DEMONSTRATIO MATHEMATICA
Vol. XXIV No 1-2 1991

K. W. Johnson

SOME RECENT RESULTS ON QUASIGROUP DETERMINANTS

1. Introduction

In two previous papers the determinant of a latin square was discussed. This is a generalisation of the group determinant which led Frobenius to introduce group characters. To each latin square there is naturally associated a quasigroup and where this is a group the factorisation of the determinant is equivalent to the decomposition of the regular representation of the group into irreducible components. A theory of quasigroup characters has been discussed in [5]-[9] and thus a natural question to consider is that of whether the factors of the quasigroup determinant give rise to a "representation theory" which ties in with the characters, and which can provide a tool in quasigroup theory. However one may also view the determinant in a more combinatorial light, and in [4] results are given on the determinant associated to pair of latin squares.

Here some recent results are described. Questions which were raised in [3] brought some comments at the conference, and these comments are discussed along with other work in progress. Whereas in the group case the pattern of factorisation of the determinant is rigidly determined by the character degrees, this no longer remains true for a general quasigroup. It is therefore of interest to give a family of examples where the factorisation pattern while different from that in the group case is completely determined by the character theory. Such a family is given here, suggested by some of the results in Frobenius' original paper [2]. It is also shown how the knowledge of the factorisation of the determinant can provide help in calculating the character table for a quasigroup.

In [2] Frobenius gives a method to construct explicitly an irreducible factor of a group determinant, starting from the corresponding irreducible character. It would be very interesting to construct the irreducible factors of a latin square determinant directly, but such a goal appears to be very difficult to achieve. Here a construction is given which produces the canonical factor of the determinant of a latin square which corresponds to a basic character of the corresponding loop, starting from the knowledge of the corresponding representation of the its mapping group.

Throughout the work quasigroup determinant and latin square determinant are used interchangeably and the choice used is related to the context. Explicitly, if L is a latin square on the set $\Omega = \{1,\dots,n\}$ there corresponds a quasigroup $(Q_L,.)$ on the set $Q = \{q_1,\dots,q_n\}$ defined by $q_i \cdot q_j = q_k$ where $k = L(i,j)$ and conversely given a quasigroup $(Q,.)$ of order n an ordering of the underlying set as above can be used to define a latin square L_Q by $L(i,j) = k$ where $q_i \cdot q_j = q_k$. Different choices of the ordering of Q give different quasigroups or latin squares which lie in the same isotopy class, and which have equivalent determinants. It may be noted here that the determinant is an invariant of the corresponding 3-web.

2. Definitions, Problems and Examples

First some definitions in [3] and [4] are recalled for the convenience of the reader. Let L be a latin square of order n. The latin square matrix X_L is defined to be the $n \times n$ matrix with (i,j)th entry x_k where $k = L(i,j)$, and the latin square determinant Θ_L is defined to be $\det(X_L)$. It will also be convenient to refer to matrices Y_L, Z_L obtained by replacing x_k by y_k (resp.) z_k in X_L. If f and g are two elements of $\mathbb{C}[x_1,\dots x_n]$ define $(\equiv)$ by $f \equiv g$ if and only if $f(x_1,\dots,x_n) =$

$= \pm\, g(x_{\sigma(1)},\ldots x_{\sigma(n)})$ where σ is an element of S_n, the symmetric group on $\{1,\ldots,n\}$. The square L^t is defined by $L^t(i,j) = L(j,i)$. Then the relation $\mathcal{R}$ is defined on the set of latin squares of order n by $L_1\, \mathcal{R}\, L_2$ if and only if L_1 is either isotopic to L_2 or to L_2^t. In an analogous manner $\mathcal{R}$ can be defined on the class of loops of order n or the class of quasigroups of order n.

The following problem is raised in [3] in the form of a question.

<u>Problem 1</u>. Find a pair (L_1, L_2) of $n \times n$ latin squares which are not $\mathcal{R}$-related such that $\Theta_{L_1} \equiv \Theta_{L_2}$.

A suggestion was made at the conference that a generic way to produce examples of such pairs might be achieved as follows. Let L and M be latin squares such that L and M are not isotopic to L^t and M^t respectively. Define Q_1 to be the direct product $Q_L \times Q_M$ and Q_2 to be $Q_L \times Q_M^t$. Then a reasonable conjecture is that Θ_{Q_1} is equal Θ_{Q_2} to under the obvious identification of the underlying sets. However a computation was carried out for the smallest example where L and M have order 6 and it was found that $\Theta_{Q_1} \neq \Theta_{Q_2}$. It remains unknown whether $\Theta_{Q_1} \equiv \Theta_{Q_2}$.

