THE ORIGIN OF REPRESENTATION THEORY

Autor(en): **CONRAD, Keith**

Objekttyp: **Article**

Zeitschrift: **L'Enseignement Mathématique**

Band (Jahr): **44 (1998)**

Heft 3-4: **L'ENSEIGNEMENT MATHÉMATIQUE**

PDF erstellt am: **21.07.2024**

Persistenter Link: https://doi.org/10.5169/seals-63909

L'Enseignement Mathématique, t. 44 (1998), p. 361–392

THE ORIGIN OF REPRESENTATION THEORY

by Keith CONRAD

ABSTRACT. Representation theory was created by Frobenius about 100 years ago. We describe the background that led to the problem which motivated Frobenius to define characters of a finite group and show how representation theory solves the problem. The first results about representation theory in characteristic p are also discussed.

1. INTRODUCTION

Characters of finite abelian groups have been used since Gauss in the beginning of the 19th century, but it was only near the end of that century, in 1896, that Frobenius extended this concept to finite nonabelian groups [21]. Frobenius' approach to group characters is not in common use today, although some of his ideas that were overlooked for a long period have recently been revived [30].

Here we trace the development of the problem whose solution led Frobenius to introduce characters of finite groups, show how this problem can be solved using classical representation theory of finite groups, and indicate some relations between this problem and modular representations.

Other surveys on the origins of representation theory are by Curtis [7], Hawkins [24, 25, 26, 27], Lam [32], Ledermann [35] and van der Waerden [38]. While Curtis describes the development of modular representation theory focusing on the work of Brauer, we examine the earlier work in characteristic p of Dickson.

2. Circulants

For a positive integer n, consider an $n \times n$ matrix where each row is obtained from the previous one by a cyclic shift one step to the right. That is, we look at a matrix of the form

$$\begin{pmatrix} X_0 & X_1 & X_2 & \dots & X_{n-1} \\ X_{n-1} & X_0 & X_1 & \dots & X_{n-2} \\ \vdots & \vdots & \vdots & \ddots & \vdots \\ X_1 & X_2 & X_3 & \dots & X_0 \end{pmatrix}.$$

Let's think of the X_i's as indeterminates. The determinant of this matrix is called a *circulant* of order n. It is a homogeneous polynomial of degree n with integer coefficients. Circulants were first introduced in 1846 by Catalan [5, p. 549].

The circulants of order 2 and 3 are

$$\begin{vmatrix} X_0 & X_1 \\ X_1 & X_0 \end{vmatrix} = X_0^2 - X_1^2 = (X_0 + X_1)(X_0 - X_1),$$

and

$$\begin{aligned} \begin{vmatrix} X_0 & X_1 & X_2 \\ X_2 & X_0 & X_1 \\ X_1 & X_2 & X_0 \end{vmatrix} &= X_0^3 + X_1^3 + X_3^3 - 3X_0X_1X_2 \\ &= (X_0 + X_1 + X_2)(X_0 + \omega X_1 + \omega^2 X_2)(X_0 + \omega^2 X_1 + \omega X_2), \end{aligned}$$

where $\omega = e^{2\pi i/3}$.

Spottiswoode stated without proof in [37, p. 375] that over the complex numbers, the circulant of order n factors into n homogeneous linear polynomials whose coefficients are n-th roots of unity, as follows.

Theorem 1.

$$\begin{aligned} \begin{vmatrix} X_0 & X_1 & X_2 & \dots & X_{n-1} \\ X_{n-1} & X_0 & X_1 & \dots & X_{n-2} \\ \vdots & \vdots & \vdots & \ddots & \vdots \\ X_1 & X_2 & X_3 & \dots & X_0 \end{vmatrix} &= \prod_{j=0}^{n-1} \Bigl(\sum_{k=0}^{n-1} \zeta^{jk} X_k \Bigr) \\ &= \prod_{j=0}^{n-1} (X_0 + \zeta^j X_1 + \dots + \zeta^{(n-1)j} X_{n-1}), \end{aligned}$$

where $\zeta \in \mathbf{C}$ is a primitive n-th root of unity.

Proof. We give two proofs. The first is essentially the first published proof, by Cremona [6], where the idea is attributed to Brioschi.

Let $f(T) = \sum_{k=0}^{n-1} X_k T^k$. We want to show the circulant of order n has determinant

$$\prod_{j=0}^{n-1} f(\zeta^j).$$

Consider the equation of $n \times n$ matrices

$$(X_{j-i})(\zeta^{ij}) = \Big(\sum_{k=0}^{n-1} \zeta^{j(k+i)} X_k\Big) = (f(\zeta^j)\zeta^{ij}).$$

In full, this reads

$$\begin{pmatrix} X_0 & X_1 & X_2 & \dots & X_{n-1} \\ X_{n-1} & X_0 & X_1 & \dots & X_{n-2} \\ \vdots & \vdots & \vdots & \ddots & \vdots \\ X_1 & X_2 & X_3 & \dots & X_0 \end{pmatrix} \begin{pmatrix} 1 & 1 & 1 & \dots & 1 \\ 1 & \zeta & \zeta^2 & \dots & \zeta^{n-1} \\ \vdots & \vdots & \vdots & \ddots & \vdots \\ 1 & \zeta^{n-1} & \zeta^{2(n-1)} & \dots & \zeta^{(n-1)^2} \end{pmatrix}$$

$$= \begin{pmatrix} \sum X_k & \sum \zeta^k X_k & \dots & \sum \zeta^{(n-1)k} X_k \\ \sum X_k & \sum \zeta^{k+1} X_k & \dots & \sum \zeta^{(n-1)(k+1)} X_k \\ \vdots & \vdots & \ddots & \vdots \\ \sum X_k & \sum \zeta^{k+n-1} X_k & \dots & \sum \zeta^{(n-1)(k+n-1)} X_k \end{pmatrix}$$

$$= \begin{pmatrix} f(1) & f(\zeta) & \dots & f(\zeta^{n-1}) \\ f(1) & f(\zeta)\zeta & \dots & f(\zeta^{n-1})\zeta^{n-1} \\ \vdots & \vdots & \ddots & \vdots \\ f(1) & f(\zeta)\zeta^{n-1} & \dots & f(\zeta^{n-1})\zeta^{(n-1)^2} \end{pmatrix}.$$

The matrix (ζ^{ij}) is Vandermonde with nonzero determinant (since ζ is a primitive n-th root of unity), so we're done by taking determinants.

For the second proof, let $0 \le r \le n-1$. Add ζ^{-ir} times the i-th row $(1 \le i \le n-1)$ of the matrix (X_{j-i}) to the zeroth (i.e., top) row. This does not affect the value of the determinant. Now the top row has j-th entry $(0 \le j \le n-1)$ equal to

$$\sum_{i \in \mathbf{Z}/n\mathbf{Z}} \zeta^{-ir} X_{j-i} = \sum_{k \in \mathbf{Z}/n\mathbf{Z}} \zeta^{r(k-j)} X_k = \zeta^{-rj} f(\zeta^r).$$

So the circulant is divisible by $f(\zeta^r)$. Since the polynomials $f(\zeta^r)$ are relatively prime for different r, the circulant is divisible by $\prod_{r=0}^{n-1} f(\zeta^r)$. This is a homogeneous polynomial of degree n, so this product equals the circulant up to a scaling factor. Since both polynomials are monic in X_0, the scaling factor is 1. □

Anticipating later extensions of Theorem 1, it is useful to regard the subscript of X_k as an element of $\mathbf{Z}/n\mathbf{Z}$. Then the circulant is $\det(X_{j-i})$. Actually, Catalan, Spottiswoode, and Cremona worked with $\det(X_{i+j})$, but these two determinants differ only in sign: $\det(X_{i+j}) = (-1)^{(n-1)(n-2)/2}\det(X_{j-i})$. Spottiswoode's formula had a sign error, Cremona's did not.

How does the circulant factor over a field of characteristic p? The use of the complex numbers is as container of appropriate roots of unity for the factorization. So the argument above works over any algebraically closed field of characteristic prime to n, since such a field contains a primitive n-th root of unity. The field doesn't have to be algebraically closed; we just need the polynomial Y^n-1 to split completely over the field into distinct linear factors. What if we work over a field of characteristic p where $p \mid n$? Let's look at an example, $p=2$ and $n=2$. Over a field of characteristic 0,

$$\begin{vmatrix} X_0 & X_1 \\ X_1 & X_0 \end{vmatrix} = (X_0 - X_1)(X_0 + X_1).$$

Over a field of characteristic 2,

$$\begin{vmatrix} X_0 & X_1 \\ X_1 & X_0 \end{vmatrix} = (X_0 + X_1)(X_0 + X_1) = (X_0 + X_1)^2.$$

This factorization reflects that of Y^2-1. In characteristic 0, $Y^2-1 = (Y-1)(Y+1)$ is a product of two relatively prime polynomials. In characteristic 2, $Y^2-1=(Y+1)^2$ is the square of a single polynomial. This gives the flavor of the general case in characteristic p. If $p \mid n$ then the circulant of order n factors in characteristic p the same way as it does in characteristic 0, except we have some repeated factors appearing as they do in the factorization of Y^n-1 in characteristic p. That is, over a field F of characteristic p where Y^n-1 splits completely,

$$\begin{vmatrix} X_0 & X_1 & X_2 & \dots & X_{n-1} \\ X_{n-1} & X_0 & X_1 & \dots & X_{n-2} \\ \vdots & \vdots & \vdots & \ddots & \vdots \\ X_1 & X_2 & X_3 & \dots & X_0 \end{vmatrix} = \prod_{\substack{\omega\in F \\ \omega^n=1}} \left(\sum_{k=0}^{n-1} \omega^k X_k\right),$$

where any n-th root of unity in F is repeated as often as its multiplicity as a root of $Y^n - 1$. Writing $n = p^r m$ with m prime to p, the right hand side of the above equation equals

$$\prod_{\substack{\omega \in F \\ \omega^m = 1}} \Big(\sum_{k=0}^{n-1} \omega^k X_k \Big)^{p^r} .$$

As an example of this, in characteristic p

$$\det(X_{j-i})_{i,j \in \mathbf{Z}/p^r\mathbf{Z}} = (X_0 + X_1 + \cdots + X_{p^r-1})^{p^r} .$$

The factorization of the circulant in characteristic p was needed by Davenport in [9], where he gave a proof using resultants. As an alternate proof, reduce the characteristic 0 formula mod p by the appropriate technical device. One choice is to work over the ring $\mathbf{Z}[\zeta_n]$ and reduce modulo a prime divisor of p. A second choice is to work over the p-adic ring $\mathbf{Z}_p[\zeta_n]$ and pass to the residue field. The factorization in characteristic 0 then passes to characteristic p, and factors that had been distinct in characteristic 0 are now repeated in the way $Y^n - 1$ factors in characteristic p.

3. THE WORK OF DEDEKIND

Parts of this section are based on [24].

