6. The group determinant in characteristic p

Objekttyp: **Chapter**

Zeitschrift: **L'Enseignement Mathématique**

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

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

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 $\mathbf{C}$ 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 $\mathbf{C}$ 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

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

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

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

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

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

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

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

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 $\mathrm{Ind}_H^G(T) = \mathrm{Ind}_K^G(\mathrm{Ind}_H^K(T))$. The representation $\mathrm{Ind}_H^K(T)$ 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.