2).$$

Example 3. Set $n = 12$. Then it follows easily that there are three possible values for i: $i_1 = 5$, $i_2 = 7$, $i_3 = 11$. We denote by G_1, G_2 G_3 the corresponding groups.

Consider first G_1. In this case, we have that $d = gcd(12, 4) = 4$ and $G_1' =< a^4 >$ so $|G_1'| = 3$ and $G_1/G_1' \cong C_4 \times C_2$.

Since $\mathbf{Q}C_4 \cong \mathbf{Q} \oplus \mathbf{Q} \oplus \mathbf{Q}(i)$ and $\mathbf{Q}(G_1/G_1') \cong \mathbf{Q}C_4 \otimes \mathbf{Q}C_2$, we have that $\mathbf{Q}(G_1/G_1') \cong \mathbf{Q} \oplus \mathbf{Q} \oplus \mathbf{Q} \oplus \mathbf{Q} \oplus \mathbf{Q}(i) \oplus \mathbf{Q}(i)$. Therefore,

$$\mathbf{Q}G_1 \cong \mathbf{Q} \oplus \mathbf{Q} \oplus \mathbf{Q} \oplus \mathbf{Q} \oplus \mathbf{Q}(i) \oplus \mathbf{Q}(i) \oplus M_2(\mathbf{Q}_3) \oplus M_2(\mathbf{Q}_6) \oplus M_2(\mathbf{Q}_{12}).$$

Clearly $\mathbf{Q}_3 \cong \mathbf{Q}_6 \cong \mathbf{Q}$ and $[\mathbf{Q}_{12} : \mathbf{Q}] = 2$. So $\mathcal{P} \cong C_2$.

We now observe that an automorphism of $\mathbf{Q}(G_1/G_1')$ which leaves invariant the simple components is necessarily the identity on the first four components. Also, note that $Gal(\mathbf{Q}(i) : \mathbf{Q}) \cong C_2$ and that an automorphism of $\mathbf{Q}(G_1/G_1')$ can actually interchange the first four simple components among themselves and also the last two ones. It is then easily seen that $Aut(\mathbf{Q}(G_1/G_1')) \cong (C_2 \times C_2) \rtimes (S_4 \times C_2)$.

Hence:

$$Aut(\mathbf{Q}G_1) \cong \Big((C_2 \times C_2) \rtimes (S_4 \times C_2)\Big) \times \Big((Inn(\mathbf{Q}G) \rtimes \mathcal{M}) \rtimes C_2\Big).$$

Now, let us consider G_2. We have that $d = gcd(12,6) = 6$ and $G_2' = < a^6 >$. So $|G_2'| = 2$ and $G_2/G_2' \cong C_6 \times C_2 \cong C_2 \times C_2 \times C_3$. Since $\mathbf{Q}C_3 \cong \mathbf{Q} \oplus \mathbf{Q}(i\sqrt{3})$, we have that:

$$\mathbf{Q}G_2 \cong \mathbf{Q} \oplus \mathbf{Q} \oplus \mathbf{Q} \oplus \mathbf{Q} \oplus \mathbf{Q}(i\sqrt{3}) \oplus \mathbf{Q}(i\sqrt{3}) \oplus \mathbf{Q}(i\sqrt{3}) \oplus \mathbf{Q}(i\sqrt{3}) \oplus M_2(\mathbf{Q}_4) \oplus M_2(\mathbf{Q}_{12}).$$

In order to compute $Aut(G_2/G_2')$ we proceed as above . Since $\mathbf{Q}_4 \neq \mathbf{Q}_{12}$, by theorem 1.5, we have that $\mathcal{P} = 1$ and thus:

$$Aut(\mathbf{Q}G_2) \cong \Big((C_2 \times C_2 \times C_2 \times C_2) \rtimes (S_4 \times S_4)\Big) \times \Big((Inn(\mathbf{Q}G) \rtimes \mathcal{M}\Big).$$

Finally, let us consider G_3. In this case $d = gcd(12,10) = 2$ and $G_3' = < a^{10} >$ so $|G_3'| = 6$ and $G_3/G_3' \cong C_2 \times C_2$. Hence:

$$\mathbf{Q}G_3 \cong \mathbf{Q} \oplus \mathbf{Q} \oplus \mathbf{Q} \oplus \mathbf{Q} \oplus M_2(\mathbf{Q}_3) \oplus M_2(\mathbf{Q}_4) \oplus M_2(\mathbf{Q}_6) \oplus M_2(\mathbf{Q}_{12}).$$

Now, it follows easily that $\mathbf{Q}_3 = \mathbf{Q}_4 = \mathbf{Q}_6 = \mathbf{Q}$. So:

$$Aut(\mathbf{Q}G_3) \cong S_4 \times \left((Inn(\mathbf{Q}G) \rtimes \mathcal{M}) \rtimes S_3\right).$$

Example 4. As a final example, we consider the case where $n = 60$ and $i = 59$. Then, $d = gcd(60, 58) = 2$ and $G' =< a^2 >$ so $G/G' \cong C_2 \times C_2$ and we have that:

$$\mathbf{Q}G \cong \mathbf{Q} \oplus \mathbf{Q} \oplus \mathbf{Q} \oplus \mathbf{Q} \oplus M_2(\mathbf{Q}_3) \oplus M_2(\mathbf{Q}_4) \oplus M_2(\mathbf{Q}_5) \oplus M_2(\mathbf{Q}_6) \oplus M_2(\mathbf{Q}_{10})$$

$$\oplus M_2(\mathbf{Q}_{12}) \oplus M_2(\mathbf{Q}_{15}) \oplus M_2(\mathbf{Q}_{20}) \oplus M_2(\mathbf{Q}_{30}) \oplus M_2(\mathbf{Q}_{60}).$$

Simple computations show that

$$\mathbf{Q}_3 = \mathbf{Q}_4 = \mathbf{Q}_6 = \mathbf{Q},$$

$$\mathbf{Q}_5 = \mathbf{Q}_{10},$$

$$\mathbf{Q}_{15} = \mathbf{Q}_{30}.$$

Consequently:

$$Aut(\mathbf{Q}G) \cong S_4 \times \left((Inn(\mathbf{Q}G) \rtimes \mathcal{M}) \rtimes (C_2 \times C_2 \times S_3)\right).$$

References

[1] D.B. Coleman, *Finite groups with isomorphic group algebras*, **Trans. Amer. Math. Soc. 105** (1962), 1 - 8.

[2] S. P Coelho and C. Polcino Milies, *Automorphisms of Group Algebras of Dihedral Groups*, **Boll. Unione Mat. Italiana**, to appear.

[3] C. W. Curtis and I. Reiner, *Representation Theory of Finite Groups and Associative Algebras*, Interscience, New York, 1962.

[4] I. N. Herstein, *Non Commutative Rings*, The Carus Math. Monographs, 1968.

[5] E. Jespers, G. Leal and C. Polcino Milies, *Units of Integral Group Rings of some Metacyclic Groups*, **Canad. Math. Bull.** to appear.

[6] G. Peterson, *On the Automorphism Group of an Integral Group Ring*, **Illinois J. of Math.**, 21, 4(1977), 836 - 844.

[7] S. K. Sehgal, *Topics in Group Rings*, Marcel Dekker, New York 1978.

Universidade de São Paulo
Caixa postal 20.570
01452-990 - São Paulo
Brazil
e-mail sonicoe@ime.usp.br

Memorial University of Newfoundland
St. John's, Newfoundland
A1C 5S7
Canada
e-mail ejespers@albert.math.mun.ca

Universidade de São Paulo
Caixa postal 20.570
01452-990 - São Paulo
Brazil
e-mail polcino@ime.usp.br

TRABALHOS DO DEPARTAMENTO DE MATEMÁTICA

TÍTULOS PUBLICADOS

95-01 BARROS, L.G.X. de and Juriaans, S.O. Loops whose Loop Algebras are Flexible. 25p.

95-02 GUIDORIZZI, H.L. - Jordan canonical form: an elementary proof, 12 p.

95-03 CATALAN A., and COSTA R. E-Ideals in Baric Algebras. 14p.

95-04 MARTIN, P.A. On the generating function of the decimal expansion of an irracional real numbers. 7p.

95-05 COELHO F.U., MARCOS E.N., MERKLEN H.A. and PLATZECK.M.I. Modules of Infinite Projective Dimension over Algebras whose Idempotent Ideals are Projective. 13p.

95-06 GUIDORIZZI, H. L. The family of functions $S_{,k}$ and the Liénard Equation. 22p.

