Group Determinants and k-Characters

Andy Hammerlindl

December 12, 2005

1 Representations as Modules

In class, we viewed representations as homomorphisms $G \to GL(V)$, but there is another way to regard representations, namely as modules over the group algebra. If G is a finite group, let $\mathbb{C}G$ be the $\mathbb{C}$-vector space with the elements of G as a basis, and the extend the multiplication defined by the group on the basis elements, ie.

$$\sum_{g \in G} a_g g + \sum_{g \in G} b_g g = \sum_{g \in G} (a_g + b_g) g \quad (a_g, b_g \in \mathbb{C}),$$

$$\left(\sum_{g \in G} a_g g \right) \left(\sum_{g' \in G} b'_g g' \right) = \sum_{h \in G} \left(\sum_{gg'=h} a_g b'_g \right) h.$$

It is straightforward to verify that this is a $\mathbb{C}$-algebra, and if G is not abelian, it is a non-commutative algebra. If $e \in G$ is the group identity, it follows that e, when regarded as an element of $\mathbb{C}G$, is the multiplicative identity for the ring. It is common to regard $\mathbb{C}$ as being a subalgebra of $\mathbb{C}G$ via the embedding $z \mapsto ze$.

If $\pi : G \to GL(V)$ is a representation, we can make V into a left $\mathbb{C}G$-module by defining the action of the ring for basis elements:

$$g \cdot v = \pi(g)(v) \quad (g \in G, v \in V)$$

and extending by linearity, ie.

$$\left(\sum_{g \in G} a_g g \right) \cdot v = \sum_{g \in G} a_g \pi(g)(v).$$

Conversely, if M is a $\mathbb{C}G$-module, then as $\mathbb{C}$ is a subalgebra of $\mathbb{C}G$, M is a $\mathbb{C}$-vector space, and we can define a homomorphism

$$\begin{aligned} \pi : G &\rightarrow GL(M) \\ g &\mapsto (m \mapsto g \cdot m) \end{aligned}$$

where $GL(M)$ is the set of $\mathbb{C}$-linear vector space isomorphisms of M and $g \cdot v$ is the action of $\mathbb{C}G$ on the module M.

These two functors between homomorphisms and modules are inverses, and show that the two forms of representations are equivalent. Under this duality, one can see that a subrepresentation corresponds to a submodule, and a subquotient of a representation corresponds to a quotient of a module. Also, two representations are equivalent if and only if their modules are isomorphic.

For a module M over a ring R, we say M is *reducible* if it has a proper submodule, *irreducible* if it does not, and *completely reducible* if it is isomorphic (as an R-module) to a direct sum of irreducible R-modules. In the specific case $R = \mathbb{C}G$, these correspond to the properties of the same name for representations.

Any ring is a module over itself, so $\mathbb{C}G$ is a left $\mathbb{C}G$-module. As a vector space, it has the elements of G as a basis, and G acts on it by

$$h \cdot \sum_{g \in G} a_g g = \sum_{g \in G} a_g (hg) = \sum_{g \in G} a_{h^{-1}g} g$$

which is the left regular representation of G.

A central theorem in the study of modules is one of Wedderburn.

Wedderburn's Theorem. *Let R be a nonzero ring with 1 (not neccessarily commutative). Then the following are equivalent:*

1. *every R-module is projective*
2. *every R-module is injective*
3. *every R-module is completely reducible*
4. *the ring R considered as a left R-module is a direct sum:*

$$R = L_1 \oplus L_2 \oplus \cdots \oplus L_n,$$

where each L_i is an irreducible module (ie. a simple left ideal) with $L_i = Re_i$, for some $e_i \in R$ with *(a)* $e_ie_j = 0$ *if* $i \neq j$

(b) $e_i^2 = e_i$ *for all* i

(c) $\sum_{i=1}^{n} e_i = 1$

5. *as rings,* R *is isomorphic to a direct product of matrix rings over division rings, ie.* $R = R_1 \times R_2 \times \cdots \times R_r$ *where* R_j *is a two-sided ideal of* R *and* R_j *is isomorphic to the ring of all* $n_j \times n_j$ *matrices with entries in a division ring* Δ_j*,* $j = 1, 2, \ldots, r$*. The integer* r*, the integers* n_j*, and the division rings* Δ_j *(up to isomorphism) are uniquely determined by* R*.*

A ring which satisfies any (and therefore all) of the above conditions is called *semisimple.*

Dummit and Foote state the theorem and give a set of exercises that lead the reader through the proof.[2] The steps are easy to follow and I recommend it as an enjoyable recreation on a lazy Sunday afternoon (especially if you like using Zorn's Lemma).

When our ring is the group algebra $\mathbb{C}G$, 1. is equivalent to saying every subquotient of a representation is a subrepresentation and 2. is equivalent to saying every subrepresentation of a representation is a subquotient. In class, we proved these facts for finite-dimensional representations of finite groups. Fortunately, the proof generalizes for vector spaces of any size, so the group algebra is semisimple. 3. is equivalent to saying every representation is completely reducible. 4. and 5. characterize the reduction of the left regular representation into irreducible components.

Regarding $\mathbb{C}G \cong R_1 \times \cdots \times R_r$ as in 5. where $R_j = M_{n_j}(\Delta_j)$, the action of $\mathbb{C}G$ on R_j depends only on its R_j component. As such, it is useful to view an element of $R_1 \times \cdots \times R_r$ as a block matrix of the form

$$\begin{pmatrix} A_1 & & & \\ & A_2 & & \\ & & \ddots & \\ & & & A_r \end{pmatrix}.$$

Then we can think of $R_j = M_{n_j}(\Delta_j)$ as acting on itself by matrix multiplication on the left. This multiplication acts on each column of a matrix separately, so R_j decomposes into n_j submodules, each a column vector of n_j entries in Δ_j. Label any one of these isomorphic submodules as L_j. Basic matrix arithmetic shows that these submodules are irreducible and so each of them must correspond to an irreducible representation of G, say π_j. It must be the case that $L_j \cong \mathbb{C}^{n_j}$ and $R_j \cong M_{n_j}(\mathbb{C})$. Then the isomorphism

$$\mathbb{C}G \to M_{n_1}(\mathbb{C}) \times \cdots \times M_{n_r}(\mathbb{C})$$

maps G to $\pi_1(g) \times \cdots \times \pi_r(g)$ where $\pi_j : G \to GL_{n_j}(\mathbb{C})$, $1 \leq j \leq r$, are the distinct irreducible representations of G.

It is possible to develop this isomorphism without knowing *a priori* the decomposition of the left regular representation; see [2] for details. This isomorphism is a useful tool for understanding the group.

2 The Group Determinant

We now take a somewhat historical look at the development of characters and the group determinant. A more in-depth history is given in [4].

For most of the nineteenth century, characters were defined only for abelian groups as homomorphisms $G \to \mathbb{C}$. Any finite abelian group can be described as a direct product of cyclic groups, say

$$G = \langle g_1 \rangle \times \langle g_2 \rangle \times \cdots \times \langle g_n \rangle$$

where $|g_k| = r_k$. Then the characters of G are exactly the homomorphisms of the form

$$g_1^{l_1} g_2^{l_2} \cdots g_r^{l_r} \mapsto \zeta_1^{l_1} \zeta_2^{l_2} \cdots \zeta_r^{l_r}$$

where $\zeta_k \in \mathbb{C}$ is an r-th root of unity. These characters have nice properties, such as the orthogonality relations, and they determine the abelian group.

In 1896, to try to understand non-abelian groups in a similar way, Dedekind and Frobenius looked at the group determinant. For a finite group G, let $\{x_g : g \in G\}$ be a set of independent variables. Define the group matrix X_G as the matrix with rows and columns indexed by the elements of G and such that the (g, h) cell is $x_{gh^{-1}}$. The group determinant $\mathfrak{D}_G$ is then $\det X_G$. This is well defined, even including the sign, so long as the rows and columns of X_G have the same ordering.

Once might justifiably ask why not use x_{gh} instead of $x_{gh^{-1}}$. This idea was also persued but wasn't nearly as useful. One advantage of our definition is that if variables y_g and z_g are defined similarly to x_g and given the relation

$$z_c = \sum_{ab=c} x_a y_b,$$

then $Z_G = X_G Y_G$ and therefore $\det Z_G = \det X_G \det Y_G$. Frobenius used this equation, along with lengthy calculations to prove many of his results.

The definition also makes intuitive sense in light of modern algebra. Any endomorphism $V \to V$ of a finite dimensional vector space can be ascribed a determinant simply by choosing a basis for V. This is well-defined as changes-of-basis do not affect the determinant. This notion extends to endomorphisms of finite dimensional algebras.