Dedekind was led to an extension of the circulant by considerations in algebraic number theory. Let $K/\mathbf{Q}$ be a finite Galois extension of degree n with Galois group $G = \{\sigma_1, \ldots, \sigma_n\}$. The *discriminant* of a set of n elements $\alpha_1, \ldots, \alpha_n$ of K is defined to be the square of the determinant

$$\begin{vmatrix} \sigma_1(\alpha_1) & \sigma_1(\alpha_2) & \ldots & \sigma_1(\alpha_n) \\ \sigma_2(\alpha_1) & \sigma_2(\alpha_2) & \ldots & \sigma_2(\alpha_n) \\ \vdots & \vdots & \ddots & \vdots \\ \sigma_n(\alpha_1) & \sigma_n(\alpha_2) & \ldots & \sigma_n(\alpha_n) \end{vmatrix} .$$

We will be using this as motivation for the group determinant below.

Dedekind had reasons to consider the discriminant of n elements formed by the $\mathbf{Q}$-conjugates $\sigma_i(\alpha)$ of a single element α. In that case the discriminant becomes the square of

$$\begin{vmatrix} \sigma_1(\sigma_1(\alpha)) & \sigma_1(\sigma_2(\alpha)) & \ldots & \sigma_1(\sigma_n(\alpha)) \\ \sigma_2(\sigma_1(\alpha)) & \sigma_2(\sigma_2(\alpha)) & \ldots & \sigma_2(\sigma_n(\alpha)) \\ \vdots & \vdots & \ddots & \vdots \\ \sigma_n(\sigma_1(\alpha)) & \sigma_n(\sigma_2(\alpha)) & \ldots & \sigma_n(\sigma_n(\alpha)) \end{vmatrix} .$$

Let $x_\sigma = \sigma(\alpha)$. Then this is the determinant of the matrix $(a_{\sigma,\tau})$ doubly indexed by G, where $a_{\sigma,\tau} = x_{\sigma\tau}$.

Dedekind's work with $\det(x_{\sigma\tau})$ soon convinced him that working with $\det(x_{\sigma\tau^{-1}})$ would be more convenient. Perhaps one reason is that the entries along the main diagonal of $(x_{\sigma\tau^{-1}})$ are all the same, x_e. For any finite group G we form a set of variables $\{X_g\}$ indexed by G and define the *group matrix* to be $(X_{gh^{-1}})$. This matrix can be thought of as one where each row is obtained from a fixed row (e.g., the top row if an ordering is put on the index set G) by the group G acting as permutations on the subscripts of the entries in the fixed row. The matrix introduced in Section 2 in connection with the circulant is the transpose of the group matrix for $\mathbf{Z}/n\mathbf{Z}$. The *group determinant* is defined to be

$$\Theta(G) = \det(X_{gh^{-1}}).$$

This is a homogeneous polynomial in the X_g's of degree $n = \#G$ with integer coefficients. Note $\det(X_{gh^{-1}}) = \det(X_{g^{-1}h})$. When $G = \mathbf{Z}/n\mathbf{Z}$, the group determinant is the circulant of order n.

The group matrix is closely related to the group algebra, for example the map $\mathbf{Z}[G] \to \mathrm{M}_n(\mathbf{Z})$ given by $\sum_g x_g g \mapsto (x_{gh^{-1}})$ is a ring homomorphism. This will be useful later on.

Around 1880, Dedekind proved that when G is any finite abelian group, $\Theta(G)$ factors over $\mathbf{C}$ into a product of linear factors with coefficients being roots of unity. Burnside proved this too [3], using the decomposition of any finite abelian group into a product of cyclic groups, and an argument similar to the second proof of Theorem 1. Although Dedekind and Burnside established basically the same factorization, Dedekind's formulation was superior because he had a conceptual idea of where the roots of unity were coming from, as can be seen in the following statement of his result, which gives some insight into the role of the roots of unity appearing in the factorization of the circulant.

THEOREM 2. *Let G be a finite abelian group. Then*

$$\det(X_{gh^{-1}}) = \prod_{\chi\in\widehat{G}} \Big(\sum_{g\in G} \chi(g) X_g\Big),$$

where $\widehat{G}$ is the character group of G, namely the group of homomorphisms from G to $\mathbf{C}^\times$.

Proof. We give two proofs. The first one is based on a proof for the circulant factorization. This argument will extend only partially to nonabelian groups. We motivate the approach to the nonabelian situation by giving a second proof that is developed inside the group algebra $\mathbf{C}[G]$.

Our first proof will mimic the second proof of Theorem 1. Fix a character χ of G. For each nonidentity element g of G, add $\chi(g)$ times the g-th row of the group matrix $(X_{gh^{-1}})$ to the row indexed by the identity, e. The entry in row e and column h becomes

$$\sum_g \chi(g) X_{gh^{-1}} = \chi(h) \sum_g \chi(g) X_g .$$

Here the sum includes $g = e$. Thus $\Theta(G)$ is divisible by $\sum_g \chi(g) X_g$. Such polynomials are relatively prime for different χ since different characters are not scalar multiples. The product of all these factors is homogeneous of degree n and monic in X_e, like $\Theta(G)$, so it equals $\Theta(G)$.

Here is a second proof. We consider two bases of $\mathbf{C}[G]$, G and $\{\sum_g \chi(g) g\}_{\chi \in \widehat{G}}$. That the second set is a basis is a different way of saying the characters of G are linearly independent. Left multiplication on $\mathbf{C}[G]$ by any element $\sum a_g g$ is a linear map. Let's express it as a matrix with respect to these two bases.

First we use the basis G. For $h \in G$,

$$\left(\sum a_g g\right) h = \sum a_{gh^{-1}} g ,$$

so the matrix is $(a_{gh^{-1}})$, whose determinant is $\det(a_{gh^{-1}})$.

Now we use the basis $\sum_g \chi(g) g$ as χ runs over $\widehat{G}$. We have

$$\begin{aligned}\left(\sum_g a_g g\right)\left(\sum_h \chi(h) h\right) &= \sum_k \left(\sum_{gh=k} a_g \chi(h)\right) k \\ &= \sum_k \left(\sum_g a_g \chi(g^{-1}) \chi(k)\right) k \\ &= \left(\sum_g a_g \chi(g^{-1})\right)\left(\sum_k \chi(k) k\right).\end{aligned}$$

The basis $\{\sum_g \chi(g) g\}$ for $\mathbf{C}[G]$ consists of eigenvectors for left multiplication by $\sum a_g g$, so the determinant of this left multiplication is the product of its eigenvalues, hence

$$\det(a_{gh^{-1}}) = \prod_{\chi \in \widehat{G}} \left(\sum_{g \in G} \chi^{-1}(g) a_g\right) = \prod_{\chi \in \widehat{G}} \left(\sum_{g \in G} \chi(g) a_g\right).$$

Therefore the polynomials $\det(X_{gh^{-1}})$ and $\prod_{\chi \in \widehat{G}} \left(\sum_{g \in G} \chi(g) X_g\right)$ are equal functions on all of $\mathbf{C}^n$, so they must be the same polynomial. □

For a proof of Theorem 2 that mimics the matrix product proof of the circulant factorization, see [2, p. 421, Exer. 14]. A variant on the second proof of Theorem 2 can be found in [34, pp. 89–90] and [2, p. 421, Exer. 12, 13].

EXAMPLE. $G = \mathbf{Z}/2\mathbf{Z} \times \mathbf{Z}/2\mathbf{Z}$. For purposes of convenient notation, writing X_g will be cumbersome. Let's write

$$X_1 = X_{(0,0)}\,,\ X_2 = X_{(0,1)}\,,\ X_3 = X_{(1,0)}\,,\ X_4 = X_{(1,1)}\,.$$

Then Dedekind's theorem says

$$\begin{vmatrix} X_1 & X_2 & X_3 & X_4 \\ X_2 & X_1 & X_4 & X_3 \\ X_3 & X_4 & X_1 & X_2 \\ X_4 & X_3 & X_2 & X_1 \end{vmatrix} = (X_1+X_2+X_3+X_4)(X_1+X_2-X_3-X_4) \\ \times (X_1-X_2+X_3-X_4)(X_1-X_2-X_3+X_4)\,.$$

What form does Theorem 2 take if we factor the group determinant of an abelian group over an algebraically closed field F of characteristic p ? If $n = \#G$ is prime to p, then G has n characters in characteristic p, i.e. there are n homomorphisms $G \to F^\times$, and the above formula of Dedekind's still works. In fact, the proof of Theorem 2 still works. If $n = p^r m$ where m is prime to p, then there are m homomorphisms $G \to F^\times$, and by reducing the characteristic 0 formula into characteristic p by either of the tools mentioned in connection with the circulant formula in characteristic p, we see that for each character $\chi\colon G \to F^\times$, the linear factor $\sum_g \chi(g) X_g$ appears in the factorization of $\Theta(G)$ over F with multiplicity p^r. For instance, if G is an abelian p-group then the only group homomorphism $G \to F^\times$ is the trivial character and

$$\Theta(G) = \Big(\sum_{g\in G} X_g\Big)^{\#G}.$$

Around 1886, Dedekind became interested in factoring the group determinant for nonabelian finite groups. His first discovery was that when the group is nonabelian, some of the irreducible factors of the group determinant might not be linear. Let's see this in two examples that Dedekind worked out.

EXAMPLE [10, pp. 423–424]. Let $G = S_3$. It is easier to write the variables as X_i, $1 \le i \le 6$, rather than as X_π, $\pi \in S_3$. We enumerate the elements of S_3 as Dedekind did:

$$\pi_1 = (1)\,,\ \pi_2 = (123)\,,\ \pi_3 = (132)\,,\ \pi_4 = (23)\,,\ \pi_5 = (13)\,,\ \pi_6 = (12)\,.$$

Set $X_i = X_{\pi_i}$. Then Dedekind calculated

$$\Theta(S_3) = \Phi_1\Phi_2\Phi_3^2,$$

where

$$\begin{aligned}
\Phi_1 &= X_1 + X_2 + X_3 + X_4 + X_5 + X_6,\\
\Phi_2 &= X_1 + X_2 + X_3 - X_4 - X_5 - X_6,\\
\Phi_3 &= X_1^2 + X_2^2 + X_3^2 - X_4^2 - X_5^2 - X_6^2\\
&\qquad - X_1X_2 - X_1X_3 - X_2X_3 + X_4X_5 + X_4X_6 + X_5X_6.
\end{aligned}$$

He used the change of variables

$$\begin{aligned}
u &= X_1 + X_2 + X_3, & v &= X_4 + X_5 + X_6,\\
u_1 &= X_1 + \omega X_2 + \omega^2 X_3, & v_1 &= X_4 + \omega X_5 + \omega^2 X_6,\\
u_2 &= X_1 + \omega^2 X_2 + \omega X_3, & v_2 &= X_4 + \omega^2 X_5 + \omega X_6,
\end{aligned}$$

to write the factorization of $\Theta(S_3)$ as

$$\Theta(S_3) = (u+v)(u-v)(u_1u_2 - v_1v_2)^2.$$

Obviously Φ_1 and Φ_2 are irreducible. What about Φ_3 ? Since the change of variables from the X's to the u's and v's is invertible, it gives a $\mathbf{C}$-algebra automorphism of the polynomial ring over $\mathbf{C}$ in the X_i's. In particular, the u's and v's are algebraically independent over $\mathbf{C}$. In $\mathbf{C}[u, v, u_1, v_1, u_2, v_2]$, $u_1u_2 - v_1v_2$ is irreducible, so Φ_3 is irreducible. For future reference, note we proved irreducibility of Φ_3 by finding a linear change of variables converting Φ_3 to the determinant of a 2×2 matrix with algebraically independent entries.

