Constructing Rational Representations of Finite Groups

Wilhelm Plesken and Bernd Souvignier

CONTENTS

We present a method to construct irreducible rational matrix representations of finite groups, based on an efficient construction of fixed points of finite groups acting on complex vector spaces.

1. INTRODUCTION

For finite fields there are satisfactory methods to construct the irreducible representations of a finite group [Parker 1984; Holt and Rees 1994]. When it comes to computing representations over the complex numbers, one can use the ideas in [Dixon 1970] to come up with approximate solutions. For algebraic applications, however, one would prefer precise descriptions. This paper outlines a first approach to the problem of how irreducible rational representations can be constructed by computing and analysing endomorphisms and homomorphisms of modules.

With the complex group algebra $\mathbb{C}G$ of a finite group G, the rational group algebra $\mathbb{Q}G$ still shares the property of being semisimple. With the group algebra $\mathbb{F}_qG$ over a finite field it shares the practical property that computations can be done in a precise rather than an approximate (numerical) way. The main point of this paper is to show that the precise calculations can be performed in a practical way when it comes to modules of dimensions around 200. However, unlike $\mathbb{C}G$ and $\mathbb{F}_qG$, the rational group algebra $\mathbb{Q}G$ might have simple modules whose endomorphism rings are not commutative, so that Schur indices are involved. Deciding whether a homogeneous $\mathbb{Q}G$-module, i.e., a module isomorphic to a multiple of a simple module,

Key words and phrases: rational representations of finite groups, algorithms.

1991 Mathematics Subject Classification: Primary 20C15; Secondary 20C05, 20C40.

is simple or not, will in general call for a p-adic analysis of its endomorphism ring. In Section 5 we outline some methods for avoiding this in most relevant cases.

The paper is centred around Theorem 2.1, which might have other applications as well, as in the computation of polynomial invariants of finite matrix groups. The theorem was known in some special situations [Dixon 1970], in which we also apply it. However, since we are dealing with the rational numbers, we can use the approximative process of Theorem 2.1 to compute precise rather than approximative solutions; see also Section 4.

There are other techniques available to construct rational representations, for instance by reducing permutation or monomial representations, where it is easy to compute the endomorphism ring, or for special classes of finite groups, such as soluble groups, or under special assumptions for the characters as in [Dixon 1993]. These topics will not be discussed in this paper.

2. APPROXIMATING THE AVERAGING OPERATOR

Theorem 2.1. *Let G be a finite group, V a finite-dimensional $\mathbb{C}G$-Module, $E \subseteq G$ a generating set of G with $1 \in E$. Define*

$$\rho : V \to V : v \mapsto \frac{1}{|G|}\sum_{g\in G} gv$$

to be the $\mathbb{C}G$-projection of V onto the stabilizer $\mathrm{Fix}_G(V)$ of the G-action on V, and

$$\rho_E : V \to V : v \mapsto \frac{1}{|E|}\sum_{g\in E} gv.$$

Then inside $\mathrm{End}_{\mathbb{C}}(V)$ one has $\lim_{n\to\infty} \rho_E^n = \rho$.

Remark. We have $\mathrm{End}_{\mathbb{C}}(V) \cong \mathbb{C}^{l\times l}$ if $l = \dim_{\mathbb{C}} V$, which clarifies the notation of convergence. Clearly $\mathbb{C}$ can be replaced by any of its subfields in the above theorem.

Proof. Since V is an epimorphic image of a finitely generated free $\mathbb{C}G$-module $({}_{\mathbb{C}G}\mathbb{C}G)^n$, one may assume that V is the regular $\mathbb{C}G$-Module ${}_{\mathbb{C}G}\mathbb{C}G$. Denote the matrix representation of V with respect to the canonical basis G by Δ. Then clearly $X := \Delta(\rho_E)$ is a doubly stochastic matrix.

Claim: X is irreducible (in the sense that there is no permutation matrix P of degree $|G|$ such that PXP^{-1} is triangular). To prove this, note that each element of G can be written as a word of length n in the elements of E, since $1 \in E$, provided n is big enough. But this means that X^n has no entries 0, hence X^n and therefore X is irreducible. By the Theorem of Perron–Frobenius on nonnegative matrices, [Huppert 1990, p. 398], X has exactly one eigenvalue 1 with multiplicity one, and all its other eigenvalues of norm less than 1. Hence X^n converges, and therefore also ρ_E^n. Obviously the limit is ρ. □

Some comments on the proof are appropriate. The result is closely connected with [Dixon 1970, Theorem 1] and [Schlosser 1978, Satz 2]. Though the main applications will be in the same context as in [Dixon 1970], we shall use it to perform precise calculations (see Section 4), rather than approximate ones as in that paper. Our proof is different and relates the result to the ideas in [Thompson 1981]. It allows the following extensions of the result:

Let $\mathbb{R}G_{1,\geq 0}$ be the set of formal convex combinations of elements of G, that is, the subset of $\mathbb{R}G$ consisting of elements of the form

$$\sum_{g\in G}\alpha_g G \quad \text{with } \sum_{g\in G}\alpha_g = 1 \text{ and } \alpha_g \geq 0 \text{ for all } g \in G.$$

For $e = \sum_{g\in G} \alpha_g g \in \mathbb{R}G_{1,\geq 0}$, define $\rho_e : V \to V$ by

$$\rho_e(v) = \sum_{g\in G} \alpha_g gv = ev.$$

Then ρ_e^n converges to ρ if $e \in \mathbb{R}G_{1,\geq 0}^{\mathrm{gen}}$, where $\mathbb{R}G_{1,\geq 0}^{\mathrm{gen}}$ is the set of $e \in \mathbb{R}G_{1,\geq 0}$ such that e^n has no nonzero coefficient in its expansion in the elements of G, for sufficiently big n. Note that $\mathbb{R}G_{1,\geq 0}$ is multiplicatively closed and convex.