Let $\mathbb{C}(x_g) = \mathbb{C}(x_g : g \in G)$ be the field of rational functions in the variables x_g. Define a group algebra $\mathbb{C}(x_g)G$ similarly to $\mathbb{C}G$, and let $\mathfrak{X}_G = \sum x_g g \in \mathbb{C}(x_g)G$. Left multiplication by $\mathfrak{X}_G$ determines an endomorphism on $\mathbb{C}(x_g)G$ and its determinant is $\mathfrak{D}_G$. If you write this endomorphism as a matrix, using G as a basis, it is simply X_G, the group matrix.

The $\mathbb{C}$-algebra isomorphism

$$\pi = (\pi_1, \ldots, \pi_r) : \mathbb{C}G \to M_{n_1}(\mathbb{C}) \times \cdots \times M_{n_r}(\mathbb{C})$$

extends to a $\mathbb{C}(x_g)$-algebra isomorphism

$$\mathbb{C}(x_g)G \to M_{n_1}(\mathbb{C}(x_g)) \times \cdots \times M_{n_r}(\mathbb{C}(x_g))$$

which we will still denote by $\pi = (\pi_1, \ldots, \pi_r)$.

The left multiplication by $\mathfrak{X}_G$ corresponds to multiplying by $\pi_j(\mathfrak{X}_G)$ in each copy of the representation. Since there are n_j copies of each representation π_j, this means that

$$\mathfrak{D}_G = \det\left(\pi_1(\mathfrak{X}_G)\right)^{n_1} \cdots \det\left(\pi_r(\mathfrak{X}_G)\right)^{n_r}. \quad (1)$$

For a matrix representation ρ, $\det\left(\rho(\mathfrak{X}_G)\right)$ is irreducible if and only if ρ is irreducible. The proof of this involves k-characters, which will be introduced later. In particular, this implies that (1) is a complete factorization of $\mathfrak{D}_G$. Each factor is a homogenous polynomial with the same degree as its corresponding representation.

If π_j is a one-degree representation, we can identify it with its character χ_j. Then,

$$\det\left(\pi_j(\mathfrak{X}_G)\right) = \chi_j(\mathfrak{X}_G) = \sum_{g \in G} \chi_j(g) x_g.$$

If G is abelian, all of its irreducible representations are one-degree, so $\mathfrak{D}_G$is just the product of irreducible factors of the form $\sum \chi_j(g) x_g$ for each character χ_j. This was an encouraging discovery in the initial study of the group determinant.

If G is not abelian, $\mathfrak{D}_G$ still has these linear factors for one-degree representations. These representations correspond to the representations of the abelianization G/G' where G' is the commutator subgroup of G. Dedekind noticed this correspondence and tried to extend the field $\mathbb{C}$ so that $\mathfrak{D}_G$ would factor into linear polynomials, but was not overly successful.

Frobenius, instead, looked at coefficients of the irreducible factors over $\mathbb{C}$. With knowledge of representations, we can get a handle on what these coefficients are. For an $n \times n$ matrix A, the determinant is defined as

$$\sum_{\sigma \in S_n} \operatorname{sgn}(\sigma) \prod_{i=1}^{n} A_{i\sigma(i)}.$$

Say π is an irreducible representation of G of degree n. Then the corresponding factor of $\mathfrak{D}_G$ is

$$\begin{aligned}
\Phi &= \det \pi(\mathfrak{X}_G) \\
&= \det \left(\sum_{g \in G} \pi(g) x_g \right) \\
&= \sum_{\sigma \in S_n} \operatorname{sgn}(\sigma) \prod_{i=1}^{n} \sum_{g \in G} (\pi(g))_{i\sigma(i)}\, x_g.
\end{aligned}$$

By the standard distributive law, exchange the inside product and sum to yield

$$\begin{aligned}
\Phi &= \sum_{\sigma \in S_n} \operatorname{sgn}(\sigma) \sum_{(g_1,\ldots,g_n) \in G^n} \left(\prod_{i=1}^{n} (\pi(g_i))_{i\sigma(i)} \right) x_{g_1} \cdots x_{g_n} \\
&= \sum_{(g_1,\ldots,g_n) \in G^n} \left(\sum_{\sigma \in S_n} \operatorname{sgn}(\sigma) \prod_{i=1}^{n} (\pi(g_i))_{i\sigma(i)} \right) x_{g_1} \cdots x_{g_n} \qquad (2)
\end{aligned}$$

Certain observations motiviated Frobenius to look at the coefficients of the terms $x_g x_e^{n-1}$ of Φ, where e is the group identity and $g \neq e$.

Suppose $g_j = g$ and $g_i = e$ for $i \neq j$. Then

$$\begin{aligned}
&\sum_{\sigma \in S_n} \operatorname{sgn}(\sigma) \prod_{i=1}^{n} (\pi(g_i))_{i\sigma(i)} \\
=&\sum_{\sigma \in S_n} \operatorname{sgn}(\sigma) (\pi(g))_{j\sigma(j)} \prod_{i \neq j} (\pi(e))_{i\sigma(i)} \\
=&\sum_{\sigma \in S_n} \operatorname{sgn}(\sigma) (\pi(g))_{j\sigma(j)} \prod_{i \neq j} \delta_{i\sigma(i)} \\
=&(\pi(g))_{jj}
\end{aligned}$$

as $\sigma = id$ is the only permutation that will not be zero for some $\delta_{i\sigma(i)}$. Coefficients of $x_g x_e^{n-1}$ in (2) will come from tuples of the above form, where j ranges from 1 to n, so the coefficient of $x_g x_e^{n-1}$ in Φ is

$$\sum_{j=1}^{n} (\pi(g))_{jj} = \operatorname{tr}(\pi(g)).$$

For an irreducible factor Φ of degree n of the group determinant, Frobenius defined the corresponding group character by setting $\chi(e) = n$ and $\chi(g)$ equal to the coefficient of $x_e x_g^{n-1}$ in Φ. In such a way, character theory was first developed for non-abelian groups without any notion of the underlying matrix representations.

Frobenius was able to prove the orthogonality relations for characters, show that they were class functions, and prove several other fundamental properties. Reasoning that $\chi : G \to \mathbb{C}$ corresponded to coefficients of Φ where all but one the variables were x_e, he defined a k-character $\chi^{(k)} : G^k \to \mathbb{C}$ that, roughly speaking, corresponds to coefficients of Φ where all but k of the vars are x_e.

These k-characters can be recursively defined by

$$\chi^{(1)}(g) = \chi(g),$$

$$\begin{aligned}
\chi^{(1)}(g_0, g_1, \ldots, g_n) =& \chi(g_0)\chi^{(k)}(g_1, \ldots, g_n) \\
&- \chi^{(k)}(g_0 g_1, \ldots, g_n) - \cdots - \chi^{(k)}(g_1, \ldots, g_0 g_n)
\end{aligned}$$

The polynomial Φ is completely determined by its k-characters and vice versa; explicitly

$$\Phi = \frac{1}{n!} \sum_{(g_1, \ldots, g_n) \in G^n} \chi^{(n)}(g_1, \ldots, g_n)\; x_{g_1} \cdots x_{g_n}.$$

Frobenius proved orthogonality relations and other small results for k-characters but, as was inevitable, several months after developing characters, he realized there were representations lying underneath. Focus turned to these objects, and the study of k-characters and group determinants was abandoned for nearly a century.

3 Determining the Group

In 1986, Johnson studied latin square determinants and revisited group determinants.[6] He established necessary conditions for two groups to have identical determinants and posed the question of whether the determinant uniquely determines the group.

The characters (ie. the 1-characters) do not determine a group uniquely, even for orders as low as eight. The k-characters encode the information of the character, but also encode some information about the group multiplication. For instance, note the $\chi(gh)$ term in

$$\chi^{(2)}(g,h) = \chi(gh) - \chi(g)\chi(h).$$

The group determinant carries the same information as all of the k-characters of all irreducible representations, but it was believed that this was only a small improvement on the 1-characters. It was somewhat of a surprise, then, when Formanek and Sibley showed that the group determinant does indeed determine the group.[3] Their proof is based on maps between group algebras.

Shortly after, Mansfield independently published a proof using only basic group theory and combinatorics.[8] He shows that if $x_{g_1} \cdots x_{g_n}$ has a non-zero coefficient in $\mathfrak{D}_G$ then $g_1, \ldots, g_n$ can be reordered so that $g_1 \cdots g_n = e$, the identity. By looking at terms of the form $x_e^{n-2} x_a x_b$ and $x_e^{n-3} x_a x_b x_c$, one can then reconstruct the group multiplication. The proof is short, easy to follow, and well worth reading. However, it does not shed much light on the structure of the group determinant or its relation to the representations of the group. As such, we will follow the proof given by Formanek and Sibley.