Dedekind's change of variables was perhaps motivated by the case of group determinants for abelian groups, where roots of unity arise as coefficients. We will see later (equation (5.1)) that an expression of Φ_3 in the form $ad - bc$ can be found where a, b, c, d are linear polynomials in the X_i's with *integer* coefficients. This is related to the fact that the irreducible 2-dimensional complex representation of S_3 can be written using matrices with integer entries.

Hamilton's 1843 discovery of quaternions gave rise to interest in "hypercomplex" number systems, i.e. associative $\mathbf{C}$-algebras. Dedekind decided that since $\Theta(S_3)$ didn't factor into linear factors over $\mathbf{C}$, he should find an appropriate hypercomplex number system over which the factors become linear. It seems plausible by looking at Φ_3 that if it can be made into a product of linear factors over some hypercomplex system, there should be two homogeneous linear factors, so [10, pp. 438–441] Dedekind wrote

$$\Phi_3 = \left(\sum \alpha_i X_i\right)\left(\sum \beta_i X_i\right), \tag{3.1}$$

for some elements α_i and β_i in an unknown hypercomplex system. In particular, $\alpha_1\beta_1 = 1$. Dedekind normalized this hypothesized factorization by setting $\alpha_1 = \beta_1 = 1$ and then multiplied out the right hand side of (3.1), keeping in mind that there may be noncommutativity among the coefficients. He obtained a number of relations between the α's and the β's, such as

$$\begin{gathered}\alpha_2 + \beta_2 = \alpha_3 + \beta_3 = -1\,, \\ \alpha_4 + \beta_4 = \alpha_5 + \beta_5 = \alpha_6 + \beta_6 = 0\,, \\ \alpha_2\beta_2 = \alpha_3\beta_3 = 1\,, \\ \alpha_4\beta_4 = \alpha_5\beta_5 = \alpha_6\beta_6 = -1\,.\end{gathered}$$

So $\alpha_4 = -\beta_4$, hence $\alpha_4^2 = -\alpha_4\beta_4 = 1$. Similarly, $\alpha_5^2 = \alpha_6^2 = 1$. Also $\alpha_2 = -1 - \beta_2$, so $\alpha_2^2 = -\alpha_2 - \alpha_2\beta_2 = -\alpha_2 - 1$, hence $1 + \alpha_2 + \alpha_2^2 = 0$, so $\alpha_2^3 = 1$. Similarly, $\alpha_3^3 = 1$. Note that π_2 and π_3 have order 3 and the coefficients of X_2 and X_3 satisfy $\alpha_2^3 = \alpha_3^3 = 1$, while π_4, π_5, π_6 have order 2 and the coefficients of X_4, X_5, and X_6 satisfy $\alpha_4^2 = \alpha_5^2 = \alpha_6^2 = 1$. So writing π_i in place of α_i and defining β_i by the above additive relation with α_i, it seems we may have factored Φ_3 into linear factors over the noncommutative ring $\mathbf{C}[S_3]$. This is not quite correct. Identifying α_i as π_i in $\mathbf{C}[S_3]$ leads to some collapsing of the ring. For example, looking at the coefficient of X_2X_3 in (3.1) leads to

$$\begin{aligned}-1 &= \alpha_2\beta_3 + \alpha_3\beta_2 = \alpha_2(-1-\alpha_3) + \alpha_3(-1-\alpha_2) \\ &= -\alpha_2 - \alpha_3 - \alpha_2\alpha_3 - \alpha_3\alpha_2 = -\pi_2 - \pi_3 - \pi_2\pi_3 - \pi_3\pi_2 = -\pi_2 - \pi_3 - 2\,,\end{aligned}$$

so we need $1 + \pi_2 + \pi_3 = 0$. Multiplying this equation through by π_4 on the left leads to $\pi_4 + \pi_5 + \pi_6 = 0$. It is left to the reader to check that (3.1) is true over $\mathbf{C}[S_3]/\Omega$, where Ω is the subspace generated by $1 + \pi_2 + \pi_3$ and $\pi_4 + \pi_5 + \pi_6$, which is a 2-sided ideal. The 4-dimensional $\mathbf{C}$-algebra $\mathbf{C}[S_3]/\Omega$ is isomorphic to the 2 by 2 matrices over $\mathbf{C}$.

EXAMPLE [10, pp. 424–425]. Let $G = Q_8$, the quaternion group $\{\pm 1, \pm i, \pm j, \pm k\}$. We index the elements of G as

$$g_1 = 1\,,\ g_2 = -1\,,\ g_3 = i\,,\ g_4 = -i\,,\ g_5 = j\,,\ g_6 = -j\,,\ g_7 = k\,,\ g_8 = -k\,.$$

Let $X_i = X_{g_i}$, $1 \leq i \leq 8$. Dedekind computed

$$\Theta(Q_8) = \Phi_1\Phi_2\Phi_3\Phi_4\Phi_5^2 ,$$

where

$$\begin{aligned}
\Phi_1 &= X_1 + X_2 + X_3 + X_4 + X_5 + X_6 + X_7 + X_8 , \\
\Phi_2 &= X_1 + X_2 + X_3 + X_4 - X_5 - X_6 - X_7 - X_8 , \\
\Phi_3 &= X_1 + X_2 - X_3 - X_4 + X_5 + X_6 - X_7 - X_8 , \\
\Phi_4 &= X_1 + X_2 - X_3 - X_4 - X_5 - X_6 + X_7 + X_8 , \\
\Phi_5 &= \sum X_i^2 - 2X_1X_2 - 2X_3X_4 - 2X_5X_6 - 2X_7X_8 \\
&= (X_1 - X_2)^2 + (X_3 - X_4)^2 + (X_5 - X_6)^2 + (X_7 - X_8)^2 .
\end{aligned}$$

Only Φ_5 is not linear, and it is irreducible over **C**. There is an obvious "hypercomplex" number system over which Φ_5 becomes a product of linear factors, namely the quaternions **H** (although **C** is not in its center).

In general, Dedekind wanted to find a hypercomplex number system over which $\Theta(G)$ factors linearly and understand how the structure of G is reflected in such a hypercomplex system. Ten years later, in 1896, Dedekind classified the finite groups all of whose subgroups are normal (Hamiltonian groups), and in a letter to Frobenius where he wrote about this result [10, pp. 420–421], Dedekind mentioned the group determinant, explained how it factors in the abelian case, and suggested Frobenius think about the nonabelian case. It is the question of factoring the group determinant of an arbitrary finite group that gave rise to representation theory by Frobenius, though other algebraic developments in the late 19th century were also heading in this direction [25].

4. The work of Frobenius

Frobenius felt the interesting problem was not finding a hypercomplex number system where $\Theta(G)$ becomes a product of linear factors, but finding the irreducible factors of $\Theta(G)$ over the complex numbers, whether or not they are linear. His solution to this problem appeared in [22], and depended on the papers [20] and [21], where he established the needed facts about commuting matrices and characters of finite groups.

Frobenius begins [21] by recalling previous uses of characters in number theory. Here is how the paper starts:

> «When he proved that every linear function of one variable represents infinitely many prime numbers if its coefficients are coprime integers, Dirichlet used for the first time certain systems of roots of unity, which also appear when one treats the closely related problem of the number of ideal classes in cyclotomic fields [...]»

Establishing Dirichlet's theorem on primes in the arithmetic progression $m+nj$ $(j \in \mathbf{N})$ and the class number formula for the cyclotomic field $\mathbf{Q}(\zeta_n)$ involve not only the characters of $(\mathbf{Z}/n\mathbf{Z})^\times$, but also something Frobenius did not explicitly refer to: L-functions of these characters. This was about thirty years before Artin [1] introduced L-functions of the characters Frobenius introduced in [21].

Towards the end of the introduction to [21] is a prescient comment:

> «In April of this year, Dedekind gave me an exercise ... [whose] solution, which I hope to be able to present soon, led me to a generalization of the notion of a character to arbitrary finite groups. I want to develop this notion here since I believe that by its introduction, group theory should undergo a major advancement and enrichment.»

We begin our analysis of the factorization of $\Theta(G)$ by writing down one factor that is always present and indicating how to normalize the factorization. Since each row of the matrix $(X_{gh^{-1}})$ contains the sequence $\{X_g\}$ in some order, adding all the columns to a fixed column shows $\Theta(G)$ is divisible by $\sum_{g\in G} X_g$. This observation, for cyclic G, was made by Catalan when he first introduced circulants.

Since $\Theta(G)$ is homogeneous of degree $n = \#G$, its irreducible factors are also homogeneous. If we set the variables X_g for $g \neq e$ equal to 0, then $\Theta(G)$ becomes the polynomial X_e^n. Therefore we fix a definite factorization of $\Theta(G)$ into irreducibles by requiring the irreducible factors to be monic in X_e. It will turn out that this is Frobenius' factorization of the group determinant of G.

What are irreducible factors of $\Theta(G)$ besides $\sum X_g$? For each character $\chi\colon G \to \mathbf{C}^\times$ we have a factor $\sum_g \chi(g)X_g$, proven just as in the proof of Theorem 2. This accounts for $\#G/[G,G]$ factors, which leaves more factors to determine for nonabelian G.

In only a few months Frobenius solved this problem. Letting s denote the number of conjugacy classes of G, Frobenius proved $\Theta(G)$ has s (homogeneous) irreducible factors that are monic in X_e, each one having degree equal to its multiplicity in the factorization of $\Theta(G)$. That is,

$$\Theta(G) = \prod_{i=1}^{s} \Phi_i^{f_i} ,$$

where Φ_i is homogeneous irreducible and f_i is the degree of Φ_i. He also [22, Sect. 12] proved $f_i \mid n$. (Taking degrees of both sides, we get $n = \sum_i f_i^2$, which should look familiar from representation theory. We'll see later that the f_i's are the degrees of the irreducible complex representations of G.) His study of this problem led him to introduce for the first time the notion of a character of a finite nonabelian group, which he defined as a conjugacy class function related to the number of solutions of the equation $ab = c$ where a, b, c run over elements in three conjugacy classes. For a description of this method, see [8, pp. 218–219] or [32, pp. 367–368]. His original notion of character only referred to irreducible ones. The following year would see Frobenius interpret characters as trace functions [23, p. 954]. The basic properties of irreducible characters, such as the orthogonality relations, were first proved without representations. A treatment in English of the group determinant and characters without representation theory was given by Dickson in his 1902 exposition [11] of Frobenius' work.