3. THE RATE OF CONVERGENCE

For each $e \in \mathbb{R}G_{1,\geq 0}$ and each character χ of G, define $\mathrm{Spec}_\chi(e)$ to be the set of all eigenvalues of $\Gamma(e)$, where Γ is a complex representation of G with character χ, and set

$$r_\chi(e) = \max\left\{|a| : a \in \mathrm{Spec}_\chi(e)\right\}.$$

Remark 3.1. Let $\chi = \sum_{i=1}^k m_i\chi_i = m_1 1 + \chi'$ be the character of the $\mathbb{C}G$-module V decomposed into complex irreducible characters $\chi_1 = 1, \chi_2, \dots, \chi_h$. For $e \in \mathbb{R}G_{1,\geq 0}$ one has:

(i) $r_{\chi'}(e) = \max\{r_{\chi_i}(e) : i = 2, \dots, h,\ m_i \neq 0\}$.

(ii) $\rho_e^n \to \rho$ for $n \to \infty$ iff $r_{\chi'}(e) < 1$.

(iii) In case $r_{\chi'}(e) < 1$, one has

$$\|\rho - \rho_e^n\| \leq (r_{\chi'}(e) + \varepsilon)^n$$

for any $\varepsilon > 0$ and n bigger than some constant depending on ε, where $\|\cdot\|$ is any algebra norm on $\mathrm{End}_{\mathbb{C}}(V)$.

Proof. Parts (i) and (ii) are clear, and (iii) follows from the proof of [Huppert 1990, Satz II.2.10], if one notes $\rho - \rho_e^n = (\rho - \rho_e)^n$. □

So one has linear convergence and wants $r_{\chi'}(e)$ to be as small as possible. Here are some ideas that are tested in examples to get a good $e \in \mathbb{R}G^{\text{gen}}_{1,\geq 0}$. Replacing $e = |E|^{-1}\sum_{g\in E} g$ by $e = \sum_{g \in E}\alpha_g g$, with $0 < \alpha_g < 1$ and $\sum_{g\in E}\alpha_g = 1$, leads only to small improvements. Replacing E by a different set E' of generators with elements of bigger order often works better. Finally, using

$$e = \prod_{g\in E',\ g\neq 1} \left(\tfrac{1}{2}(1 - g)\right)$$

usually leads to drastic improvements. Often

$$e = \prod_{g\in E,\ g\neq 1} \frac{1}{|g|}(1 + g + g^2 \dots + g^{|g|-1})$$

yields a smaller $r_{\chi'}(e)$, but one step of the iterations becomes much more expensive. In this context it should be noted that for applications in Section 5 these factorised versions of elements of $\mathbb{R}G_{1,\geq 0}$ turn out to be time-saving, since one can compute factor by factor; however, for an element of the form $\sum_{g\in E}\alpha_g g$ one is forced to compute the gv first and then form the $\sum_{g\in E}\alpha_g(gv)$. The example in Section 7 below demonstrates how good candidates for e can be found.

Finally, in an actual computation with a given $e \in \mathbb{R}G^{\text{gen}}_{1,\geq 0}$ and $v \in V$, one needs a reasonable estimate for $\|\rho(v) - \rho_e^n(v)\|$ for some suitable norm $\|\cdot\|$ on V. Let $v_n = \rho_e^n(v)$. Then $v_{n+1} - v_n$ has no $\mathrm{Fix}_G(V)$-component. In case $\|v_{n+1} - v_n\| \neq 0$ for one n it will be nonzero for all $n > 0$, and

$$\lambda_n := \frac{\|v_{n+1} - v_n\|}{\|v_n - v_{n-1}\|}$$

converges to some λ (see also [Huppert 1990, Satz IV.1.15]), which is equal to the biggest absolute value of the biggest eigenvalues $\neq 1$ of ρ_e on the space spanned by the v_i. Usually this λ will be equal to $r_{\chi'}(e)$, hence the geometric series yields $\lambda^n/(1-\lambda)$ as a realistic estimate for $\|\rho(v) - \rho_e^n(v)\|$.

4. EXACT SOLUTIONS AND INTEGRALITY

In this section we assume that V is a $\mathbb{Q}G$-module rather than a $\mathbb{C}G$-module and that V is given by a full $\mathbb{Z}G$-lattice L in V. In terms of the matrix representation Δ with respect to a lattice basis of L one gets integral matrices, and for any $v \in L$ one has already a divisor d of $|G|$ with $d\rho(v) \in L$. Therefore one will proceed as follows: In the course of the iteration $v = v_1, v_2, \dots, v_n = \rho_e^n(v), \dots$ one will test whether the coordinates of v_n with respect to a lattice basis of L are very close to a rational number with a promising denominator, e.g., by using a continued fraction expansion of the coordinates. Having found a reasonable denominator d one replaces v_n by $v = d^{-1}\bar{v}_n$ with $\bar{v}_n$ the vector in L closest to v_n. If $v \in \mathrm{Fix}_G(V)$ one is done; otherwise one continues the iteration. By the remarks at the end of Section 3 one has good control over the error. This procedure works well, even if the order of G is not known (and therefore yields divisors of $|G|$ in this situation). We have successfully used it for modules of dimension around $40,000$.

5. APPLICATION TO THE CONSTRUCTION OF RATIONAL REPRESENTATIONS

In this section we demonstrate how the ideas developed so far can be used to find the irreducible constituents of a rational representation of G.

Assume that a $\mathbb{Q}G$-module M is given by a full $\mathbb{Z}G$-lattice $L \subseteq M$. Then the following are $\mathbb{Z}G$-lattices that span $\mathbb{Q}G$-modules to which one can apply Theorem 2.1.

(i) $\overline{\mathbb{Z}G}$, the image of $\mathbb{Z}G$ in $\mathrm{End}_{\mathbb{Q}}(M)$ under the representation $^{-} : \mathbb{Q}G \to \mathrm{End}_{\mathbb{Q}}(M)$. We have $\overline{\mathbb{Z}G} \subseteq \overline{\mathbb{Q}G}$. Here G acts by conjugation: $g : \varphi \mapsto \bar{g}\varphi\bar{g}^{-1}$ for $g \in G$ and $\varphi \in \overline{\mathbb{Z}G}$.

(ii) $\mathrm{End}_{\mathbb{Z}}(L) \subseteq \mathrm{End}_{\mathbb{Q}}(M)$. Here G acts by conjugation as in (i); indeed $\overline{\mathbb{Z}G}$ is a $\mathbb{Z}$-sublattice of $\mathrm{End}_{\mathbb{Q}}(M)$.

(iii) $\mathrm{Bil}_{\mathbb{Z}}(L)$, the space of $\mathbb{Z}$-bilinear maps $\Phi : L \times L \to \mathbb{Z}$, and a subspace of $\mathrm{Bil}_{\mathbb{Q}}(L)$. Here $g \in G$ maps $\Phi \in \mathrm{Bil}_{\mathbb{Z}}(L)$ to the map ${}_g\Phi$ defined by ${}_g\Phi(m_1, m_2) = \Phi(g^{-1}m_1, g^{-1}m_2)$ for all m_1 and m_2 in L.

(iv) If M' is a further $\mathbb{Q}G$-representation module spanned by a $\mathbb{Z}G$-lattice $L' \subseteq M'$, one has a further $\mathbb{Z}G$-lattice $\mathrm{Hom}_{\mathbb{Z}}(L, L') \subseteq \mathrm{Hom}_{\mathbb{Q}}(M, M')$, where G acts as in (ii).

The machinery developed in Sections 2–4 allows to compute, as fixed point sets of the modules above, elements or even a basis of each of the following:

(i) $Z(\overline{\mathbb{Q}G}) = Z(\mathrm{End}_{\mathbb{Q}G}(M))$, where Z denotes the centre.

(ii) $\mathrm{End}_{\mathbb{Q}G}(M)$.

(iii) $\mathrm{Bil}_{\mathbb{Q}G}(M)$, the space of $\Phi \in \mathrm{Bil}_{\mathbb{Q}}(M)$ such that ${}_g\Phi = \Phi$ for all $g \in G$.

(iv) $\mathrm{Hom}_{\mathbb{Q}G}(M, M')$.

We comment on each case separately.

5(i). $Z(\mathrm{End}_{\mathbb{Q}G}(\mathsf{M}))$: Splitting M into its Homogeneous Components

Lemma 5.1. Let $V = \overline{\mathbb{Q}G}$ and ρ as in Theorem 2.1. Denote the image of $g \in G$ in $\overline{\mathbb{Q}G} \subseteq \mathrm{End}_{\mathbb{Q}}(M)$ by $\bar{g}$. Then the eigenvalues of $\rho(\bar{g})$ are given by $\chi(g)/\chi(1)$ with multiplicity $m_\chi\chi(1)$, where χ is a complex irreducible character of G occurring with multiplicity m_χ in the character afforded by M.

Proof. It suffices to assume that M is an irreducible $\mathbb{C}G$-module with character χ. Then $\rho(\bar{g}) = |G|^{-1} \sum_{h \in G} \bar{h}^{-1}\bar{g}\bar{h} = \lambda\, \mathrm{id}_M$ by Schur's Lemma. The result follows by comparing traces. □

Hence, if the splitting of the character of M into irreducibles is known and one has access to representatives of the conjugacy classes, one can easily produce elements $x_i \in \mathrm{End}_{\mathbb{Q}G}(M)$ such that the kernels (or the images) of the x_i are the homogeneous components of M. If one does not know the irreducible characters one still can produce elements of $Z(\mathrm{End}_{\mathbb{Q}G}(M))$, but then one has to factorise the minimum polynomials of the elements computed to get a splitting of M. If this fails, one computes a basis for $Z(\mathrm{End}_{\mathbb{Q}G}(M))$ and decomposes $Z(\mathrm{End}_{\mathbb{Q}G}(M))$ into its minimal ideals, again by factorising minimum polynomials.