The proof at its core, uses a theorem of linear algebra proven by Dieudonne.[1]

Theorem 1. *Let K be a field (in our case $\mathbb{C}$) and $\theta : M_n(K) \to M_n(K)$ an isomorphism of vector spaces, such that*

$$\det(\theta(X)) = 0 \quad \textit{if and only if} \quad \det X = 0.$$

Then either $\theta(X) = AXB$ for all $X \in M_n(K)$ or $\theta(X) = AX^tB$ for all $X \in M_n(K)$ where A, B are fixed invertible matrices.

For a ring R, let $\mathcal{U}(R)$ be the units of R. Then the result we need can be succinctly stated.

Corollary 2. *Let $\theta : M_n(\mathbb{C}) \to M_n(\mathbb{C})$ be an isomorphism of vector spaces such that $\mathcal{U}(\theta(M_n(\mathbb{C}))) = \mathcal{U}(M_n(\mathbb{C}))$ and $\theta(1) = 1$. Then θ is either an isomorphism of algebras or an anti-isomorphism (ie. $\theta(XY) = \theta(Y)\theta(X)$).*

We now generalize this result to semisimple algebras.

Lemma 3. *Let $R = R_1 \times \cdots \times R_r$ be a ring where $R_j = M_{n_j}(\mathbb{C})$. Let W be a subspace of nonunits of R. Then, for some j, the projection of W to R_j consists entirely of nonunits; that is, $\det(w_j) \neq 0$ for every $w = (w_1, \ldots, w_r) \in W$.*

Proof. We prove the contrapositive. Assume each W_j has a unit and, using induction, construct a unit in W. For the base case, simply choose $w = (w_1, \ldots, w_r) \in W$ such that $\det(w_1) \neq 0$.

For the inductive case, assume that there is $w = (w_1, \ldots, w_r) \in W$ such that $\det(w_j) \neq 0$, $1 \leq j \leq k-1$. There is also $v = (v_1, \ldots, v_r) \in W$ such that $\det(v_k) \neq 0$. Consider $w + \alpha v$ for $\alpha \in \mathbb{C}$, $\alpha \neq 0$ yet to be determined. For $1 \leq j \leq k$,

$$\det(w_j + \alpha v_j) = 0 \quad \Leftrightarrow \quad \alpha^{-1} \text{ is an eigenvector of } -w_j^{-1}v_j,$$

and

$$\det(w_k + \alpha v_k) = 0 \quad \Leftrightarrow \quad \alpha \text{ is an eigenvector of } -w_k v_k^{-1}.$$

The set of eigenvectors of a matrix is finite, and here there are only a finite number of matrices involved, so there are a finite number of "bad" values for α. As $\mathbb{C}$ is infinite, by carefully choosing α, we can ensure $\det(w_j + \alpha v_j) \neq 0$ for all $1 \leq j \leq k$. By induction, there is $w = (w_1, \ldots, w_r) \in W$ such that $\det(w_j) \neq 0$ for $1 \leq j \leq r$, ie. w is a unit of R. □

Corollary 4. *If W is a subspace of R (as above) consisting of nonunits and is maximal with respect to that property then W is of the form*

$$R_1 \times \cdots \times R_{j-1} \times W_j \times R_{j+1} \times \cdots \times R_r$$

for some j and some maximal subspace W_j of nonunits in R_j.

Under the same conditions as Corollary 2, a map between two semisimple algebras may not be an isomorphism or anti-isomorphism, but at worst, it is a combination of the two.

Theorem 5. *Let $R = R_1 \times \ldots \times R_r$ and $S = S_1 \times \times \cdots \times S_s$ be semisimple algebras where $R_i = M_{n_i}(\mathbb{C})$ and $S_j = M_{m_j}(\mathbb{C})$. Suppose $\psi : R \to S$ is an isomorphism of vector spaces such that $\mathcal{U}(\psi(R)) = \mathcal{U}(S)$. Then $r = s$ and there is a permutation σ of the set $\{1, \ldots, r\}$ such that $\psi(R_i) = S_{\sigma(i)}$. Moreover, if $\psi(1) = 1$, each $\psi_i : R_i \to S_{\sigma(i)}$, $\psi_i = \psi|_{R_i}$ is either an isomorphism or an anti-isomorphism.*