Rather than go through all of Frobenius' original proof of the factorization of $\Theta(G)$, which did not use representations, we will invoke representation theory in the next section to explain its decomposition.

However, to give a flavor of how Frobenius analyzed the group determinant, we prove a property of its irreducible factors by his techniques (Theorem 3 below). Recall $n = \#G$. We will abbreviate $\Theta(G)$ as Θ.

LEMMA 1. *The adjoint of the group matrix* $(X_{gh^{-1}})$ *has* (g, h) *entry* $(1/n)\, \partial\Theta/\partial X_{hg^{-1}}$.

Proof. Let D be the determinant of a matrix $(a_{g,h})$ doubly indexed by G and having independent entries, so D is a polynomial in $\mathbf{Z}[a_{g,h}]$. The adjoint of the matrix $(a_{g,h})$ is $(\partial D/\partial a_{h,g})$.

Let $\varphi\colon \mathbf{Z}[a_{g,h}] \to \mathbf{Z}[X_r]$ be the ring homomorphism where $\varphi(a_{g,h}) = X_{gh^{-1}}$. So $\varphi(D) = \Theta$, the group determinant. We want to show

$$\varphi\left(\frac{\partial D}{\partial a_{h,g}}\right) = \frac{1}{n}\frac{\partial \Theta}{\partial X_{hg^{-1}}}.$$

By the chain rule, or checking on monomials, for all f in $\mathbf{Z}[a_{g,h}]$ and r in G

$$\frac{\partial \varphi(f)}{\partial X_r} = \sum_{gh^{-1}=r} \varphi\left(\frac{\partial f}{\partial a_{g,h}}\right) = \sum_{k \in G} \varphi\left(\frac{\partial f}{\partial a_{g_0k,h_0k}}\right),$$

where (g_0, h_0) is any pair with $g_0h_0^{-1} = r$.

Let ψ_k be the ring automorphism of $\mathbf{Z}[a_{g,h}]$ where $\psi_k(a_{g,h}) = a_{gk,hk}$. Then $\varphi\psi_k = \varphi$, so

$$\frac{\partial\varphi(f)}{\partial X_r} = \sum_{k\in G} \varphi\psi_k\left(\frac{\partial\psi_k^{-1}f}{\partial a_{g_0,h_0}}\right) = \sum_{k\in G} \varphi\left(\frac{\partial\psi_k^{-1}f}{\partial a_{g_0,h_0}}\right) = \sum_{k\in G} \varphi\left(\frac{\partial\psi_k f}{\partial a_{g_0,h_0}}\right).$$

Now set $f = D$, and note $\psi_k(D) = D$. □

Letting $Y_r = (1/n)\,\partial\Theta/\partial X_{r^{-1}}$, we see the adjoint of $(X_{gh^{-1}})$ has the form $(Y_{gh^{-1}})$.

Polynomials in the X_g's can be viewed as functions on matrices of the form $x = (x_{gh^{-1}})$ or as functions on elements of the group algebra $x = \sum_g x_g g$. For example, viewing the group determinant Θ as such a function, it is multiplicative: $\Theta(xy) = \Theta(x)\,\Theta(y)$. The element xy has g-coordinate $\sum_{ab=g} x_a y_b$.

The next theorem, which appeared in [22, Sect. 1], shows the multiplicative property of Θ passes to its irreducible factors, and in fact characterizes them.

THEOREM 3. *Let Φ be a homogeneous irreducible polynomial in the variables X_g. Then $\Phi(xy) = \Phi(x)\,\Phi(y)$ if and only if Φ is monic in X_e and is a factor of Θ.*

Proof. First we assume Φ is monic in X_e and is a factor of Θ.

Choose indeterminates $\{X_g\}$ and $\{Y_g\}$. Let $Z_g = \sum_{ab=g} X_a Y_b$, so in $\mathbf{C}[X_g, Y_h]$ we have $\Theta(Z) = \Theta(X)\,\Theta(Y)$. Since $\Phi(Z) \mid \Theta(Z)$, $\Phi(Z) = \Lambda(X)\,M(Y)$ for some polynomials Λ in the X's and M in the Y's. Set $Y_e = 1$ and $Y_g = 0$ for $g \neq e$. We get $\Phi(X) = \Lambda(X)M(1,0,0,\dots)$. Similarly, $\Phi(Y) = \Lambda(1,0,0,\dots)M(Y)$. Therefore

$$\Phi(X)\,\Phi(Y) = \Phi(Z)\,\Lambda(1,0,0,\dots)\,M(1,0,0,\dots) = \Phi(XY)\,\Phi(1,0,0,\dots).$$

Since Φ is homogeneous and monic in X_e, $\Phi(1,0,0,\dots) = 1$.

Now assume Φ is multiplicative. Since Φ is homogeneous, we have $\Phi(X_e,0,0,\dots) = cX_e^d$. Letting $Y_e = 1$ and $Y_g = 0$ for $g \neq e$, we have $\Phi(X) = \Phi(X)\Phi(1,0,0,\dots)$, so $\Phi(1,0,0,\dots) = c = 1$, hence Φ is monic in X_e.

By Lemma 1, we can write the adjoint matrix of $(X_{gh^{-1}})$ in the form $(Y_{gh^{-1}})$. For this choice of the Y's, we have in $\mathbf{C}[X_g]$ that $\Phi(X)\,\Phi(Y) = \Phi(\Theta,0,0,\dots) = \Theta^d$, so $\Phi \mid \Theta$. □

The "if" direction did not need Φ to be irreducible. It can also be removed as a hypothesis in the "only if" direction by weakening the conclusion to Φ dividing a power of Θ.

Theorem 3 allowed Frobenius to establish a conjecture of Dedekind [10, p. 422], which said that the linear factors of Θ, monic in X_e, are related to the characters of the abelian group $G/[G,G]$. More precisely, Frobenius showed the linear factors of Θ, monic in X_e, are exactly the polynomials $\sum_g \chi(g)X_g$, where $\chi\colon G \to \mathbf{C}^\times$ is a character, and each such linear factor arises exactly once in the factorization of Θ. (Since we already showed such polynomials are factors, only the "if" direction of Theorem 3 is needed and therefore Lemma 1 is not required for this.) The reader is referred to the paper of Frobenius [22, Sect. 2] or Dickson [11, Sect. 6] for details of this argument.

It is of interest to see what is mentioned about the group determinant in Thomas Muir's *The Theory of Determinants in the Historical Order of Development*, which aimed to describe all developments in the subject up until 1900. In the preface to the final volume, Muir expresses the hope that "little matter of any serious importance has been passed over that was needed for this History." There are many references to the circulant, one to Dedekind's calculation of $\Theta(S_3)$, but there is no mention of any work on the group determinant by Frobenius. However, his List of Writings in the 1907 *Quart. J. Pure Appl. Math.* shows he was aware of such papers.

5. Factoring the group determinant by representation theory

We now use representation theory to completely factor the group determinant. As in the second proof of Theorem 2, let's compute the matrix for left multiplication in $\mathbf{C}[G]$ by an element $\sum a_g g$, with respect to the basis G of $\mathbf{C}[G]$. Since

$$\Big(\sum_g a_g g\Big)h = \sum_g a_{gh^{-1}} g\,,$$

the matrix for left multiplication by $\sum a_g g$ is $(a_{gh^{-1}})$. Hence

$$\det(a_{gh^{-1}}) = \mathrm{N}_{\mathbf{C}[G]/\mathbf{C}}\Big(\sum_g a_g g\Big)\,.$$

Since $\mathbf{C}[G]$ decomposes into a product of matrix algebras, this norm will decompose into a product of determinants. More specifically, let $\{(\rho, V_\rho)\}$ be a full set of mutually nonisomorphic irreducible representations of G (over the complex numbers). Then the map

$$\mathbf{C}[G] \to \prod_{\rho \text{ irred}} \mathrm{End}_{\mathbf{C}}(V_\rho),$$

given by

$$\sum_{g\in G} a_g g \mapsto \Big(\sum_{g\in G} a_g \rho(g)\Big)_{\rho \text{ irred}},$$

is an isomorphism of $\mathbf{C}$-algebras. Thus

$$\begin{aligned} \mathrm{N}_{\mathbf{C}[G]/\mathbf{C}}\Big(\sum_g a_g g\Big) &= \prod_{\rho \,\text{irred}} \mathrm{N}_{\mathrm{End}_{\mathbf{C}}(V_\rho)/\mathbf{C}}\Big(\sum_g a_g \rho(g)\Big) \\ &= \prod_{\rho\,\text{irred}} \det\Big(\sum_g a_g \rho(g)\Big)^{\deg(\rho)}. \end{aligned}$$

This last equation arises from the fact that in the endomorphism ring $\mathrm{End}(V)$ of an m-dimensional vector space V, left multiplication by an element is a linear map $\mathrm{End}(V) \to \mathrm{End}(V)$ whose determinant is equal to the m-th power of the usual determinant of the element. Therefore

$$\Theta(G) = \det(X_{gh^{-1}}) = \prod_{\rho \text{ irred}} \det\Big(\sum_g X_g \rho(g)\Big)^{\deg(\rho)}.$$

Note $\det(\sum_g X_g\rho(g))$ is a homogeneous polynomial of degree $\deg(\rho)$, monic in X_e.

We now show that the irreducible factors of $\Theta(G)$ (which are monic in X_e) can be put in a one-to-one correspondence with the irreducible representations of G by proving

THEOREM 4. *For an irreducible complex representation ρ of G,*

(i) *the polynomial* $\det(\sum_g X_g\rho(g))$ *is irreducible and*

(ii) *ρ is determined by* $\det(\sum_g X_g\rho(g))$.

We begin with a lemma originally due to Burnside [4].

LEMMA 2. *If (ρ, V) is an irreducible representation of G, then the $\mathbf{C}$-algebra map* $\mathbf{C}[G] \to \mathrm{End}_{\mathbf{C}}(V)$ *given by* $\sum_{g\in G} a_g g \mapsto \sum_{g\in G} a_g\rho(g)$ *is onto. That is, the transformations $\rho(g)$ linearly span* $\mathrm{End}_{\mathbf{C}}(V)$.

Proof. This map is basically a projection of $\mathbf{C}[G]$ onto one of its simple $\mathbf{C}[G]$-submodules, so it is onto. Alternatively, for a proof that works for representations over any algebraically closed field, even one with characteristic dividing the size of G, see [33]. □

LEMMA 3. *Let $\rho\colon G \to \mathrm{GL}_d(\mathbf{C})$ be a representation. Write*

$$\sum_{g\in G} X_g\rho(g) = (L_{ij}),$$

where the L_{ij}'s are linear polynomials in the X_g's. If ρ is irreducible then the L_{ij}'s are linearly independent over $\mathbf{C}$.

