The modular isomorphism problem for the groups of order 512

BETTINA EICK* and ALEXANDER KONOVALOV†

∗ Institut Computational Mathematics, Technical University Braunschweig, Pockelsstrasse 14, Braunschweig, 38106 Germany

† School of Computer Science & Centre for Interdisciplinary Research in Computational Algebra, University of St Andrews, St Andrews, Fife, KY16 9SX, Scotland

Abstract

For a prime p let G be a finite p-group and K a field of characteristic p. The Modular Isomorphism Problem (MIP) asks whether the modular group algebra KG determines the isomorphism type of G. We briefly survey the history of this problem and report on our computer-aided verification of the Modular Isomorphism Problem for the groups of order 512 and the field K with 2 elements.

1 Introduction

The Modular Isomorphism Problem is known for more than 50 years now. Despite various attempts to prove it or to find a counterexample for it, it is still open and remains one of the challenging problems in the theory of finite p-groups bordering on the theory of associative algebras.

Solutions for the modular isomorphism problem are available for various special types of p-groups. For example, MIP holds for

- abelian p-groups (Deskins [14]; an alternative proof was given by Coleman [12]);
- p-groups G of class 2 with G' elementary abelian (Sandling [34], Theorem 6.25);
- metacyclic p-groups (Bagiński [1] for $p > 3$; completed by Sandling [36]);
- 2-groups of maximal class (Carlson [11]; alternative proof by Bagiński [3]);
- p-groups G of maximal class, $p \neq 2$, where $|G| \leq p^{p+1}$ and G contains an abelian maximal subgroup (Caranti and Bagiński [2]);
- elementary abelian-by-cyclic groups (Bagiński [4]);
- p-groups with the center of index p^2 (Drensky [16]); and
- p-groups having a cyclic subgroup of index p^2 (Baginski and Konovalov, [5]).

This large number of rather special cases shows the significant interest in the problem, but it also exhibits that the problem is difficult to attack.

There are results on the groups of various small orders and the field with p elements available. For example, MIP holds for

- groups of order dividing p^4 (Passman [29]);
- groups of order 2^5 (Makasikis [26] with remarks by Sandling [34]; alternative proof by Michler, Newman and O'Brien [27]);
- groups of order p^5 (Kovacs and Newman, due to Sandling's remark in [35]; alternative proof by Salim and Sandling [32, 33]);

- groups of order 2^6 (Wursthorn [41, 42] using computers; theoretical proof by Hertweck and Soriano [21]);
- groups of order 2^7 (Wursthorn [9] using computers); and
- groups of orders 2^8 and 3^6 (Eick [17] using computers).

The results on the groups of order dividing 2^8 or 3^6 have been established using computers. As the groups of order dividing 2^8 or 3^6 are classified, this mainly requires an algorithm to check whether two modular group algebras are isomorphic. The first method for this purpose is due to Wursthorn [42]. It has been implemented in the C programming language. The implementation was used on the groups of order dividing 2^7, but this seems to be its limit. Eick [17] has developed a new and independent approach for such an isomorphism test. This is implemented in the ModIsom package [19] of the computational algebra system GAP [20] and proved to be practical for the groups of order 2^8 and 3^6.

We applied the implementation by Eick successfully to the 10494213 groups of order 512. This required some improvements as well as a parallelization of the implementation. We report on details of this large-scale computation below.

It is worth to mention that there is even stronger conjecture than MIP: the Modular Isomorphism Problem for Normalized Unit Groups (UMIP) asks whether a finite p-group G is determined by the normalized unit group of its modular group algebra over the field of p elements. Only a few results are known in this direction. For a long time, the positive solution of UMIP was known only for abelian p-groups. Recently it was solved for 2-groups of maximal class in [6] and for p-groups with the cyclic Frattini subgroup for $p > 2$ in [7]. In [23] UMIP was verified in GAP [20] for all 2-groups of order at most 32 using the LAGUNA package [10].

2 Invariants

A first step for a computational check of MIP is the computation of invariants of the considered groups which are known to be determined by the modular group algebra. Hence groups with different such invariants have non-isomorphic modular group algebras. The following lists some such invariants. For a group G we denote with $\mathcal{J}_i(G)$ the i-th term of the Jennings series of G.

(a) The exponent of the group G ([25]; see also [36]).