95-07 GUIDORIZZI, H. L. On the Existence of Periodic Solution for the Equation $\ddot{x} + \alpha x^{2n+1}\dot{x} + x^{4n+3} = 0$. 5p.

95-08 CORTIZO, S.F. Extensões Virtuais. 27p.

95-09 CORTIZO, S.F. Cálculo Virtual. 31p.

95-10 GUIDORIZZI, H. L. On Periodic Solutions of Systems of the Type

$$\ddot{x} = H(y),\ \dot{y} = -\sum_{i=1}^{n} f_i(x)H_i(y) - g(x).$$ 16p.

95-11 OLIVA, S. M., PEREIRA, A. L. Attractors for Parabolic Problems with Non linear Boundary Conditions in Fractional Power Spaces. 28p.

95-12 CORDARO, P. D. Global hypoellipticity for $\overline{\partial}_b$ on certain compact three dimensional CR manifolds. 11p.

95-13 COELHO, F.U. and SKOWRONSKI, A. On Auslander-Reiten Components for Quasitilted Algebras. 16p.

95-14 COELHO, F.U. and HAPPEL, D. Quasitilted algebras admit a preprojective component. 12p.

95-15 GOODAIRE, E.G. and POLCINO MILIES, C. The torsion product property in alternative algebras. 10p.

95-16 GOODAIRE, E. G. and POLCINO MILIES, C. Central idempotents in alternative loop algebras. 7p.

95-17 GOODAIRE, E. G. and POLCINO MILIES, C. Finite conjugacy in alternative loop algebras. 7 p.

95-18 EXEL, R. Unconditional integrability for dual actions. 22p.

95-19 OLIVA, W.M. and SALLUM, E.M. The dynamic of malaria at a rice irrigation system. 11p.

95-20 FIGUEIREDO, L.M.V., GONÇALVES, J.Z. and SHIRVANI, M. Free Group Algebras in Certain Division Rings. 28p.

95-21 SHIRVANI, M. and GONÇALVES, J. Z. Algebraically Independent Orbits and Free Algebras.17p.

95-22 ARAGONA, J. Generalized functions on quasi-regular sets. 17p.

95-23 GUZZO JR., H. On normal and composition series for baric algebras. 18p.

95-24 DRUCK, I. de F. Um pouco da história de potências, exponenciais e logaritmos. 25p.

95-25 BARROS, L.G.X. de and JURIAANS, S.O. Integral Loop Rings of Code Loops. 7p.

95-26 GARCIA D., LOURENÇO M.L., MORAES L.A., and PAQUES O.W. The spectra of some algebras of analytic mappings. 15p.

95-27 BRASIL, A. JR Complete hipersurfaces of S^{n+1} with constant mean curvature and constant scalar curvature. 11p.

95-28 GUZZO JR., H. The bar-radical of baric algebras. 19p.

95-29 MARTINS, M.I.R. Composition factors of indecomposable modules. 26p.

95-30 CORTIZO, S.F. Cálculo Virtual - Parte II. 19p.
95-31 CORTIZO, S.F. Sobre o Cálculo Delta de Dirac. 18p.
95-32 COSTA, R. and SUAZO, A. The Multiplication Algebra of a Bernstein Algebra: Basic Results. 13p.
95-33 FABEL, E., GORODSKI, C. and RUMIN, M. Holonomy of Sub-Riemannian Manifolds. 34p.
95-34 MELO, S.T. Characterizations of Pseudodifferential Operators on the Circle. 9p.
96-01 GUZZO JR., H. On commutative train algebras of rank 3. 15p.
96-02 GOODAIRE, E. G. and POLCINO MILIES, C. Nilpotent Moufang Unit Loops. 9p.
96-03 COSTA, R. and SUAZO, A. The multiplication algebra of a train algebra of rank 3. 12p.
96-04 COELHO, S.P., JESPERS, E. and POLCINO MILIES, C. Automorphisms of Groups Algebras of Some Metacyclic Groups. 12p.

NOTA: Os títulos publicados nos Relatórios Técnicos dos anos de 1980 a 1994 estão à disposição no Departamento de Matemática do IME-USP.
Cidade Universitária "Armando de Salles Oliveira"
Rua do Matão, 1010 - Butantã
Caixa Postal - 66281 (Ag. Cidade de São Paulo)
CEP: 05389-970 - São Paulo - Brasil