5(ii). $\mathrm{End}_{\mathbb{Q}G}(\mathsf{M})$

Usually one will approach this problem only if M is already homogeneous, that is, (i) is performed and $Z(\mathrm{End}_{\mathbb{Q}G}(M))$ is already computed. Again the characters tell us the dimension of $\mathrm{End}_{\mathbb{Q}G}(M)$, which is a simple $\mathbb{Q}$-algebra. Hence one will compute two elements of $\mathrm{End}_{\mathbb{Q}G}(M)$, say $\rho(x_1)$ and $\rho(x_2)$, for $x_1, x_2 \in \mathrm{End}_{\mathbb{Q}}(M)$, and see whether they generate $\mathrm{End}_{\mathbb{Q}G}(M)$ as an algebra, and compute more $\rho(x_i)$ if necessary. One ends up with a basis of $\mathrm{End}_{\mathbb{Q}G}(M)$ and the regular representation of $\mathrm{End}_{\mathbb{Q}G}(M)$. If one has not found singular elements in the course of the computation, one has to analyse $\mathrm{End}_{\mathbb{Q}G}(M)$, some ideas for this will be sketched in Section 6. There is one more situation where it is worthwhile to work with $\mathrm{End}_{\mathbb{Q}}(M)$, namely if one wants to compute $Z(\mathrm{End}_{\mathbb{Q}G}(M))$ for irreducible M, when the Schur index of M is 1, i.e., $\mathrm{End}_{\mathbb{Q}G}(M)$ is commutative: This is because in (i) one might have difficulties finding a suitable $g \in G$ to start with if there are only few classes with irrational character values.

5(iii). $\mathrm{Bil}_{\mathbb{Q}G}(M)$: Invariant Bilinear Forms

There are various situations when bilinear forms, both symmetric and antisymmetric, are relevant. First of all, one is well advised to keep with each matrix representation an invariant positive definite scalar product, because this allows one to manipulate the basis by various reduction routines to keep small coefficients for the matrix entries in the representation. For dimensions below forty the algorithm of [Seysen 1993] is often very efficient for this purpose. If one does not have an invariant symmetric positive definite bilinear form, one gets one by applying the averaging operator ρ to any symmetric positive definite $\Phi \in \mathrm{Bil}_{\mathbb{Z}}(L)$. In practice one will start with some $\Phi \in \mathrm{Bil}_{\mathbb{Z}}(L)$, whose symmetric part is only positive semidefinite $\neq 0$ and whose antisymmetric part is nonzero. Then $\rho(\Phi) = \Phi_s + \Phi_a$, where the symmetric and antisymmetric parts $\Phi_s, \Phi_a \in \mathrm{Bil}_{\mathbb{Q}G}(M)$ can easily be extracted from $\rho(\Phi)$. (Note that switching the arguments in Φ commutes with ρ.) Φ_s will be nonzero positive semidefinite. If it is not positive definite, its radical will be a $\mathbb{Q}G$-submodule of M, which is always a welcome reduction. If Φ_s is positive definite, it turns $\mathrm{End}_{\mathbb{Q}G}(M)$ into an algebra with involution. This becomes immediately clear if one identifies $\mathrm{Bil}_{\mathbb{Q}G}(M)$ with $\mathrm{Hom}_{\mathbb{Q}G}(M, M^{\#})$, where $M^{\#} = \mathrm{Hom}_{\mathbb{Q}}(M, \mathbb{Q})$ is the contragredient module of M. Of course one can do this on the level of $\mathbb{Z}G$-lattices as well.

Remark 5.2. Let $\Phi \in \mathrm{Bil}_{\mathbb{Q}G}(M) \equiv \mathrm{Hom}_{\mathbb{Q}G}(M, M^{\#})$ be nondegenerate, and symmetric or antisymmetric. Then Φ turns $\mathrm{End}_{\mathbb{Q}G}(M)$ into a $\mathbb{Q}$-algebra with involution ι by

$$\iota : \mathrm{End}_{\mathbb{Q}G}(M) \to \mathrm{End}_{\mathbb{Q}G}(M) : \alpha \mapsto \Phi\alpha^{\mathrm{tr}}\Phi^{-1},$$

where $\alpha^{\mathrm{tr}} : M^{\#} \to M^{\#}$ is the transpose of α.