Proof. By Lemma 2, any set of d^2 complex numbers (z_{ij}) arises as $\sum a_g\rho(g) = (L_{ij}(a_g))$ for some vector (a_g) in $\mathbf{C}^n$. So

$$\begin{aligned}\sum c_{ij}L_{ij} = 0 \text{ in } \mathbf{C}[X_g] &\Rightarrow \sum c_{ij}L_{ij}(a_g) = 0 \text{ for all } (a_g)\in\mathbf{C}^n\\ &\Rightarrow \sum c_{ij}z_{ij} = 0 \text{ for all } (z_{ij})\in\mathbf{C}^{d^2}\\ &\Rightarrow \text{all } c_{ij} = 0. \quad \square\end{aligned}$$

Proof of Theorem 4. (i) By Lemma 3, choose $n-\deg(\rho)^2$ homogeneous linear polynomials L_k such that $\{L_{ij}, L_k\}$ is a basis of the homogeneous linear polynomials in $\mathbf{C}[X_g]$. Then we can move between the sets $\{X_g\}$ and $\{L_{ij}, L_k\}$ by a linear change of variables. This gives a $\mathbf{C}$-algebra automorphism of $\mathbf{C}[X_g]$, so the set $\{L_{ij}, L_k\}$ consists of algebraically independent elements over $\mathbf{C}$. In particular,

$$\det\Bigl(\sum_{g\in G} X_g\rho(g)\Bigr) = \det(L_{ij})$$

is the determinant of a matrix whose entries are algebraically independent. It is a standard fact (see [36, p. 96] for an elementary proof) that such a determinant is irreducible in $\mathbf{C}[L_{ij}]$, so it is also irreducible if we append the extra algebraically independent variables $\{L_k\}$ to the ring, so this polynomial is irreducible in $\mathbf{C}[L_{ij}, L_k] = \mathbf{C}[X_g]$.

(ii) We need to show that ρ is determined by $\det(\sum X_g\rho(g))$. It is enough to show the corresponding character χ_ρ is determined, and that is what we will do.

The number $\chi_\rho(e)$ is the degree of the homogeneous polynomial $\det(\sum X_g\rho(g))$. For $h \neq e$, we will recover $\chi_\rho(h)$ as the coefficient of $X_e^{\deg(\rho)-1}X_h$. To see this, we ignore all variables besides X_e and X_h by setting X_g equal to 0 for $g \neq e, h$. Then our polynomial becomes $\det(X_eI + X_h\rho(h))$. We want to know the coefficient of $X_e^{\deg(\rho)-1}X_h$ in this polynomial. For any matrix A, the polynomial $\det(TI + A)$ in the variable T has second leading coefficient $\mathrm{Tr}(A)$. Apply this to $A = X_h\rho(h)$, whose trace is $\chi_\rho(h)X_h$. $\square$

Let's work through the proof of Theorem 4(i) in a case we've already seen, $G = S_3$. Recall

$$\pi_1 = (1),\ \pi_2 = (123),\ \pi_3 = (132),\ \pi_4 = (23),\ \pi_5 = (13), \pi_6 = (12).$$

Let $\rho\colon S_3 \to \mathrm{GL}(V)$ be the irreducible 2-dimensional representation on

$$V = \{(z_1, z_2, z_3) \in \mathbf{C}^3 : z_1 + z_2 + z_3 = 0\},$$

given by permutation of the cooordinates. Using $(1,0,-1),(0,1,-1)$ as an ordered basis of V, we get the matrix realizations

$$[\rho(\pi_1)] = \begin{pmatrix} 1 & 0 \\ 0 & 1 \end{pmatrix}, \quad [\rho(\pi_2)] = \begin{pmatrix} -1 & -1 \\ 1 & 0 \end{pmatrix}, \quad [\rho(\pi_3)] = \begin{pmatrix} 0 & 1 \\ -1 & -1 \end{pmatrix},$$
$$[\rho(\pi_4)] = \begin{pmatrix} 1 & 0 \\ -1 & -1 \end{pmatrix}, \quad [\rho(\pi_5)] = \begin{pmatrix} -1 & -1 \\ 0 & 1 \end{pmatrix}, \quad [\rho(\pi_6)] = \begin{pmatrix} 0 & 1 \\ 1 & 0 \end{pmatrix}.$$

Therefore

$$(5.1) \qquad \sum_{i=1}^{6} X_i[\rho(\pi_i)] = \begin{pmatrix} X_1 - X_2 + X_4 - X_5 & -X_2 + X_3 - X_5 + X_6 \\ X_2 - X_3 - X_4 + X_6 & X_1 - X_3 - X_4 + X_5 \end{pmatrix},$$

which tells us what the L_{ij} in Lemma 3 are, $1 \leq i, j \leq 2$. Taking the determinant of the right hand side of (5.1) gives an expression $ad - bc$ for the factor Φ_3 of $\Theta(S_3)$ where a, b, c, d are linear polynomials with integer coefficients (such an expression was given by Dickson in [14, Eq. 2]). In the expression of Dedekind's for Φ_3 which we saw earlier, a, b, c, and d had coefficients involving cube roots of unity. The fact that we can get integer coefficients is related to the 2-dimensional irreducible representation of S_3 being realizable in $\mathrm{GL}_2(\mathbf{Z})$. In general, the irreducible factors of $\Theta(S_n)$ have integer coefficients since all irreducible representations of S_n are defined over the rational numbers.

As a basis of the linear forms in $\mathbf{C}[X_i]$ we use the L_{ij} and matrix entries of all $\sum X_i\rho'(\pi_i)$ where ρ' runs over irreducible representations of S_3 not isomorphic to ρ. These are the trivial and sign representations, which yield $L_1 = X_1 + X_2 + X_3 + X_4 + X_5 + X_6$ and $L_2 = X_1 + X_2 + X_3 - X_4 - X_5 - X_6$, so we can also use $X_1 + X_2 + X_3$ and $X_4 + X_5 + X_6$. These are essentially elements Dedekind came across when factoring $\Theta(S_3)$ into linear factors in some hypercomplex number system. Compare this means of manufacturing $\pi_1 + \pi_2 + \pi_3$ and $\pi_4 + \pi_5 + \pi_6$ with Dedekind's calculation.

As an illustration of the proof of Theorem 4(ii), the quadratic irreducible factor of $\Theta(S_3)$ corresponds to the irreducible 2-dimensional representation of S_3, and its coefficients of X_1X_i for $2 \leq i \leq 6$ (some of which are zero) coincide with the character values at π_i.

The proof given for Frobenius' theorem on the factorization of $\Theta(G)$ can be adapted to show that for any finite-dimensional complex representation ρ of G, the *determinant attached to* ρ, namely

$$\Theta_\rho(G) = \det\Bigl(\sum_{g \in G} X_g \rho(g)\Bigr),$$

decomposes into homogeneous irreducible factors (monic in X_e) in accordance with the decomposition of ρ into irreducible representations. Frobenius' theorem on the group determinant involves the regular representation.

In Frobenius' initial work on the group determinant, he felt the most remarkable (and difficult to prove) feature of the factorization was that the degree of each irreducible factor coincides with its multiplicity as a factor. We recognize this feature as a familiar statement about the multiplicity of irreducible representations in the regular representation.

Since every factor (monic in X_e) of the group determinant has the form $\det(\sum_g X_g\rho(g))$ for some representation ρ, the "if" direction of Theorem 3 gets a second proof from the definition of a representation and the multiplicativity of determinants.

According to Hawkins [26, 27], Frobenius' original approach to characters of G (which is not the first one that appeared in print) was as follows. Let Φ be an irreducible factor of $\Theta(G)$ which is monic in X_e and of degree d. Define the associated character χ by letting $\chi(g)$ be the coefficient of X_e^{d-1} in $\partial\Phi/\partial X_g$. This is equivalent to the description we gave in the proof of Theorem 4(ii), except that we speak of the character attached to an irreducible representation of G while Frobenius (at first) spoke of the character attached to an irreducible factor of the group determinant of G.

Here is another point of view that Frobenius had on characters. Let Φ be an irreducible factor of the group determinant of G, monic in X_e and of degree d. We regard Φ as a function $\mathbf{C}[G] \to \mathbf{C}$ by $\sum a_g g \mapsto \Phi(a_g)$. Let $x = \sum a_g g \in \mathbf{C}[G]$. For a variable u, set

$$\Phi(x + ue) = u^d + C_1u^{d-1} + \cdots + C_d, \tag{5.2}$$

where C_i is a polynomial function of the a_g's which is homogeneous of degree i. In particular, C_1 is a linear homogeneous polynomial of the a_g's. Frobenius observed in [22, p. 1360] that its coefficients are the values of the character χ corresponding to Φ : $C_1 = \sum_g \chi(g)a_g$. Since (5.2) is essentially a characteristic polynomial, so C_1 is basically a trace, the connection Frobenius eventually found between characters and traces is not surprising.

In [22], Frobenius explicitly showed how *all* the coefficients of an irreducible factor of the group determinant can be expressed explicitly in terms of its corresponding character. We will show more generally that for any (complex) representation ρ of G, irreducible or not, the coefficients of $\det(\sum X_g \rho(g))$ can be expressed in terms of χ_ρ. Our discussion is based on the matrix formula (5.3) below, which we now explain.

For $N \geq 1$ and $\sigma \in S_N$ consisting of disjoint cycles of length $N_1, \ldots, N_r$, define a trace map $\operatorname{Tr}_\sigma \colon \mathrm{M}_d(\mathbf{C}) \to \mathbf{C}$ by $\operatorname{Tr}_\sigma(A) = \operatorname{Tr}(A^{N_1}) \cdot \ldots \cdot \operatorname{Tr}(A^{N_r})$. For example, $\operatorname{Tr}_{(1)(2)\ldots(N)}(A) = (\operatorname{Tr} A)^N$, $\operatorname{Tr}_{(1,\ldots,N)}(A) = \operatorname{Tr}(A^N)$, and $\operatorname{Tr}_\sigma(I_d) = d^r$. If σ and τ are conjugate in S_N, they have the same cycle structure (and vice versa), so $\operatorname{Tr}_\sigma = \operatorname{Tr}_\tau$. Note Tr_σ is typically not linear.

For our application, we set $N = d$. We will prove that for $A \in \mathrm{M}_d(\mathbf{C})$,

$$\det(A) = \frac{1}{d!} \sum_{\sigma \in S_d} \operatorname{sgn}(\sigma) \operatorname{Tr}_\sigma(A). \tag{5.3}$$

A formula equivalent to (5.3) was used by Frobenius in [22, Sect. 3, Eq. 8].

For example, when $d = 2$ let A have eigenvalues λ and μ. The right hand side is

$$\frac{1}{2}\left((\operatorname{Tr} A)^2 - \operatorname{Tr}(A^2)\right) = \frac{1}{2}\left((\lambda + \mu)^2 - (\lambda^2 + \mu^2)\right) = \lambda\mu = \det(A).$$

To prove (5.3), let $\lambda_1, \ldots, \lambda_d$ be the eigenvalues of A, repeated with multiplicity. For $k \geq 1$, let $s_k = \lambda_1^k + \cdots + \lambda_d^k$.

If σ has m_1 1-cycles, m_2 2-cycles, and so on, then $m_1 + 2m_2 + \cdots + dm_d = d$ and $\operatorname{sgn}(\sigma) = \prod_k \left((-1)^{k-1}\right)^{m_k}$. Since $\sum k m_k = d$, $\operatorname{sgn}(\sigma) = (-1)^{d - \sum_k m_k}$. Also, $\operatorname{Tr}_\sigma(A) = s_1^{m_1} s_2^{m_2} \cdot \ldots \cdot s_d^{m_d}$. Therefore

$$\operatorname{sgn}(\sigma) \operatorname{Tr}_\sigma(A) = (-1)^d \prod_{k=1}^{d} (-1)^{m_k} s_k^{m_k}.$$

If σ and τ have the same cycle structure, $\operatorname{sgn}(\sigma) \operatorname{Tr}_\sigma(A) = \operatorname{sgn}(\tau) \operatorname{Tr}_\tau(A)$. For our evaluation of

$$\frac{1}{d!} \sum_{\sigma \in S_d} \operatorname{sgn}(\sigma) \operatorname{Tr}_\sigma(A),$$

we want to collect all the terms corresponding to permutations with the same cycle structure. The permutations in S_d having a cycle structure with m_1 1-cycles, m_2 2-cycles, and so on form a conjugacy class whose size is $d!/\prod_{k=1}^{d} k^{m_k} \cdot m_k!$. Thus

$$\frac{1}{d!}\sum_{\sigma\in S_d}\operatorname{sgn}(\sigma)\operatorname{Tr}_\sigma(A)=\frac{1}{d!}\sum_{\substack{m_1,m_2,\dots\geq 0\\ m_1+2m_2+\dots=d}}(-1)^d d!\prod_{k=1}^{d}\frac{(-1)^{m_k}s_k^{m_k}}{k^{m_k}m_k!}$$
$$=(-1)^d\sum_{\substack{m_1,m_2,\dots\geq 0\\ m_1+2m_2+\dots=d}}\prod_{k=1}^{d}\frac{(-1)^{m_k}s_k^{m_k}}{k^{m_k}m_k!}.$$

We want to show this equals $\lambda_1\cdot\ldots\cdot\lambda_d$. To do this, we use generating functions:

$$\sum_{i\geq 0}\Big(\sum_{\substack{m_1,m_2,\dots\geq 0\\ m_1+2m_2+\dots=i}}\prod_{k=1}^{d}\frac{(-1)^{m_k}s_k^{m_k}}{k^{m_k}m_k!}\Big)t^i=\sum_{i\geq 0}\sum_{\substack{m_1,m_2,\dots\geq 0\\ m_1+2m_2+\dots=i}}\prod_{k=1}^{d}\frac{(-1)^{m_k}(s_kt^k)^{m_k}}{k^{m_k}m_k!}$$
$$=\prod_{k=1}^{d}\sum_{m_k\geq 0}\Big(\frac{-s_kt^k}{k}\Big)^{m_k}\frac{1}{m_k!}=\prod_{k=1}^{d}e^{-s_kt^k/k}$$
$$=\exp\Big(-\sum_{k=1}^{d}\frac{s_kt^k}{k}\Big)=\exp\Big(-\sum_{j=1}^{d}\sum_{k=1}^{d}\frac{\lambda_j^kt^k}{k}\Big)$$
$$=\prod_{j=1}^{d}\exp\Big(-\sum_{k=1}^{d}\lambda_j^kt^k/k\Big)\equiv\prod_{j=1}^{d}\exp(\log(1-\lambda_jt))\mod t^{d+1}$$
$$\equiv\prod_{j=1}^{d}(1-\lambda_jt)\mod t^{d+1}.$$

The coefficient of t^d here is $(-1)^d\lambda_1\cdot\ldots\cdot\lambda_d$, as desired.

More generally, for $N\geq 1$ and $A\in M_d(\mathbf{C})$, the coefficient of t^N in $\prod_{j=1}^{d}(1-\lambda_jt)$ is $(-1)^N\operatorname{Tr}(\bigwedge^N A)$, so by an argument similar to the one above,

$$\operatorname{Tr}\Big(\bigwedge^N A\Big)=(-1)^N\sum_{\substack{m_1,m_2,\dots\geq 0\\ m_1+2m_2+\dots=N}}\prod_{k=1}^{N}\frac{(-1)^{m_k}s_k^{m_k}}{k^{m_k}m_k!}=\frac{1}{N!}\sum_{\sigma\in S_N}\operatorname{sgn}(\sigma)\operatorname{Tr}_\sigma(A).$$

It is interesting to write (5.3) using the classical definition of the determinant of the $d\times d$ matrix (a_{ij}):

$$\sum_{\sigma\in S_d}\operatorname{sgn}(\sigma)a_{1\sigma(1)}a_{2\sigma(2)}\cdot\ldots\cdot a_{d\sigma(d)}=\frac{1}{d!}\sum_{\sigma\in S_d}\operatorname{sgn}(\sigma)\operatorname{Tr}_\sigma((a_{ij})).$$

Although these sums are both taken over S_d, the addends corresponding to the same permutation σ are typically not equal. For instance, for a diagonal matrix the left hand side has only one nonzero term while the right hand side has many nonzero terms.

Let's apply (5.3) to representation theory. It says that for a d-dimensional representation ρ of G,

$$\det\Bigl(\sum_{g\in G} X_g\rho(g)\Bigr) = \frac{1}{d!}\sum_{\sigma\in S_d}\operatorname{sgn}(\sigma)\operatorname{Tr}_\sigma\Bigl(\sum_{g\in G} X_g\,\rho(g)\Bigr)$$
$$= (-1)^d \sum_{\substack{m_1,m_2,\dots\geq 0\\ m_1+2m_2+\dots=d}} \prod_{k=1}^{d} \frac{(-1)^{m_k}}{k^{m_k}m_k!}\left(\operatorname{Tr}\Bigl(\Bigl(\sum_g \rho(g)X_g\Bigr)^k\Bigr)\right)^{m_k}.$$

which equals

$$(-1)^d \sum_{\substack{m_1,m_2,\dots\geq 0\\ m_1+2m_2+\dots=d}} \prod_{k=1}^{d} \frac{(-1)^{m_k}}{k^{m_k}m_k!}\Bigl(\sum_{(g_1,\dots,g_k)\in G^k}\chi_\rho(g_1\cdot\ldots\cdot g_k)X_{g_1}\cdot\ldots\cdot X_{g_k}\Bigr)^{m_k}.$$

So all coefficients can be expressed in terms of χ_ρ. For the connection between the coefficients and the higher characters of ρ, see Johnson [30, p. 301].

In particular, if ρ is 1-dimensional then $\det\bigl(\sum X_g\rho(g)\bigr) = \sum\chi_\rho(g)X_g$. For 2-dimensional ρ,

$$\det\Bigl(\sum X_g\rho(g)\Bigr) = \frac{1}{2}\Bigl(\sum_{g\in G}\chi_\rho(g)X_g\Bigr)^2 - \frac{1}{2}\sum_{(g,h)\in G^2}\chi_\rho(gh)X_gX_h$$
$$= \frac{1}{2}\sum_{(g,h)\in G^2}(\chi_\rho(g)\chi_\rho(h) - \chi_\rho(gh))X_gX_h$$
$$= \frac{1}{2}\sum_g(\chi_\rho(g)^2 - \chi_\rho(g^2))X_g^2$$
$$+ \sum_{\{g,h\}\text{ unequal}}(\chi_\rho(g)\chi_\rho(h) - \chi_\rho(gh))\,X_gX_h.$$

To conclude this section, let's use the point of view developed here to factor the group determinant of D_8, the group of symmetries of the square (also denoted by some as D_4). We index the elements of D_8 as

$$g_1 = 1,\quad g_2 = (13)(24),\quad g_3 = (1234),\quad g_4 = (1432),$$
$$g_5 = (13),\quad g_6 = (24),\quad g_7 = (12)(34),\quad g_8 = (14)(23).$$

The conjugacy classes are

$$c_1 = \{1\}, \; c_2 = \{g_2\}, \; c_3 = \{g_3, g_4\}, \; c_4 = \{g_5, g_6\}, \; c_5 = \{g_7, g_8\}.$$

The character table of D_8 is

	c_1	c_2	c_3	c_4	c_5
χ_1	1	1	1	1	1
χ_2	1	1	1	-1	-1
χ_3	1	1	-1	1	-1
χ_4	1	1	-1	-1	1
χ_5	2	-2	0	0	0

Therefore $\Theta(\mathrm{D}_8) = \Phi_1\,\Phi_2\,\Phi_3\,\Phi_4\,\Phi_5^2$, where

$$\begin{aligned}
\Phi_1 &= X_1 + X_2 + X_3 + X_4 + X_5 + X_6 + X_7 + X_8\,,\\
\Phi_2 &= X_1 + X_2 + X_3 + X_4 - X_5 - X_6 - X_7 - X_8\,,\\
\Phi_3 &= X_1 + X_2 - X_3 - X_4 + X_5 + X_6 - X_7 - X_8\,,\\
\Phi_4 &= X_1 + X_2 - X_3 - X_4 - X_5 - X_6 + X_7 + X_8\,,\\
\Phi_5 &= \det\Big(\sum X_g \rho(g)\Big)\,.
\end{aligned}$$

where ρ is the 2-dimensional irreducible representation of D_8. So

$$\begin{aligned}
\Phi_5 &= \sum_g \frac{1}{2}(\chi_5(g)^2 - \chi_5(g^2))X_g^2 + \sum_{\{g,h\}\ \text{unequal}} (\chi_5(g)\chi_5(h) - \chi_5(gh))X_g X_h\\
&= X_1^2 + X_2^2 + X_3^2 + X_4^2 - X_5^2 - X_6^2 - X_7^2 - X_8^2\\
&\quad - 2X_1X_2 - 2X_3X_4 + 2X_5X_6 + 2X_7X_8\,.
\end{aligned}$$

Although Q_8 and D_8 have identical character tables, and all coefficients of an irreducible factor of the group determinant are determined by the corresponding character, the quadratic irreducible factors of $\Theta(\mathrm{Q}_8)$ and $\Theta(\mathrm{D}_8)$ are different. This illustrates that the determination of all coefficients of a factor from its character depends on the character as a function on group elements, not only on conjugacy classes.

6. THE GROUP DETERMINANT IN CHARACTERISTIC p

In 1902, six years after Frobenius began his work on $\Theta(G)$ and characters over the complex numbers, Dickson began studying these ideas over fields with characteristic p, perhaps as an outgrowth of his interest in finite fields and linear groups. As the variables x_g run over a field F, the matrices of the form $(x_{gh^{-1}})$ with nonzero determinant are a group under multiplication. Dickson was interested in the structure of this group, and its size when F is finite. In terms of the group algebra, this group is the unit group of $F[G]$, although Dickson did not use this point of view in his papers. He worked out examples for explicit groups in [12, 13, 14].

In [15] he examined $\Theta(G) \bmod p$ when $\#G$ is not divisible by p, indicating the case $p \mid \#G$ was quite different, illustrating some examples when $p \mid \#G$ in [16]. In 1907, Dickson presented a more general account of what happens in characteristic p, allowing for the possibility [17, 18] that $\#G$ is divisible by p. We will discuss some of Dickson's results in this section, although our proofs are not always the same as his.

First let's look at examples. We've already indicated how the group determinant of an abelian group factors in characteristic p. Let's factor $\Theta(S_3)$ over an algebraically closed field of characteristic p. Recall that

$$\Theta(S_3) = \Phi_1\Phi_2\Phi_3^2,$$

where

$$\begin{aligned}
\Phi_1 &= X_1 + X_2 + X_3 + X_4 + X_5 + X_6, \\
\Phi_2 &= X_1 + X_2 + X_3 - X_4 - X_5 - X_6, \\
\Phi_3 &= X_1^2 + X_2^2 + X_3^2 - X_4^2 - X_5^2 - X_6^2 \\
&\quad - X_1X_2 - X_1X_3 - X_2X_3 + X_4X_5 + X_4X_6 + X_5X_6.
\end{aligned}$$

Over the complex numbers, Φ_3 is an irreducible polynomial. Dedekind's proof of this uses primitive cube roots of unity, which exist in characteristic p for $p \neq 3$, in which case his proof still applies. For $p \neq 2$ we have $\Phi_1 \neq \Phi_2$, so except in characteristics 2 and 3, $\Theta(S_3)$ factors in characteristic p exactly as it does in characteristic 0. In characteristic 2 we get $\Phi_1 = \Phi_2$, so

$$\Theta(S_3) \equiv (\Phi_1\Phi_3)^2 \mod 2.$$

Unlike the factorization over $\mathbf{C}$, an irreducible factor in characteristic 2 appears with multiplicity not equal to its degree. Since

$$\Phi_1\Phi_2 = \Phi_3 + 3(X_1X_2 + X_1X_3 + X_2X_3 - X_4X_5 - X_4X_6 - X_5X_6),$$

in characteristic 3 we have

$$\Theta(S_3) \equiv (\Phi_1\Phi_2)^3 \mod 3\,.$$

Again we have irreducible factors appearing with multiplicity not equal to their degree.

From now on, F denotes a characteristic p algebraically closed field (except in Theorem 7).

If $p \nmid \#G$, then $F[G]$ is semisimple, in which case the factorization of $\Theta(G)$ over F behaves just as over the complex numbers: irreducible factors (that are monic in X_e) are in bijection with irreducible representations of G in characteristic p and the multiplicity of an irreducible factor equals its degree. The proofs over $\mathbf{C}$ go through with no changes.

What if perhaps $p \mid \#G$?

First, note that Theorem 3 is still true in characteristic p, by the same proof. (The entries of the adjoint matrix as given in Lemma 1 make sense mod p since they are minors from the group matrix and are thus polynomials with integer coefficients.)

Therefore linear factors of $\Theta(G) \bmod p$ arise exactly as over the complex numbers, i.e. characters $\chi\colon G \to F^\times$ correspond to linear factors $\sum \chi(g)X_g$. The treatment of linear factors by Frobenius [22, Sect. 2] or Dickson [11, Sect. 6] applies in characteristic p to show all linear factors look like this and they all appear with the same multiplicity (which might be greater than 1). So the number of distinct linear factors of $\Theta(G) \bmod p$ is the p-free part of the size of $G/[G,G]$, as Dickson first noted in [18, Sect. 7].

To write down nonlinear irreducible factors of $\Theta(G)$ over F, we use Jordan-Hölder series instead of the (possibly false) complete reducibility of the regular representation of G over F. This works for any F-representation space (ρ, V) of G, so we work in this setting.

Consider the factor modules appearing in a Jordan-Hölder series of V as an $F[G]$-module:

$$0 = V_0 \subset V_1 \subset \cdots \subset V_r = V\,,$$

where each V_i is an $F[G]$-submodule and V_i/V_{i-1} is a simple $F[G]$-module. Viewing $\sum a_g g \in F[G]$ as an F-linear operator $V \to V$, it induces endomorphisms of each V_i/V_{i-1} $(1 \le i \le r)$ and

$$\det\Big(\sum a_g\,\rho(g)\Big) = \prod_{i=1}^{r} \det\Big(\sum a_g \rho(g)\Big|_{V_i/V_{i-1}}\Big)\,. \tag{6.1}$$

Therefore the determinant attached to ρ, $\Theta_\rho(G)$, factors into a product of determinants attached to the simple constituents of a Jordan-Hölder series for V as an $F[G]$-module. A representation and its semisimplification have identical group determinants.

We have seen before that an abelian p-group has mod p group determinant equal to $(\sum X_g)^{\#G}$. Let's generalize this to any finite p-group [17, Sect. 5].

THEOREM 5. *Let G be a finite p-group, $\rho\colon G \to \mathrm{GL}(V)$ a mod p representation of G. Then*

$$\Theta_\rho(G) = \Big(\sum_g X_g\Big)^{\dim(V)}.$$

In particular, $\Theta(G) = (\sum X_g)^{\#G}$.

Proof. The only irreducible representation in characteristic p of a p-group is the trivial representation. For the trivial representation of G, $\sum a_g g$ acts like multiplication by $\sum a_g$, so the determinant of this action is $\sum a_g$. Now use (6.1). □

To show the determinant attached to an irreducible representation over F is an irreducible polynomial, we follow Dickson [18, Sect. 5] and begin by extending Lemma 2.

LEMMA 4. *If (ρ, V) is an irreducible representation of G over any algebraically closed field, then the transformations $\rho(g)$ linearly span* $\mathrm{End}(V)$.

Proof. The second proof of Lemma 2 is valid in this setting. □

COROLLARY 1. *If (ρ, V) is an irreducible representation of G over any algebraically closed field, then its character is not identically zero.*

Proof. Assume $\chi_\rho(g) = 0$ for all $g \in G$. Then $\mathrm{Tr}(\sum a_g\rho(g)) = 0$ for all scalars a_g. By Lemma 4, the trace is identically zero, which is false. □

THEOREM 6. *If (ρ, V) is an irreducible representation of G over any algebraically closed field, then*

(i) $\Theta_\rho(G) = \det(\sum_g X_g\rho(g))$ *is an irreducible polynomial and*

(ii) ρ *is determined by* $\Theta_\rho(G)$.

Proof. The proof of Theorem 4(i) applies to any algebraically closed field. The same is true of Theorem 4(ii), because absolutely irreducible representations are determined by their character and irreducibility is the same as absolute irreducibility over an algebraically closed field. □

If a representation ρ of G is reducible, then $\Theta_\rho(G)$ is a reducible polynomial, by (6.1).

Applying (6.1) and Theorem 6 to the regular representation, we see that even in characteristic p, irreducible factors of the group determinant (monic in X_e) are in bijection with irreducible representations.

To be accurate, the second part of Theorem 6 was not stated by Dickson, but he did write about a related issue. In [18, Sect. 5] he noted that over **C** Frobenius "gives a method of determining all the coefficients of Φ in terms of the [corresponding] characters $\chi(R)$". Here Φ is the determinant attached to an irreducible representation. We illustrated such a formula earlier. Dickson added that "The method must be modified in the case of a modular field." The formula over **C** breaks down mod p when the degree of the representation is greater than or equal to p.

Dickson never indicated that he had a general modified method, but he worked out explicit formulas for coefficients of irreducible factors of degree 2 in the group determinant mod 2, and of degree 3 in the group determinant mod 2 and mod 3, in terms of the corresponding character.

Here is an example of one of his formulas. Let ρ be a 2-dimensional representation of G. Set

$$A = \sum_g X_g \rho(g), \quad \det(A - uI_2) = u^2 + \Phi_1 u + \Phi_2,$$

where $\Phi_1 = \sum_g \chi(g) X_g$ and $\Phi_2 = \Theta_\rho(G)$, say

$$\Phi_2 = \sum_{g \leq h} c_{g,h} X_g X_h .$$

The ordering on G is introduced to avoid repeating monomials. Our task is to find a formula for $c_{g,h}$ when ρ is irreducible.

Dickson [18, p. 483] used the Newton identities relating the symmetric functions and the power sums in the eigenvalues of A to show in all characteristics that

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

for $g < h$,

$$\chi(g)c_{g,g} = \chi(g)\chi(g^2) - \chi(g^3),$$

and

$$\chi(h)c_{g,g} = -3\chi(g^2h) + 3\chi(g)\chi(gh) + \chi(g^2)\chi(h) - \chi(g)^2\chi(h),$$

for $g \neq h$. To compute $c_{g,h}$ for a characteristic 2 representation, view our task first as a problem in matrices with indeterminate entries over the integers (with

ρ replaced by any such 2×2 matrix-valued function on G, not necessarily multiplicative), so we can cancel the 2 on both sides of the first formula and then reduce mod 2, thus getting a valid formula for $c_{g,h}$ when $g < h$. By Corollary 1, χ is not identically zero, so the last two equations suffice to determine $c_{g,g}$. In characteristic 2, we get the formula

$$c_{g,g} = \frac{\chi(g^2h) + \chi(g)\chi(gh)}{\chi(h)},$$

for any h in G with $\chi(h) \neq 0$.

Looking back at the example of the factorization of $\Theta(S_3)$ in characteristics 2 and 3, we saw that irreducible factors do not appear with multiplicity equal to their degree. This is a general phenomenon first proven by Dickson in [17]. His arguments involve binomial coefficient manipulations (coming from a change of variables in the group matrix), which we will replace with the language of induced representations.

Let T be the trivial representation space in characteristic p for a group G. The regular representation of G is $\mathrm{Ind}_{\{1\}}^G(T)$. For a p-Sylow subgroup H of G,

$$\mathrm{Ind}_{\{1\}}^G(T) = \mathrm{Ind}_H^G(\mathrm{Ind}_{\{1\}}^H(T)).$$

THEOREM 7. *If G is a finite group, H a subgroup, F a field, and W_1 and W_2 are F-representation spaces of H with the same Jordan-Hölder quotients, then $\mathrm{Ind}_H^G(W_1)$ and $\mathrm{Ind}_H^G(W_2)$ are F-representation spaces of G with the same Jordan-Hölder quotients.*

Proof. Using a decomposition of G into left H-cosets, $F[G]$ is a free right $F[H]$-module, so the operation $\mathrm{Ind}_H^G(\cdot) = F[G] \otimes_{F[H]} (\cdot)$ is an exact functor. Therefore $\mathrm{Ind}_H^G(W_1)$ and $\mathrm{Ind}_H^G(W_2)$ admit decomposition series with isomorphic quotients, so their refinements to Jordan-Hölder series have isomorphic quotients. □

Let $\#G = p^r m$, where m is not divisible by p. Any representation in characteristic p of the p-Sylow subgroup H of G has Jordan-Hölder quotients which are all equal to the trivial representation, so by Theorem 7 the Jordan-Hölder quotients of $\mathrm{Ind}_{\{1\}}^G(T)$ coincide with those of

$$\mathrm{Ind}_H^G\left(\bigoplus_{i=1}^{p^r} T\right) = \bigoplus_{i=1}^{p^r} \mathrm{Ind}_H^G(T).$$

Since $\operatorname{Ind}_H^G(T)$ is the permutation representation of G on the left cosets of H, we have in characteristic p that

$$(6.2) \qquad \Theta(G) = D^{p^r},$$

where D is the determinant attached to the mod p permutation representation of G on the left cosets of a p-Sylow subgroup H of G. (I thank Ron Solomon and Pham Huu Tiep for showing me many G where this representation is not semisimple.)