Proof. Let $i \in \{1, \ldots, r\}$. $R_i = M_{n_i}(\mathbb{C})$ for some $n_i \in \mathbb{Z}$. Pick $\alpha \in \mathbb{C}^{n_i}$, $\alpha \neq 0$. Then $V_\alpha = \{r \in R_i : r\alpha = 0\}$ is a maximal subspace of nonunits in R_i and

$$V = R_1 \times \cdots \times R_{i-1} \times V_\alpha \times R_{i+1} \times \cdots \times R_r$$

is a maximal subspace of nonunits in R. The conditions on ψ ensure that $\psi(V) \subset S$ is also a maximal subspace of nonunits, so it is of the form

$$\psi(V) = S_1 \times \cdots \times S_{j(\alpha)-1} \times W_{j(\alpha)} \times S_{j(\alpha)+1} \times \cdots \times S_s$$

where $W_{j(\alpha)}$ is a subspace of the component $S_{j(\alpha)}$ and the index $j(\alpha)$ presumably depends on α.

Suppose $\beta \in \mathbb{C}^{n_i}$ yields a different index. That is

$$\psi(R_1 \times \cdots \times V_\beta \times \cdots \times R_r) = S_1 \times \cdots \times W_{j(\beta)} \times \cdots \times S_s$$

and $j(\beta) \neq j(\alpha)$. Then $V_{\alpha+\beta} \supset V_\alpha \cap V_\beta$ implies

$$\psi(R_1 \times \cdots \times V_{\alpha+\beta} \times \cdots \times R_r) \supset S_1 \times \cdots \times W_{j(\alpha)} \times \cdots \times W_{j(\beta)} \times \cdots \times S_s.$$

By Corollary 4, either

$$\psi(R_1 \times \cdots \times V_{\alpha+\beta} \times \cdots \times R_r) \supset S_1 \times \cdots \times W_{j(\alpha)} \times \cdots \times S_s.$$

in which case $V_{\alpha+\beta} = V_\alpha$, or

$$\psi(R_1 \times \cdots \times V_{\alpha+\beta} \times \cdots \times R_r) \supset S_1 \times \cdots \times W_{j(\beta)} \times \cdots \times S_s.$$

in which case $V_{\alpha+\beta} = V_\beta$. Either way, $V_{\alpha+\beta} = V_\alpha = V_\beta$ which contradicts $j(\beta) \neq j(\alpha)$. Hence, $j = j(\alpha) = j(\beta)$ depends only on the index i. Set $\sigma(i) = j$.

Using the fact $\bigcap\{V_\alpha : \alpha \in \mathbb{C}^{n_i}, \alpha \neq 0\} = 0$,

$$\psi(R_1 \times \cdots \times 0_i \times \cdots \times R_r) \supset S_1 \times \cdots \times 0_{\sigma(i)} \times \cdots \times S_s.$$

Similarly,

$$\psi^{-1}(S_1 \times \cdots \times 0_{\sigma(i)} \times \cdots \times S_s) \supset R_1 \times \cdots \times 0_{i'} \times \cdots \times R_r.$$

for some i'. Combining the two, it must be that $i = i'$ and

$$\psi(R_1 \times \cdots \times 0_i \times \cdots \times R_r) = S_1 \times \cdots \times 0_{\sigma(i)} \times \cdots \times S_s.$$

As $\sigma : \{1, \ldots, r\} \to \{1, \ldots, s\}$ is invertible, it is a permutation and $r = s$. By intersecting subspaces of R and S of the above form, one can show $\psi(R_i) = S_{\sigma(i)}$. The rest of the theorem follows from Dieudonne's theorem and its corollary. □

We will not deal with arbitrary maps between semisimple algebras, but with special maps between group algebras that yield information about the groups. In this specific case, the maps are more well-behaved.