Further searches have been made on squares of small orders in an attempt to produce a suitable pair of squares. Θ_Q was calculated for a representative from each $\mathcal{R}$-class of loops of order n which have the cyclic group C_4 as a homomorhic image but it was found that all such determinants were inequivalent under ($\equiv$).

It was also pointed out at the conference that Problem 1 is intimately connected to the theory of normed algebras. The author is indebted to Professor Hoenhke for this insight, which opens up an interesting line of research.

For a loop Q the loop matrix X_Q is defined by $X_Q(i,j) = x_{q_k}$ where $q_i(q_j\rho) = q_k$ and $q\rho$ is the right inverse of q, i.e. $q(q\rho) = e$. When Q is a group

(2.1) $$X_Q Y_Q = Z_Q$$

where

(2.2) $$z_q = \sum_{hk=q} x_h y_k .$$

It is shown in [3] that (2.1) is equivalent to the associativity condition for Q. However the results of Frobenius use only the identity

(2.3) $$\det(X_Q)\det(Y_Q)=\det(Z_Q).$$

The following problem was introduced in [3].

Problem 2. Find a non-associative loop Q such that (2.3) holds. This may be difficult. One may formulate the weaker version:

Problem 3. Find a loop Q such that

$$\det(X_Q)\det(Y_Q)\equiv\det(Z_Q).$$

3. Frobenius Extensions

Let $G = \{e,g_2,..,g_n\}$ be a finite group. Define the quasigroup $(Q,.)$ on the set $G \times \{0,1\}$ by

(3.1) $$(g,0).(h,0) = (gh,0) - (g,1).(h,1) \qquad (g,h)\in G,$$

(3.2) $$(g,1).(h,0) = (hg,1) - (g,0).(h,1) \qquad (g,h)\in G.$$

Then $(e,0)$ is an identity element and Q is a loop, the Frobenius extension of G. It will be denoted by G^F. Note that if G is commutative $G^F \approx G \times C_2$. Also note that the inverse of (g,ϵ) in Q is (g^{-1},ϵ) where $\epsilon = 0,1$. Now consider X_Q the loop matrix of Q, with rows and columns indexed by the elements of Q in the the order $(e,0)$, $(g_2,0),\ldots,(g_n,0)$, $(e,1),(g_2,1),\ldots,(g_n,1)$. The (i,j)th entry of X_Q is x_k where k is as follows:

$$k = (g_i,0)\ (g_j,0)^{-1}= (g_i g_j^{-1},0) \qquad i,j \le n,$$

$$k = (g_i,0)\ (g_{j-n},1)^{-1}= (g_{i-n}^{-1} g_i,1) \qquad i \le n, j > n,$$

$$k = (g_{i-n},1)\ (g_j,0)^{-1} = (g_j^{-1}g_{i-n},1) \qquad i > n, j \le n,$$

$$k = (g_{i-n},1)\ (g_{j-n},1)^{-1} = (g_{i-n}g_{j-n}^{-1},0) \qquad i,j > n.$$

To simplify the discussion y_g and z_g will be used to denote the elements $x_{(g,0)}$ and $x_{(g,1)}$ respectively. The matrix X_Q can then be written in the form

$$(3.3) \qquad X_Q = \begin{pmatrix} Y & Z^* \\ Z^* & Y \end{pmatrix}$$

where $Y(i,j) = y_{(g_i g_j^{-1})}$ and $Z^*(i,j) = z_{(g_j^{-1}g_i)}$.

Lemma 3.1. $\theta_Q = \det(Y+Z^*)\det(Y-Z^*)$.

Proof. This follows from (3.3) and the elementary result from determinant theory that $\det\begin{pmatrix} A & B \\ B & A\end{pmatrix} = \det(A+B)\det(A-B)$, where A and B are square matrices.■

There is an oblique proof of the following proposition in [2], § 10. The proof given here is much more direct.

Proposition 3.2. Let $F(\alpha)$ be the matrix $Y + \alpha Z^*$, where α is constant. Then $\det(F(\alpha))$ factors into distinct irreducible factors which are in 1:1 correspondence with the irreducible characters of G. If χ is an irreducible character of G, the corresponding factor φ_χ is of degree $(\chi(e))^2$ and $\det(F(\alpha)) = \Pi_\chi\, \varphi_\chi$.