In the above situation, if Φ_a or Φ_s is nondegenerate, that is, represents a $\mathbb{Q}G$-isomorphism $M \to M^{\#}$, then $\Phi_a\Phi_s^{-1}$ and $\Phi_s\Phi_a^{-1}$ lie in $\mathrm{End}_{\mathbb{Q}G}(M)$. So one gets an element of $\mathrm{End}_{\mathbb{Q}G}(M)$ and via the involution a new element for each further element one computes in $\mathrm{End}_{\mathbb{Q}G}(M)$. Of course, there are also theoretical reasons why one should be interested in $\mathrm{End}_{\mathbb{Q}G}(M)$ as an algebra with involution. For instance, the Brauer–Speiser Theorem, which says that a Schur index of an irreducible representation can be at most two if $Z(\mathrm{End}_{\mathbb{Q}G}(M))$ is a real number field, is due to the fact that an algebra with involution fixing the centre is split or a matrix ring over a quaternion algebra. Here is one more reason why antisymmetric bilinear forms might be relevant.

Lemma 5.3. Assume that the character χ of M contains a $\mathbb{C}$-irreducible real-valued character ψ with odd multiplicity $m > 1$. Then $\mathrm{Bil}_{\mathbb{Q}G}(M)$ contains nonzero antisymmetric forms and each such form is degenerate.

Proof. Tensoring with $\mathbb{R}$ and splitting into homogeneous components reduces the problem to $\mathbb{R}G$-modules of the form $\bigoplus_{i=1}^{m} M_0$, where M_0 is an irreducible $\mathbb{R}G$-module with character ψ. By Schur's lemma M_0 allows up to scalar multiples only one G-invariant bilinear form Φ_0. Moreover Φ_0 is symmetric and can be chosen to be positive definite. By choosing an Φ_0-orthonormal basis of M_0, one obtains a matrix representation Δ_0 for G on M_0 and a representation $\dotplus_{i=1}^{m} \Delta_0$ on $\bigoplus_{i=1}^{m} M_0$. The antisymmetric G-invariant bilinear forms on $\bigoplus_{i=1}^{m} M_0$ have Gram matrices $A \otimes I_n$, where $A \in \mathbb{R}^{m\times m}$ is antisymmetric and I_n is the $n \times n$-unit matrix. Since m is odd, $\det A = 0$ and the result follows. □

Note that, if M in Lemma 5.3 is homogeneous, so are $\mathrm{Rad}(\Phi)$ and $M/\mathrm{Rad}(\Phi)$. Either one of these is a simple $\mathbb{Q}G$-module, or the hypothesis of Lemma 5.3 applies again to one of them.

Finally we mention that real Schur indices of real valued $\mathbb{C}$-irreducible characters can be determined by the distribution of invariant bilinear forms into symmetric and antisymmetric ones.

5(iv). $\mathrm{Hom}_{\mathbb{Q}G}(M, M')$

This becomes relevant when $\dim_{\mathbb{Q}} M$ is so big that one hesitates to compute $\mathrm{End}_{\mathbb{Q}G}(M)$, and some irreducible $\mathbb{Q}G$-modules M' are already known. In this case one can compute a nonzero element

$$\varphi \in \operatorname{Hom}_{\mathbb{Q}G}(M, M')$$

and continue with the kernel of φ as new M (of course, one will always work with lattices).

There are more situations where the possibility of computing $\operatorname{Hom}_{\mathbb{Q}G}(M, M')$ might be relevant. We mention only one:

Remark 5.4. Assume M and M' are isomorphic to multiples $\bigoplus^{m_1} M_0$ and $\bigoplus^{m_2} M_0$ of a simple $\mathbb{Q}G$-module M_0. Then one can construct a $\mathbb{Q}G$-module $M'' \cong \bigoplus^{m_3} M_0$ where $m_3 = \gcd(m_1, m_2)$.

6. SOME REMARKS ON HOMOGENEOUS MODULES

The essential problem that might be left is to extract the irreducible constituent from a homogeneous $\mathbb{Q}G$-module M. Hence $\mathcal{E} := \operatorname{End}_{\mathbb{Q}G}(M)$ is a simple $\mathbb{Q}$-algebra, and one has two problems:

(i) Decide whether $\mathcal{E}$ is a division algebra.
(ii) If not, find a singular element in $\mathcal{E}$.

Obviously, (i) can in principle be decided by using p-adic methods, which we do not want to go into here. However, there does not seem to be a feasible procedure for (ii). Here, we just give a few easy solutions for (i) and (ii) in the most frequently occurring situations.

Clearly $\mathcal{E} \cong D^{n\times n}$ for some $\mathbb{Q}$-division algebra D and $n \in \mathbb{N}$. Let $Z := Z(\mathcal{E}) = Z(D)$, $k := \dim_{\mathbb{Q}} Z$ and $\dim_Z D = s^2$. Hence $\dim_{\mathbb{Q}} \mathcal{E} = k(ns)^2$.

Task (i) means determining n, or equivalently the Schur index s. We treat the cases $ns \le 3$ and assume that Z is known and $\mathcal{E}$ is given, for example, in its regular representation over Z, which will be of degree $(ns)^2$. We note that there are efficient procedures available to solve relative norm equations in algebraic number fields [Pohst 1989; Fieker et al. 1996].

Lemma 6.1. Assume $ns = 2$. Then problem (i) can be reduced to deciding whether a certain norm equation for some quadratic extension of Z can be solved, and problem (ii) to finding a solution if there is one.