Theorem 6. *Let G, H be finite groups and let $\psi : G \to H$ be a bijection of sets that induces a vector space isomorphism $\psi : \mathbb{C}G \to \mathbb{C}H$. Then the following are equivalent:*

1. *$\psi : G \to H$ is an isomorphism or an anti-isomorphism,*
2. *$\psi(\mathcal{U}(\mathbb{C}G)) = \mathcal{U}(\mathbb{C}H)$ and $\psi(1) = 1$.*

Proof. One direction is immediate. For the other, let

$$\pi = (\pi_1, ..., \pi_r) : \mathbb{C}G \to R = R_1 \times \cdots \times R_r$$

$$\rho = (\rho_1, ..., \rho_s) : \mathbb{C}H \to S = S_1 \times \cdots \times S_s$$

be the Wedderburn decompositions of the group algebras and define $\theta = \rho\psi\pi^{-1} : R \to S$. As π and ρ are algebra isomorphisms, θ is an isomorphism of vector spaces, $\theta(\mathcal{U}(\mathbb{C}G)) = \mathcal{U}(\mathbb{C}H)$, and $\theta(1) = 1$.

Applying Theorem 5, $r = s$ and $\theta(R_i) = S_{\sigma(i)}$ for some permutation σ. Each $\theta_i : R_i \to S_{\sigma(i)}$ is either an isomorphism or an anti-isomorphism (or both, if R_i corresponds to a one-degree representation). Let

$$R^+ = \prod\{R_i : \theta_i \text{ is an isomorphism}\},$$

$$R^- = \prod \{R_i : \theta_i \text{ is an anti-isomorphism}\},$$

and consider the maps

$$\pi^+ : G \to \mathbb{C}G \to R \to R^+$$

$$\pi^+ : G \to \mathbb{C}G \to R \to R^-$$

defined in the obvious manner.

Let $N^+, N^- \subset G$ be the respective kernels, ie. the elements in the group that map to 1 in the algebra. Suppose $g \in N^+ \cap N^-$. Then $\pi^+(g) = 1$, $\pi^-(g) = 1$, but $R^+ + R^- = R$, so $\pi(g) = 1 \in R$ and g is the identity. As these subgroups are normal and intersect trivially, $N^+ \times N^- \cong N^+N^-$ and we may regard the direct product of the two as a subgroup of G.

Assume both N^+ and N^- are non-trivial. Let (ν^+, V^+) and (ν^-, V^-) be non-trivial irreducible representations for N^+ and N^- respectively. Then $(\nu^+ \otimes \nu^-, V^+ \otimes V^-)$ is an irreducible representation of $N^+ \times N^-$. We know (either directly or by Frobenius Reciprocity) that $\nu^+ \otimes \nu^-$ lies inside one of the irreducible representations π_j of G. That is, the restriction of π_j to $N^+ \times N^-$ has $\nu^+ \otimes \nu^-$ as a component. Since ν^+ and ν^- are non-trivial, the kernel of π_j can contain neither N^+ nor N^-. However, the construction of R^+ and R^- ensures that either N^+ or N^- is in the kernel of any π_j.

This contradiction shows that either N^+ or N^- is trivial. If $N^+ = 1$, $\theta : R \to S$ is an algebra isomorphism, so $\psi : G \to H$ is a group isomorphism. If $N^- = 1$, $\psi : G \to H$ is an anti-isomorphism. □

Corollary 7. *If G and H are finite groups and $\psi : G \to H$ is a bijection of sets such that $\psi(\mathcal{U}(\mathbb{C}G)) = \mathcal{U}(\mathbb{C}H)$ then G and H are isomorphic.*

Proof. Replace the bijection ψ, with $\tilde{\psi}(g) = \psi(g)\psi(e)^{-1}$, where e is the identity of G, and apply the theorem. □

This fact is remarkable, as it gives a seemingly weak but yet sufficient condition for two groups to be isomorphic. Formanek and Sibley proved this result as a step in the proof that the group determinant determines the group. Either they didn't realize the result could stand on its own, or they didn't think it worth mentioning.

Before proving the final result, we need to rigourously define what it means for two groups to have the same determinant. Let G and H be finite groups, $\psi : G \to H$ a bijection. Then ψ defines a field isomorphism

$$\hat{\psi} : \mathbb{C}(x_g) \to \mathbb{C}(x_h), \qquad x_g \mapsto x_{\psi(g)}.$$

If $\hat{\psi}(\mathfrak{D}_G) = \mathfrak{D}_H$ for some bijection ψ then G and H have the same determinant.

Theorem 8. *If finite groups G and H have the same determinant, they are isomorphic.*

Proof. Let $\psi : G \to H$ be a bijection such that $\hat{\psi}(\mathfrak{D}_G) = \mathfrak{D}_H$. ψ induces a map $\psi : \mathbb{C}G \to \mathbb{C}H$ on the group algebras. By Corollary 7, we need only show that ψ maps units in $\mathbb{C}G$ to units in $\mathbb{C}H$.