(b) The isomorphism type of the center of the group G ([38, 40]).

(c) The isomorphism type of the factorgroup G/G' ([40]; see also [29, 34]).

(d) The isomorphism type of the factorgroup $G/\Phi(G)$ ([15]).

(e) The isomorphism type of the factorgroup $G/(\gamma_2(G)^p\gamma_3(G))$ ([35]). This is also called *Sandling factor*.

(f) The minimal number of generators $d(G')$ of G' (follows immediately from Prop.III.1.15(ii) of [39]).

(g) The length of the Jennings series and the isomorphism types of the factors $\mathcal{J}_i(G)/\mathcal{J}_{i+1}(G)$, $\mathcal{J}_i(G)/\mathcal{J}_{i+2}(G)$, and $\mathcal{J}_i(G)/\mathcal{J}_{2i+1}(G)$ ([28, 31]).

(h) The number of conjugacy classes of elements of the group G and the number of conjugacy classes of all p^n-th powers of elements of the group G for all $n \in \mathbb{N}$ ([41]).

(i) The number of conjugacy classes of maximal elementary abelian subgroups of given rank ([30]). This is also called *Quillen invariant.*

(j) The so-called *Roggenkamp parameter*

$$R(G) = \sum_{i=1}^{t} \log_p |C_G(g_i)/\Phi(C_G(g_i))|,$$

where $\{g_1, \ldots, g_t\}$ is a set of representatives of the conjugacy classes of the group G (Roggenkamp, see [41]).

Additionally, the nilpotency class of a group G is determined provided if G has exponent p, or class 2, or G' is cyclic or G is a group of maximal class and contains an abelian subgroup of index p (see [5]).

3 Isomorphism testing for group algebras

In this section we recall the algorithm by Eick [17] and exhibit some refinements of it which have been necessary to deal with the groups of order 512.

Let $\mathbb{F}$ be the field with p elements and A a finite dimensional $\mathbb{F}$-algebra. The *automorphism group* $Aut(A)$ is the set of all bijective linear maps $\alpha : A \to A$ which are compatible with the multiplication: $\alpha(ab) = \alpha(a)\alpha(b)$ holds for all $a, b \in A$. The *canonical form* $Can(A)$ is a structure constants table for A which describes A up to isomorphism; that is, $A \cong B$ for two $\mathbb{F}$-algebras A and B if and only if $Can(A) = Can(B)$ holds.

Given a finite p-group G, our aim is to determine $Aut(\mathbb{F}G)$ and $Can(\mathbb{F}G)$. This facilitates an effective check of the modular isomorphism problem for the groups of a given order: we determine the canonical forms $Can(\mathbb{F}G)$ for all groups G considered and then determine isomorphisms by simply comparing the canonical forms.

3.1 A reduction to nilpotent algebras

Let G be a finite p-group and $\mathbb{F}$ the field with p elements. Let $I(G)$ denote the Jacobson radical of the modular group algebra $\mathbb{F}G$. As a first step, we recall the well-known reduction of our given task to the same task for $I(G)$.

Lemma 3.1

a) *$I(G)$ is a nilpotent subalgebra of $\mathbb{F}G$. Thus there exists an $l \in \mathbb{N}$ with*

$$I(G) > I(G)^2 > \ldots > I(G)^l > I(G)^{l+1} = \{0\}.$$

b) *$I(G)$ coincides with the augmentation ideal of $\mathbb{F}G$. Thus $\{g - 1 \mid g \in G, g \neq 1\}$ is a $\mathbb{F}$-basis for $I(G)$ and $\mathbb{F}G = I(G) \oplus \mathbb{F}$.*

Lemma 3.1 (b) implies that we can readily extend $Aut(I(G))$ and $Can(I(G))$ to $Aut(\mathbb{F}G)$ and $Can(\mathbb{F}G)$. Hence it is sufficient to compute $Aut(I(G))$ and $Can(I(G))$ only. The main advantage of this reduction is that $I(G)$ is a nilpotent algebra by Lemma 3.1 (a).

It is well-known that the Jennings series of the finite p-group G yields a basis for $I(G)$ which contains bases for all ideals of the power series of $I(G)$. This facilitates an efficient determination of the ideals of the power series of $I(G)$.