Proof. Pick $x \in \mathcal{E} - Z$ of regular trace 0. Let $t^2 - d \in Z[t]$ be the minimal polynomial of x. If $t^2 - d$ splits over Z, we are done. If not, find $y \in \mathcal{E}$ with $y \ne 0$ and $yx = -xy$, so that y induces the nontrivial Galois automorphism of $Z[x] \cong Z[\sqrt{d}]$. Then $\mathcal{E} \cong Z^{2\times 2}$ if and only if there exists $r \in Z[x]$ with $N_{Z[x]/Z}(r) = y^{-2}$, i.e., if $\mathcal{E}$ is a split crossed product of $Z[x]$ by $C_2 = \operatorname{Gal}(Z[x]/Z)$. If r exists then $(ry)^2 = 1$, hence $ry - 1$ is nonzero singular. □

It should be remarked that there are other possibilities to deal with the case $ns = 2$, namely to find or prove nonexistence of an $u \in \mathcal{E}$ with $\operatorname{trace}(u) = 0$ and $\operatorname{trace}(u^2) = 0$, which amounts to finding a trace zero element representing 0 in the trace bilinear form. For $Z = \mathbb{Q}$ constructive procedures of finding isotropic vectors for ternary quadratic forms are known [Mordell 1969]. However, the crossed product approach of Lemma 6.1 still works for $ns = 3$, although less efficiently. But the case $ns = 3$ is only relevant in case Z is not a real number field because of the Brauer–Speiser theorem.

Lemma 6.2. Assume $ns = 3$. Then problem (i) reduces to deciding whether a certain norm equation $N_{L/K}(x) = b$ is solvable with $K = Z$ or a certain quadratic extension of Z, $b \in K$, and L/K a certain cubic cyclic extension of K. If it is solvable, (ii) reduces to finding a solution.

Proof. Choose $a \in \mathcal{E} - Z$. If the minimum polynomial $p(t) \in Z[t]$ of a over Z is reducible we are done. Assume it is irreducible and define $L_0 = Z[a] \cong Z[t]/(p(t))$. Then L_0 is a cubic extension of Z contained in $\mathcal{E}$. If (L_0/Z) is a Galois extension, let $L := L_0$; otherwise let L be the normal closure of L_0. In the second case $\operatorname{Gal}(L/Z) \cong S_3$. Set $K = Z$ in the first case; in the second, define K as the subfield of L fixed by an element σ of order three in $\operatorname{Gal}(L_0/Z)$. Since $[K : Z]$ is relatively prime to $ns = 3$, $\mathcal{E}$ splits over Z if and only if $K \otimes_Z \mathcal{E}$ splits over K. Identify $a \in \mathcal{E}$ with $1 \otimes a$.

Represent $K \otimes_Z \mathcal{E}$ as a crossed product of $K[a]$ by $\mathrm{Gal}(L/K) \cong C_3$ by solving $ya = a^\sigma y$ for $y \in K \otimes \mathcal{E}$. Let $b := y^{-3}$. Then b commutes with a and lies in $K[a] = L$. The crossed product $K \otimes_Z \mathcal{E}$ splits if and only if the norm equation $N_{L/K}(x) = b(= y^{-3})$ is solvable. If x is a solution, then $(xy)^3 = 1$. Clearly

$$V := \{v \in K \otimes_z \mathcal{E} : (xy - 1)v = 0\}$$

is an irreducible $K \otimes_Z \mathcal{E}$-module (note that $K \otimes_Z \mathcal{E} \cong K^{3\times 3}$ in this stage). Restricting the action of $K \otimes_Z \mathcal{E}$ to $\mathcal{E}$ on V turns V into a reducible $\mathcal{E}$-module of composition length 2. The composition length of the regular $\mathcal{E}$-module is 3 since $\mathcal{E} \cong Z^{3\times 3}$. Hence one can construct an irreducible $\mathcal{E}$-module, i.e. an isomorphism $\mathcal{E} \to Z^{3\times 3}$ (see also Remark 5.4). This clearly exhibits a singular element of $\mathcal{E}$. □

7. AN EXAMPLE

From [Conway et al. 1985], for example, we get this list of irreducible rational characters for $G = \mathrm{Sp}_4(3)$:

1 (trivial),
$5ab, 6, 10ab, 15, 15', 20, 24, 30, 30ab, 40ab, 45ab,$
$60, 64, 81$ (factoring over $\mathrm{SU}_4(2)$),
$4ab, 20', 20ab, 20'ab, 36ab, 60', 60ab, 64', 80$ (faithful).

(The notation is based on the characters' degrees and their splitting into complex irreducible characters.) From [Holt and Plesken 1989, p. 338], for example, we are given the rational representation with character $4ab$, and want to construct all the faithful irreducible rational representations.