Let π, ρ be the respective left regular representations of G and H. For $\sum a_g g \in \mathbb{C}G$, $\pi\left(\sum a_g g\right) = \sum a_g \pi(g)$ represents left multiplication by $\sum a_g g$ in $\mathbb{C}G$. In particular,

$$\det \pi \left(\sum a_g g \right) \neq 0$$

if and only if $\sum a_g g$ is a unit of $\mathbb{C}G$.

Recall $\mathfrak{X}_G = \sum x_g g \in \mathbb{C}(x_g)G$ and $\mathfrak{D}_G = \det \pi(\mathfrak{X}_G)$. Then

$$\begin{aligned} \hat{\psi}(\mathfrak{D}_G) = \mathfrak{D}_H \quad &\Rightarrow \\ \hat{\psi}(\det \pi(\mathfrak{X}_G)) = \det \rho(\mathfrak{X}_H) \quad &\Rightarrow \\ \hat{\psi}\left(\det \sum_g \pi(g) x_g \right) = \det \sum_h \rho(h) x_h \quad &\Rightarrow \\ \det \sum_g \pi(g) x_{\psi(g)} = \det \sum_h \rho(h) x_h. & \end{aligned} \tag{3}$$

Take $\sum a_g g \in \mathbb{C}G$. Then $\psi(\sum a_g g) = \sum a_g \psi(g) \in \mathbb{C}H$.

$$\begin{aligned} \det \rho \left(\sum_g a_g \psi(g) \right) &= \det \sum_g a_g \rho(\psi(g)) \\ &= \det \sum_h a_{\psi^{-1}(h)} \rho(h) \end{aligned}$$

Set $x_h = a_{\psi^{-1}(h)}$. Then $x_{\psi(g)} = a_g$, and (3) becomes

$$\det \sum_g \pi(g) a_g = \det \sum_h \rho(h) a_{\psi^{-1}(h)}$$

so

$$\det\rho\left(\psi\left(\sum_g a_g g\right)\right) = \det\pi\left(\sum_g a_g g\right).$$

In particular, $\sum a_g g$ is a unit if and only if $\psi(\sum a_g g)$ is a unit. Then by Corollary 7, G and H are isomorphic. □

As the group determinant carries the same amount of information as all of the k-characters of all irreducible representations of the group, the k-characters also determine the group. However, neither of these forms may be practical to use for a large group, particularly if it has irreducible representations of high degree.

Fortunately, one can show that the 1- 2- and 3-characters uniquely determine the group.[5] Loosely speaking, this is because these characters determine coefficients of terms of the group determinant of the form $x_e^{n-3}x_a x_b x_c$. Mansfield showed that the group is uniquely determined by terms of this form. With the orthogonality relations of k-characters, it is feasable to build a 3-character table to aid in studying a group.

The 2-characters do not uniquely determine the group, which can be seen with group orders as low as 27, but there is likely an invariant between the 2-characters and 3-characters that does.[7] Research continues to develop and understand useful invariants for finite groups.

References

[1] J. Dieudonne. Sur une generalisation du groupe orthogonal a quatre variables. *Arch. Math.*, 1:282–287, 1949.

[2] David S. Dummit and Richard M. Foote. *Abstact Algebra*. Wiley, 1999.

[3] Edward Formanek and David Sibley. The group determinant determines the group. *Proc. Amer. Math. Soc.*, 112(3):649–656, 1991.

[4] T. Hawkins. The origins of the theory of group characters. *Arch. Hist. Exact. Sci.*, 7:142–170, 1971.

[5] H.-J. Hoehnke and K. W. Johnson. The 1-, 2-, and 3-characters determine a group. *Bull. Amer. Math. Soc.*, 27(2):243–245, 1992.

[6] K. W. Johnson. *Algebraic, extremal and metric combinatorics*, chapter Latin square determinants, pages 146–154. London Math. Soc. Lecture Notes Series 131. Cambridge Univ. Press, 1988.

[7] Kenneth W. Johnson and Surinder K. Sehgal. The 2-characters of a group and the group determinant. *European J. Combin.*, 14(2):103–112, 1993.

[8] Richard Mansfield. A group determinant determines it group. *Proc. Amer. Math. Soc.*, 116(4):939–941, 1992.