3.2 An induction approach

Let I be a finite dimensional nilpotent associative $\mathbb{F}$-algebra. We describe a method to determine the automorphism groups and the canonical form for I. The basic idea of this method is to use induction on the quotients of the power series $I > I^2 > \ldots > I^l > I^{l+1} = \{0\}$ of I; that is, we successively determine $C_j = Can(I/I^j)$ and $A_j = Aut(I/I^j)$ from $Can(I/I^{j-1})$ and $Aut(I/I^{j-1})$. Denote $I_j = I/I^j$ and let $d = dim(I_2)$.

The first step: In the initialisation step of the induction we consider the algebra I_2. This algebra satisfies $ab = 0$ for all $a, b \in I_2$. Thus every structure constants table for I_2 is a zero-table. Hence C_2 is the zero-table and $A_2 = GL(d, \mathbb{F})$ holds.

The induction step: In the induction step, we have determined C_{j-1} and generators and the order of A_{j-1}. Our aim is to compute C_j and generators and the order of A_j.

Let F be the free nilpotent associative algebra on d generators over $\mathbb{F}$. Then I_{j-1} is a quotient of F, say $I_{j-1} \cong F/R$ for some ideal R. Define $\overline{R}$ be the two-sided ideal of F generated by $FR \cup RF$. Then

$$I^*_{j-1} = F/\overline{R}$$

is the so-called *covering algebra* of I_{j-1}.

Eick [17] provides a detailed investigation of the covering algebra and an effective algorithm to compute a canonical table C^*_{j-1} for this algebra from the canonical table C_{j-1} of I_{j-1}. Here we recall the most important features of the covering algebra only. First, we note that the automorphism group A_{j-1} acts naturally on the covering algebra I^*_{j-1} by directly extending the action on F/R to $F/\overline{R}$.

Theorem 1 (Eick [17])
Let $\rho_j : A_j \to A_{j-1}$ be the natural homomorphism.

a) $I_j \cong I^*_{j-1}/U$ for some ideal U in I^*_{j-1}.
b) Let V be a canonical element in the orbit $U^{A_{j-1}}$. Then $I_j \cong I^*_{j-1}/V$ and C_j is the table of I^*_{j-1}/V with respect to the basis underlying the table C^*_{j-1}.
c) $im(\rho_j) = Stab_{Aut_{j-1}}(V)$ and $ker(\rho_j)$ is the elementary abelian p-group consisting of the automorphism which fix I/I^{j-1} and I^{j-1}/I^j pointwise.

Theorem 1 is used to reduce the induction step to an orbit-stabilizer computation. A general algorithm to compute orbits and stabilizers for finite groups is described in [22]. The problem inherent in this algorithm is that if the considered orbit is long, then the computation is time- and space-consuming. In our applications, the arising orbits are often huge. Thus the generic algorithm for finite groups is not going to succeed in most cases.

Eick [17] uses a special orbit-stabilizer algorithm. This exploits the fact that the kernel of the natural homomorphism $A_{j-1} \to A_2$ is a normal p-subgroup of A_{j-1}. Orbit representatives and their stabilizers under the action of a p-group can be determined with a highly effective method due to Schwingel [37]; This method avoids the explicit computation of the orbits. Using Schwingel's method, our desired orbit-stabilizer computations mainly reduce to an orbit-stabilizer computation under the action of $A_2 \cong GL(d, \mathbb{F})$. This reduction has been sufficient to determine canonical forms for the modular group algebras of the groups of order 2^8.

However, even with this very significant reduction of the problem, the arising orbits and stabilizers in the application to the groups of order 2^9 are frequently too large to be computed. Thus for this new application, we had to reduce the orbit-stabilizer problem further. We exploited an approach which is also used in [18]: we try to reduce the initial group $A_2 \cong GL(d, \mathbb{F})$ *a priori*.

3.3 Fingerprints and precomputing

Let $\varphi : I \to I_2$ denote the natural homomorphism and recall that $I_2 \cong \mathbb{F}^d$. Thus I_2 has $l = (p^d - 1)/(p - 1)$ one-dimensional subspaces. Let $M_1, \ldots, M_l$ denote their preimages under φ and note that $M_1, \ldots, M_l$ are subalgebras of I. In particular, each algebra M_i is nilpotent.

We *fingerprint* each of these subalgebras M; that is, we determine invariants of M. Suitable invariants are, for example, the dimensions of the quotients of the k initial terms of their power series for some given k. That is, given a subalgebra M, we compute $M = M^1 \geq M^2 \geq \ldots \geq M^{k+1}$ and determine the sequence $d_1, \ldots, d_k$ defined by $d_i = dim(M^i/M^{i+1})$. The larger we choose k, the better is the resulting fingerprint, but also the more time-consuming is its determination.

Given a fingerprint for each M in the list $M_1, \ldots, M_l$, we partition the subalgebras according to their fingerprints. For every occurring fingerprint f let L_f be the set of subalgebras with fingerprint f. Define V_f as the sum of all subalgebras in L_f. Then V_f is a subalgebra of I which contains I^2 and is an invariant for $Aut(I)$ and $Can(I)$.

We sort the set of all arising fingerprints and thus obtain a list $f_1, \ldots, f_r$ of fingerprints. Let $V_{f_1}, \ldots, V_{f_r}$ denote the corresponding set of subalgebras of I. Then in the first step of our algorithm we start with a basis for I_2 which exhibits the images of the subalgebras $V_{f_1}, \ldots, V_{f_r}$ under φ and we use the stabilizer in $GL(d, \mathbb{F})$ of these images as initialization for A_2.

As a result we can often reduce *a priori* to a comparatively small subgroup A_2 of $GL(d, \mathbb{F})$. This reduces the subsequent orbit-stabilizer computations significantly, since we act with a comparatively small subgroup of $GL(d, \mathbb{F})$ only.

4 The groups of order 512

The complete and non-redundant list of groups of order 512 contains 10494213 groups: these are available in the GAP Small Groups Library [8]. In this section we describe our strategy to check MIP for these groups and we provide some numerical information on the steps of computation.

Our strategy splits the computation into two steps: first, split the groups of order 512 into possibly small clusters by determining invariants of the groups which are determined by their group algebras and then, secondly, check MIP for the groups in a cluster for each cluster.

4.1 Computing invariants

We used the invariants listed in Section 2 for the first step. Most of these invariants can be computed readily using available GAP functions; the others are implemented in the LAGUNA package [10]. The computation of these invariants for all groups of order 512 was already a first long-term computation. We outline some more details in the following.

On the initial stage, the following parameters were computed for all groups of order 512 to obtain an initial distribution of groups into clusters: the exponent of G, the number of conjugacy classes of G, orders of $Z(G)$, G', the Frattini subgroup of G and the Sandling factor $G/(\gamma_2(G)^p\gamma_3(G))$, the length of the Jennings series and the Roggenkamp parameter $\sum_{i=1}^{t} \log_p|C_G(g_i)/\Phi(C_G(g_i))|$. These parameters were selected on the ground that they can be computed very effectively and some of them, especially the Roggenkamp parameter, are known to be rather efficient invariants to check that group algebras are non-isomorphic.

As a result of this initial computation, the groups of order 512 were split into 30605 clusters of various sizes. For example, we obtained 5678 clusters of size 1; The groups contained in these need not be considered any further. On the other end, there were four clusters containing more than 100000 groups each, with sizes 110248, 112390, 115807 and 118504.

However, it occurs that the majority of these groups has a Sandling factor of order 512. In this case, the groups are determined by their modular group algebras. After filtering out such groups and also all clusters of size 1, it remained 1646012 groups in 19877 clusters, including 3373 pairs of groups, and the biggest cluster had size 9175 ('only').

To further refine the set of clusters, the following invariants were computed for the remaining groups: the isomorphism type of $Z(G)$ and G/G', and the number of conjugacy classes of p^n-th powers of elements. This step ruled out only 23222 groups, leaving still 1622790 groups to go, but, however, it increased the number of clusters to 51103 and reduced an average size of the cluster: now we already had 14770 pairs, and the largest cluster contained 5424 groups.

The above mentioned computations were made using the GAP package ParGAP [13] on an 8-core computer.

To split families further, the Quillen invariant (that is, the number of conjugacy classes of maximal elementary abelian subgroups of each rank) was selected. Its computation is rather time-consuming, since it involves computation of the lattice of subgroups. Thus we extended computations on other CIRCA machines, GILDA cluster available to the 2nd author for the time of the International Winter School in Grid Computing 2009, and Beowulf cluster in the Heriot-Watt University. Dependently on the architecture, we used various technologies: SCSCP package [24], ParGAP package [13] or the Condor job submission system (`http://www.cs.wisc.edu/condor/`). This computation finished with the following improvement: 1553963 groups in 97116 clusters, including 35486 pairs and the largest cluster of size 1827.

Two more group-theoretical invariants were applied after this stage: the minimal number of generators of G' and the isomorphism types of factors of the Jennings series.

As a final result of the invariant computation, we obtained 345367 clusters containing 1297026 groups mostly in small clusters, including 168486 pairs and the biggest cluster of size 210.

4.2 Isomorphism testing

Now we were able to split each of the clusters using the isomorphism test implemented in the ModIsom package.

This computation consumed about 14000 CPU hours during three weeks of computations on the UK National Grid Service (`http://www.ngs.ac.uk/`).

At first, Modisom split successfully all clusters except 293 exceptional clusters containing in total 1660 groups. These clusters needed an improvement of the implementation in Modisom as described in Section 3.3 of this paper.

After implementing this improvement, Modisom was able to split the remaining clusters and hence returned the result that there are no counterexamples to the modular isomorphism problem among the groups of order 512.

Acknowledgments: Besides the CIRCA computational facilities in St Andrews, we used the research server of the Functional Programming group in the University of St Andrews, Beowulf cluster in the Heriot-Watt University (Edinburgh), the GILDA cluster provided for IWSGC'09, and the UK National Grid Service. We acknowledge all involved organizations for these opportunities.

References

[1] C. Bagiński, The isomorphism question for modular group algebras of metacyclic p-groups, Proc. Amer. Math. Soc. **104** (1988), no. 1, 39–42.
[2] C. Bagiński and A. Caranti, The modular group algebras of p-groups of maximal class, Canad. J. Math. **40** (1988), no. 6, 1422–1435.
[3] C. Bagiński, Modular group algebras of 2-groups of maximal class, Comm. Algebra **20** (1992), no. 5, 1229–1241.
[4] C. Bagiński, On the isomorphism problem for modular group algebras of elementary abelian-by-cyclic p-groups, Colloq. Math. **82** (1999), no. 1, 125–136.
[5] C. Bagiński and A. Konovalov, The modular isomorphism problem for finite p-groups with a cyclic subgroup of index p^2, Groups St. Andrews 2005. Vol. 1, 186–193,

London Math. Soc. Lecture Note Ser., 339, Cambridge Univ. Press, Cambridge, 2007.

[6] Zs. Balogh, A. Bovdi, On units of group algebras of 2-groups of maximal class, Comm. Algebra **32** (2004), no. 8, 3227–3245.

[7] Zs. Balogh, A. Bovdi, Group algebras with unit group of class p, Publ. Math. Debrecen **65** (2004), no. 3-4, 261–268.

[8] H.U. Besche, B. Eick and E. O'Brien. The SmallGroups Library. `http://www-public.tu-bs.de:8080/~beick/soft/small/small.html`.

[9] F. M. Bleher et al., Computational aspects of the isomorphism problem, in *Algorithmic algebra and number theory (Heidelberg, 1997)*, 313–329, Springer, Berlin.

[10] V. Bovdi, A. Konovalov, R. Rossmanith and Cs. Schneider. *LAGUNA – Lie AlGebras and UNits of group Algebras*, Version 3.5.0; 2009, `http://www.cs.st-andrews.ac.uk/~alexk/laguna.htm`.

[11] J. F. Carlson, Periodic modules over modular group algebras, J. London Math. Soc. (2) **15** (1977), no. 3, 431–436.

[12] D. B. Coleman, On the modular group ring of a p-group, Proc. Amer. Math. Soc. **15** (1964), 511–514.

[13] G. Cooperman. *ParGAP – Parallel GAP, Version 1.1.2*; 2004, `http://www.ccs.neu.edu/home/gene/pargap.html`.

[14] W. E. Deskins, Finite Abelian groups with isomorphic group algebras, Duke Math. J. **23** (1956), 35–40.

[15] E. M. Dieckmann, Isomorphism of group algebras of p-groups, Ph.D. thesis, Washington University, St. Louis, Missouri, 1967.

[16] V. Drensky, The isomorphism problem for modular group algebras of groups with large centres, in *Representation theory, group rings, and coding theory*, 145–153, Contemp. Math., 93, Amer. Math. Soc., Providence, RI.

