3. The work of Dedekind

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

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

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*

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

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 $h \in G$,

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

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

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

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

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

Therefore the polynomials $\det(X_{gh^{-1}})$ and $\prod_{\chi\in\widehat{G}}\Big(\sum_{g\in G}\chi(g)X_g\Big)$ 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

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

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

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

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 $\mathbf{C}$. There is an obvious "hypercomplex" number system over which Φ_5 becomes a product of linear factors, namely the quaternions $\mathbf{H}$ (although $\mathbf{C}$ 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: