Zeitschrift: L'Enseignement Mathématique
Herausgeber: Commission Internationale de l'Enseignement Mathématique
Band: 44 (1998)
Heft: 3-4: L'ENSEIGNEMENT MATHÉMATIQUE

Artikel: THE ORIGIN OF REPRESENTATION THEORY
Autor: CONRAD, Keith
Kapitel: 2. Circulants
DOI: https://doi.org/10.5169/seals-63909

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

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

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

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

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.

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

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

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

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,

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

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

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

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

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