[17] B. Eick, Computing automorphism groups and testing isomorphisms for modular group algebras, J. Algebra **320** (2008), 3895 – 3910.

[18] B. Eick, C.R. Leedham-Green and E.A. O'Brien, Constructing automorphism groups of p-groups, Comm. Alg. **30** (2002), 2271 – 2295.

[19] B. Eick, *ModIsom – Computing automorphisms and checking isomorphisms for modular group algebras of finite p-groups, Version 1.0*; 2009, `http://www-public.tu-bs.de:8080/~beick/so.html`.

[20] The GAP Group, *GAP – Groups, Algorithms, and Programming, Version 4.4.12*; 2008, (`http://www.gap-system.org`).

[21] M. Hertweck and M. Soriano, On the modular isomorphism problem: groups of order 2^6. Groups, rings and algebras, Contemp. Math., 420, Amer. Math. Soc., Providence, RI, 2006, 177–213.

[22] D.F. Holt, B. Eick and E.A. O'Brien, *Handbook of computational group theory*, CRC Press, 2005.

[23] A. Konovalov and A. Krivokhata, On the isomorphism problem for unit groups of modular group algebras. Acta Sci. Math. (Szeged) **73** (2007), no. 1-2, 53–59.

[24] A. Konovalov and S. Linton, *SCSCP – Symbolic Computation Software Composability Protocol, Version 1.1*; 2009, (`http://www.cs.st-andrews.ac.uk/~alexk/scscp.htm`).

[25] B. Külshammer, Bemerkungen über die Gruppenalgebra als symmetrische Algebra. II, J. Algebra **75** (1982), no. 1, 59–69.

[26] A. Makasikis, Sur l'isomorphie d'algèbres de groupes sur un champ modulaire, Bull. Soc. Math. Belg. **28** (1976), no. 2, 91–109.

[27] G. O. Michler, M. F. Newman and E. A. O'Brien, Modular group algebras. Unpublished report, Australian National Univ., Canberra, 1987

[28] I. B. S. Passi and S. K. Sehgal, Isomorphism of modular group algebras, Math. Z. **129** (1972), 65–73.

[29] D. S. Passman, The group algebras of groups of order p^4 over a modular field, Michigan Math. J. **12** (1965), 405–415.

[30] D. Quillen, The spectrum of an equivariant cohomology ring: I, Ann. of Math. (2)**94** (1971), 549–572.

[31] J. Ritter and S. Sehgal, Isomorphism of group rings, Arch. Math. (Basel) **40** (1983), no. 1, 32–39.

[32] M. A. M. Salim and R. Sandling, The modular group algebra problem for groups of order p^5, J. Austral. Math. Soc. Ser. A **61** (1996), no. 2, 229–237.

[33] M. A. M. Salim and R. Sandling, The modular group algebra problem for small p-groups of maximal class, Canad. J. Math. **48** (1996), no. 5, 1064–1078.

[34] R. Sandling, The isomorphism problem for group rings: a survey, in *Orders and their applications (Oberwolfach, 1984)*, 256–288, Lecture Notes in Math., 1142, Springer, Berlin.

[35] R. Sandling, The modular group algebra of a central-elementary-by-abelian p-group, Arch. Math. (Basel) **52** (1989), no. 1, 22–27.

[36] R. Sandling, The modular group algebra problem for metacyclic p-groups, Proc. Amer. Math. Soc. **124** (1996), no. 5, 1347–1350.

[37] R. Schwingel, Two matrix group algorithms with applications to computing the automorphism group of a finite p-group, PhD Thesis, Queen Mary University, London.

[38] S. K. Sehgal, On the isomorphism of group algebras, Math. Z. **95** (1967), 71–75.

[39] S. K. Sehgal, *Topics in group rings*, Dekker, New York, 1978.

[40] H. N. Ward, Some results on the group algebra of a p-group over a prime field, Seminar on Finite Groups and Related Topics, pp.13-19. Mimeographed notes, Harvard Univ.

[41] M. Wursthorn, Die modularen Gruppenringe der Gruppen der Ordnung 2^6. Diplomarbeit, Universität Stuttgart, 1990.

[42] M. Wursthorn, Isomorphisms of modular group algebras: an algorithm and its application to groups of order 2^6, J. Symbolic Comput. **15** (1993), no. 2, 211–227.