Step 1: We carry out some character calculations in GAP [Schönert et al. 1994] to find a good order for the construction of the irreducible representations. Each time we find a new character needed later on, we underline it. Each time we get a faithful character we are looking for, we underline it twice.

$$4ab \cdot 4ab = 2 \cdot 1 + 2 \cdot \underline{6} + 2 \cdot \underline{15} + \underline{10ab}$$
$$10ab \cdot 4ab = 4ab + \underline{\underline{36ab}} + \underline{\underline{20ab}} + \underline{\underline{20'ab}}$$
$$6 \cdot 6 = 1 + 15 + \underline{20}$$
$$20 \cdot 4ab = 20'ab + 2 \cdot \underline{\underline{60'}}$$
$$6 \cdot 20 = 6 + 20 + \underline{30} + 64$$
$$6 \cdot 30 = \underline{15'} + 20 + 64 + 81$$
$$15' \cdot 4ab = \underline{\underline{60ab}}$$
$$6 \cdot 20ab = 2 \cdot \underline{\underline{20'}} + 36ab + 2 \cdot \underline{\underline{64'}}$$
$$6 \cdot 20' = 20ab + \underline{\underline{80}}$$

Step 2 (choosing a suitable $e \in \mathbb{R}G^{\mathrm{gen}}_{1,\geq 0}$): We first compute $\mathrm{End}_{\mathbb{Q}G}(M)$ where M has character $4ab$ [Holt and Plesken 1989, p. 338]. For each generating set $\{x, y\}$ that we tested for rate of convergence, three tests were performed:

$$e = \tfrac{1}{3}(1 + x + y), \tag{7.1}$$

$$e = \tfrac{1}{2}(1 + x)\tfrac{1}{2}(1 + y), \tag{7.2}$$

$$e = \frac{(1 + x + \cdots + x^{|x|-1})(1 + y + \cdots + y^{|y|-1})}{|x|\,|y|} \tag{7.3}$$

They require 2, 2, and $|x| + |y| - 2$ conjugations in each step, respectively. Analogously, we tried generating sets $\{x, y, z\}$ with three generators. See Tables 1 and 2.

So $e = \frac{1}{2}(1 + ab)\frac{1}{2}(1 + ab^3ab)\frac{1}{2}(1 + (abab^3ab)^2)$ is the element we work with.

Step 3 (Computing the representations): $4ab \cdot 4ab$ yields the modules with characters $2 \cdot 6$, $2 \cdot 15$, $10ab$ which one gets by computing $\rho(a) \in Z(\mathrm{End}_{\mathbb{Q}G}(4ab \cdot 4ab))$ in one go. To split up $2 \cdot 6$ and $2 \cdot 15$ one has to compute $\mathrm{End}_{\mathbb{Q}G}$ for these two modules, which are easily recognised as $\mathbb{Q}^{2\times 2}$. For $10ab \cdot 4ab$ one computes $\rho(a) \in Z(\mathrm{End}_{\mathbb{Q}G}(10ab \cdot 4ab))$ and gets the desired splitting as indicated in step 1. One proceeds in the order suggested in step 1. For example, $20 \cdot 4ab$ yields (via $\rho((ab)^3)$) the module $2 \cdot 60'$, whose endomorphism ring is a positive definite rational quaternion algebra. Similarly $20'$ and $64'$ can not be realised over $\mathbb{Q}$ but only $2 \cdot 20'$ and

			(7.1)		(7.2)		(7.3)	
x	y	z	#conj	λ^{-1}	#conj	λ^{-1}	#conj	λ^{-1}
a	b	–	$300 \cdot 2$	1.036	$150 \cdot 2$	1.075	$90 \cdot 6$	1.129
$(ab)^3$	ab^3ab	–	$470 \cdot 2$	1.024	$180 \cdot 2$	1.067	$150 \cdot 6$	1.079
ab	ab^3ab	–	$60 \cdot 2$	1.229	$50 \cdot 2$	1.316	$10 \cdot 12$	3.158
ab	ba	–	$110 \cdot 2$	1.103	$100 \cdot 2$	1.111	$20 \cdot 16$	1.939
ab^3ab	b^2abab	–	$190 \cdot 2$	1.062	$130 \cdot 2$	1.094	$80 \cdot 8$	1.316
ab	ab^3ab	$(abab^3ab)^2$	$50 \cdot 3$	1.279	$50 \cdot 3$	1.278	$10 \cdot 14$	3.871

TABLE 1. Experiments with generators acting on the module M with character $4ab$. The first three columns express x, y, z in terms of the generators a, b given in [Holt and Plesken 1989]. (Note that a^2 is central, $|b| = 4$, $|ab| = 9$, $|ab^3ab| = 5$, $|(ab)(ab^3ab)| = 6$.) The remaining columns refer to the choices of e given in (7.1)–(7.3), and they show the number of conjugations needed (number of steps times conjugations per step) and λ^{-1}, where λ is as in the end of Section 3.

			(7.1)			(7.2)			(7.3)		
x	y	z	#conj	λ^{-1}	time	#conj	λ^{-1}	time	#conj	λ^{-1}	time
ab	ab^3ab	–	$260 \cdot 2$	1.062	99.5 s	$170 \cdot 2$	1.099	65.7 s	$60 \cdot 12$	1.304	133.2 s
ab	ab^3ab	$(abab^3ab)^2$	$170 \cdot 3$	1.099	97.4 s	$70 \cdot 3$	1.267	41.9 s	$40 \cdot 14$	1.600	104.5 s

TABLE 2. For the two best generating sets of Table 1, we tested the performance on the 64-dimensional module $M \otimes M$. We show the time needed to compute one endomorphism, on an HP9000/730.

$2 \cdot 64'$. These two modules are obtained from splitting the 240-dimensional module $6 \cdot 20ab$, where it takes about 70 minutes to compute one endomorphism. The irreducibility of $2 \cdot 20'$ of course means that the representation in the last row ($6 \cdot 20' = \cdots$) has to be replaced by $6 \cdot (2 \cdot 20')$ which is of degree 240 rather than 120. Also $2 \cdot 80$ belongs to an irreducible $\mathbb{Q}G$-module.

If the reader tries to continue the exercise to find also the irreducible non-faithful representations of $\mathrm{Sp}_4(3)$, i.e., the ones factoring over $U_4(2)$, he will find that $5ab$ is the most difficult one to get, for instance via the symmetrised tensor square $10ab^{[2]} = 1 + 5ab + 15 + 2 \cdot 20 + 24 + 30ab + 60$, which means to decompose a module of dimension 210, and it takes about 40 minutes to find one endomorphism. Here of course (as well as in some of the cases above) one can profit from the fact that homomorphisms rather than endomorphisms can be computed as well.

Remark. As an afterthought, one might ask what sort of information one might want to store about the representations constructed. At first glance, one will think of the generators a, b, possibly the invariant scalar product and generators for the endomorphism ring. But sometimes it might be more advantageous to store the way the representations were constructed, i.e., the matrices of the kernels of the various module homomorphisms etc., in such a way that one is able to first compute a (long) word $w(a, b)$ in a and b in the first representation (here of degree 8) and then go quickly through the various constructions of intermediate representations for $w(a, b)$ to get $\Delta(w(a, b))$ for the desired representation Δ. If $w(a, b)$ is a long word and Δ of big degree, this might be considerable cheaper than computing $w(\Delta(a), \Delta(b))$ naively.

REFERENCES

[Conway et al. 1985] J. H. Conway, R. T. Curtis, S. P. Norton, R. A. Parker and R. A. Wilson, *Atlas of Finite Groups: Maximal Subgroups and Ordinary Characters for Simple Groups*, Oxford University Press, Oxford, 1985.

[Dixon 1970] J. D. Dixon, "Computing irreducible representations of groups", Math. Comp., **24** (1970), 707–712.

[Dixon 1993] J. D. Dixon, "Constructing representations of finite groups", pp. 105–112 in *Groups and computation*, New Brunswick, NJ, 1991 (edited by L. Finkelstein and W. M. Kantor), DIMACS Series in Discrete Mathematics and Theoretical Computer Science **11**, Amer. Math. Soc., Providence, RI, 1993.

[Fieker et al. 1996] C. Fieker, A. Jurk and M. Pohst, "On solving relative norm equations in algebraic number fields", to appear in *Math. Comp.*

[Holt and Plesken 1989] D. F. Holt and W. Plesken, *Perfect Groups*, Oxford University Press, Oxford, 1989

[Holt and Rees 1994] D. F. Holt and S. Rees, "Testing modules for irreducibility", *J. Australian Math. Soc.* (Series A) **57** (1994), 1–16.

[Huppert 1990] B. Huppert, *Angewandte Lineare Algebra*, de Gruyter, Berlin, 1990.

[Mordell 1969] L. J. Mordell, *Diophantine Equations*, Academic Press, London 1969,

[Parker 1984] R. A. Parker, "The computer calculation of modular characters (The 'Meat-axe')", pp. 267–274 in *Computational Group Theory: Proceedings of the London Mathematical Society Symposium* (edited by M. D. Atkinson), Academic Press, London, 1984.

[Pohst 1993] M. Pohst, *Computational Algebraic Number Theory*, DMV Seminar **21**, Birkhäuser, Basel, 1993.

[Pohst and Zassenhaus 1989] M. Pohst and H. Zassenhaus, *Algorithmic Algebraic Number Theory*, Cambridge University Press, Cambridge, 1989.

[Schlosser 1978] H. Schlosser, "Zur Berechnung von 'Strong Intertwining Operators' unitärer Darstellungen von Gruppen und einige Anwendungen", *Math. Nachr.* **85** (1978), 37–45.

[Schönert et al. 1994] M. Schönert et al., *GAP: Groups, Algorithms, and Programming*, Lehrstuhl D für Mathematik, RWTH Aachen, Germany, 1994. Available by anonymous ftp, together with the GAP system, on the servers ftp.mth.pdx.edu, archives. math.utk.edu, or math.rwth-aachen.de.

[Seysen 1993] M. Seysen, "Simultaneous reduction of a lattice basis and its reciprocal basis", *Combinatorica* **13** (1993), 363–376.

[Thompson 1981] J. G. Thompson, "Rational functions associated to presentations of finite groups", *J. Algebra* **71** (1981), 481–489.

Wilhelm Plesken, Lehrstuhl B für Mathematik, RWTH Aachen, Templergraben 64, 52062 Aachen, Germany (plesken@willi.math.rwth-aachen.de)

Bernd Souvignier, Lehrstuhl B für Mathematik, RWTH Aachen, Templergraben 64, 52062 Aachen, Germany (bs@willi.math.rwth-aachen.de)

Received Received June 19, 1995; accepted in revised form November 28, 1995