Let's get an explicit formula for D. Denoting the left H-cosets of G by $g_1H, \dots, g_mH$, the space for this representation is $V = \bigoplus_{i=1}^m Fe_{g_iH}$ with the usual left G-action on the basis. For $g_j \in \{g_1, \dots, g_m\}$,

$$\Big(\sum_{s\in G} a_s s\Big) e_{g_jH} = \sum_{s\in G} a_s e_{sg_jH} = \sum_{s\in G} a_{sg_j^{-1}} e_{sH} = \sum_{i=1}^{m}\Big(\sum_{h\in H} a_{g_ihg_j^{-1}}\Big) e_{g_iH}.$$

Therefore

$$(6.3) \qquad D = \det\Big(\sum_{h\in H} X_{g_ihg_j^{-1}}\Big)_{1\le i,j\le m}.$$

Equations (6.2) and (6.3) constitute the theorem of Dickson in [17, Sect. 3], except he used right coset representatives. If p does not divide the size of G, then D is the group matrix and (6.2) becomes a tautology, with $p^r = 1$.

In [17, Sect. 10], Dickson indicated one way to possibly factor D. Let K be the normalizer of H in G. Then $\operatorname{Ind}_H^G(T) = \operatorname{Ind}_K^G(\operatorname{Ind}_H^K(T))$. The representation $\operatorname{Ind}_H^K(T)$ is the regular representation of K/H, a group whose size is prime to p, so this representation is semisimple in characteristic p. Decomposing this representation into irreducibles (each such factor has multiplicity equal to its degree), we get a corresponding factorization of D, although not necessarily into irreducible factors.

The study of modular representations remained largely unexplored after Dickson, until Brauer's work beginning in the 1930s. See Curtis [7] for a discussion of Brauer's ideas.

Brauer's initial papers contained some results having a bearing on the group determinant in characteristic p. For example, he gave his own proof of a consequence of equation (6.2), namely that every irreducible mod p representation of a group with size $p^r m$ (m prime to p) occurs as a composition factor of the regular representation with multiplicity divisible by p^r. And while Dickson did not examine the number of irreducible factors (monic in X_e) of the group determinant mod p, i.e. the number of nonisomorphic mod p

irreducible representations of a finite group, a theorem of Brauer says this number equals the number of conjugacy classes in the group consisting of elements with order prime to p.

7. RECENT RESULTS

Character tables do not provide a way to distinguish any two finite groups, in general. For example, for any prime p the two nonisomorphic nonabelian groups of order p^3 have the same character table. Can we find a computational tool extending the character table which will distinguish any two non-isomorphic finite groups? In 1991, Formanek and Sibley [19] showed that if there is a bijection between two groups G and H which converts $\Theta(G)$ to $\Theta(H)$, then G and H are isomorphic. Since the irreducible characters can be read off (in principle) from the factors of $\Theta(G)$, we see $\Theta(G)$ is one answer to the question. However, if $\#G$ is large then $\Theta(G)$ is too hard to compute. Is there something closer to the character table which works? Yes. See the articles of Hoehnke and Johnson [28, 29] and Johnson and Sehgal [31].

ACKNOWLEDGEMENTS. I thank T. Geisser, K. Khuri-Makdisi, T. Klenke, T. Y. Lam, A. Ofer, R. Pollack, J.-P. Serre, and R. Vakil for their assistance, and MSRI for its hospitality, where part of this was written.

REFERENCES

[1] ARTIN, E. Über eine neue Art von L-Reihen. *Math. Ann. 89* (1923), 89–108.

[2] BOREVICH, Z. I. and I. R. SHAFAREVICH. *Number Theory.* Academic Press, New York, 1966.

[3] BURNSIDE, W. On a property of certain determinants. *Mess. of Math. (N.S.) 23* (1894), 112–114.

[4] —— On the condition of reducibility of any group of linear substitutions. *Proc. London Math. Soc. (2) 3* (1905), 430–434.

[5] CATALAN, E. Recherches sur les déterminants. *Bulletins de l'Académie Royale des sciences, des lettres et des beaux-arts de Belgique 13* (1846), 534–555.

[6] CREMONA, L. Intorno ad un teorema di Abel. *Annali di Scienze matematiche e fisiche 7* (1856), 99–105.

[7] CURTIS, C. Representation theory of finite groups: from Frobenius to Brauer. *Math. Intelligencer 14* (1992), 48–57.

[8] CURTIS, C. and I. REINER. *Methods of Representation Theory, Vol. 1.* John Wiley & Sons, New York, 1981.

[9] DAVENPORT, H. Bases for finite fields. *J. London Math. Soc. 43* (1968), 21–39.

[10] DEDEKIND, R. *Gesammelte mathematische Werke, Vol. II.* Chelsea, New York, 1969.

[11] DICKSON, L.E. An elementary exposition of Frobenius' theory of group characters and group-determinants. *Ann. of Math. (2) 4* (1902), 25–49; also *Mathematical Papers, Vol. II.* Chelsea, New York, 1975, 737–761.

[12] —— The order of a certain senary linear group. *Amer. Math. Monthly 9* (1902), 149–152; also *Mathematical Papers, Vol. VI.* Chelsea, New York, 1983, 477–480.

[13] —— A matrix defined by the quaternion group. *Amer. Math. Monthly 9* (1902), 243–248; also *Mathematical Papers, Vol. I.* Chelsea, New York, 1975, 495–500.

[14] —— The groups defined for a general field by the rotation groups. *University of Chicago Decennial Publications 9* (1902), 35–51; also *Mathematical Papers, Vol. I.* Chelsea, New York, 1975, 397–411.

[15] —— On the group defined for any given field by the multiplication table of any given finite group. *Trans. Amer. Math. Soc. 3* (1902), 285–301; also *Mathematical Papers, Vol. II.* Chelsea, New York, 1975, 75–91.

[16] —— On the groups defined for an arbitrary field by the multiplication table of certain finite groups. *Proc. London Math. Soc. 35* (1903), 68–80; also *Mathematical Papers, Vol. VI.* Chelsea, New York, 1983, 176–188.

[17] —— Modular theory of group-matrices. *Trans. Amer. Math. Soc. 8* (1907), 389–398; also *Mathematical Papers, Vol. II.* Chelsea, New York, 1975, 251–260.

[18] —— Modular theory of group characters. *Bull. Amer. Math. Soc.* (2) *13* (1907), 477–488; also *Mathematical Papers, Vol. IV.* Chelsea, New York, 1975, 535–546.

[19] FORMANEK, E. and D. SIBLEY. The group determinant determines the group. *Proc. Amer. Math. Soc. 112* (1991), 649–656.

[20] FROBENIUS, F.G. Über vertauschbare Matrizen. *Sitzungsberichte der Königlich Preussischen Akademie der Wissenschaften zu Berlin* (1896), 601–614; also *Gesammelte Abhandlungen, Band II.* Springer-Verlag, New York, 1968, 705–718.

[21] —— Über Gruppencharaktere. *Sitzungsberichte der Königlich Preussischen Akademie der Wissenschaften zu Berlin* (1896), 985–1021; also *Gesammelte Abhandlungen, Band III.* Springer-Verlag, New York, 1968, 1–37.

[22] —— Über die Primfactoren der Gruppendeterminante. *Sitzungsberichte der Königlich Preussischen Akademie der Wissenschaften zu Berlin* (1896), 1343–1382; also *Gesammelte Abhandlungen, Band III.* Springer-Verlag, New York, 1968, 38–77.

[23] —— Über die Darstellung der endlichen Gruppen durch lineare Substitutionen. *Sitzungsberichte der Königlich Preussischen Akademie der Wissenschaften zu Berlin* (1897), 944–1015; also *Gesammelte Abhandlungen, Band III.* Springer Verlag, New York, 1968, 82–103.

[24] HAWKINS, T. The origins of the theory of group characters. *Arch. Hist. Exact Sci. 7* (1971), 142–170.

[25] —— Hypercomplex numbers, Lie groups, and the creation of group representation theory. *Arch. Hist. Exact Sci. 8* (1972), 243–287.

[26] —— New light on Frobenius' creation of the theory of group characters. *Arch. Hist. Exact Sci. 12* (1974), 217–243.

[27] —— The creation of the theory of group characters. *Rice University Studies 64* (1978), 57–71.

[28] HOEHNKE, H.-J. and K.W. JOHNSON. The 1-, 2-, and 3-characters determine a group. *Bull. Amer. Math. Soc. (N.S.) 27* (1992), 243–245.

[29] HOEHNKE, H.-J. and K.W. JOHNSON. k-characters and group invariants. *Comm. Algebra 26* (1998), 1–27.

[30] JOHNSON, K.W. On the group determinant. *Math. Proc. Cambridge Philos. Soc. 109* (1991), 299–311.

[31] JOHNSON, K.W. and S.K. SEHGAL. The 2-characters of a group and the group determinant. *European J. Combin. 16* (1995), 632–631.

[32] LAM, T.Y. Representations of finite groups: A hundred years. *Notices Amer. Math. Soc. 45* (1998), pp. 361–372, 465–474.

[33] —— A theorem of Burnside on matrix rings. *Amer. Math. Monthly 105* (1998), 651–653.

[34] LANG, S. *Cyclotomic Fields I and II.* Springer-Verlag, New York, 1990.

[35] LEDERMANN, W. The origin of group characters. *J. Bangladesh Math. Soc. 1* (1981), 35–43.

[36] SATAKE, I. *Linear Algebra.* Marcel Dekker, New York, 1975.

[37] SPOTTISWOODE, W. Elementary theorems relating to determinants. *J. Reine Angew. Math. 51* (1856), 209–271, 328–381.

[38] van der WAERDEN, B. L. *A History of Algebra.* Springer-Verlag, New York, 1985.

(Reçu le 27 avril 1998)

Keith Conrad

Department of Mathematics,
Ohio State University,
Columbus, OH 43210-1174
U. S. A.
e-mail: kconrad@math.ohio-state.edu