Proof. Let $\mathcal{B}$ be basis $\{e, g_2^{-1}, \ldots, g_n^{-1}\}$ for $\mathbb{C}G$. Let $\overline{R}(g)$ and $\overline{L}(g)$ be the respective matrices of $R(g)$ and $L(g)$ with respect to $\mathcal{B}$. Then

$$Y = \sum_{g\in G} \overline{R}(g)y_g$$

and

$$Z^* = \sum_{g\in G} \overline{L}(g)z_g.$$

It is a well-known result that if $M(G)$ is the mapping group of G i.e.

$$M(G) = gp < L(g),\ R(g) : g\in G >$$

the irreducible constituents of the permutation matrix representation $\pi: R(g)\to\bar{R}(g)$, $L(g)\to\bar{L}(g)$ are in 1:1 correspondence with the irreducible representations of G (see [1], 2.7.). Moreover if ρ is an irreducible representation of G and ρ^* is the corresponding representation of $M(G)$ $\deg(\rho^*) = (\deg(\rho))^2$. Thus if the matrices $\bar{L}(g)$ and $\bar{R}(g)$ are decomposed into block diagonal matrices according to the splitting $\pi = \oplus\rho^*$, $F(\alpha)$ is decomposed into a block diagonal matrix and this produces a factorisation of $\det(F(\alpha))$ into factors φ^* in 1:1 correspondence with the ρ^* and with $\deg(\varphi^*)$ $= \deg(\rho^*)$. The proposition follows if it can be shown that each factor φ^* is irreducible and that the φ^* are all distinct. From results which are in Frobenius' initial papers the specialisation of φ^* obtained by inserting 0 for z_g, $g\in G$, in φ^* produces φ^f where φ is the factor of Θ_G corresponding to ρ (with suitable replacement of x_g by y_g) and f = $\deg(\varphi)$. Now Frobenius' results imply that inequivalent representations of G give distinct factors of Θ_G and thus the φ^* are all distinct. It remains to show that for $\bar{\rho}^*$ a matrix realisation of ρ^*

$$\varphi^* = \det\ (\sum_{g\in G} \bar{\rho}^*(R(g))y_g + \alpha \sum_{g\in G} \bar{\rho}^*(L(g))z_g)$$

is irreducible. Suppose that $\varphi^*=\varphi_1(\underline{y},\underline{z})\varphi_2(\underline{y},\underline{z})$ is a non-trivial factorisation. It follows that $\det(\sum_{g\in G} \bar{\rho}^*(R(g))y_g)$ and $\det(\sum_{g\in G} \bar{\rho}^*(L(g))z_g)$ factorise as $\varphi_1(\underline{y},\underline{0})\varphi_2(\underline{y},\underline{0})$ and $\varphi_1(\underline{0},\underline{z})\varphi_2(\underline{0},\underline{z})$ respectively. Thus

$$\det(\sum_{g\in G} \bar{\rho}^*(R(g))y_g)\ \det[(\sum_{g\in G} \bar{\rho}^*(L(g))z_g) =$$
$$= \det[(\sum_{g\in G} \bar{\rho}^*(R(g))y_g)\ (\sum_{g\in G} \bar{\rho}^*(L(g))z_g)]$$

has a non-trivial factorisation. But

$$(3.4)\qquad (\sum_{g\in G} \bar{\rho}^*(R(g))y_g)(\sum_{g\in G} \bar{\rho}^*(L(g))z_g) = (\sum_{g,h\in G} \bar{\rho}^*(R(g)L(h))y_g z_h.$$

Moreover if $y_g z_h$ is replaced by x_k where $k=R(g)L(h)$ the matrix $(\sum_{g\in G} \bar{R}(g)\bar{L}(h)y_g z_h$ becomes $|Z(G)|X_{M(G)}$. This follows from the exact sequence

$$0 \longrightarrow Z(G) \longrightarrow G \times G \longrightarrow M(G) \longrightarrow \{e\}.$$

Thus we have shown that the factor of $X_{M(G)}$ corresponding to ρ^* has a non-trivial factorisation, which leads to a contradiction since by Frobenius' theory it must be irreducible. Hence φ^* itself is irreducible and the proposition follows.■

It is now possible to give a complete description of the character table of Q. The conjugacy classes of Q are the orbits of the inner mapping group of Q. This is generated by the elements $R(x,y)$, $L(x,y)$, $T(x)$ of the mapping group of Q defined as follows:

$$R(x,y) = R(x)R(y)R(xy)^{-1},$$
$$L(x,y) = L(x)L(y)L(yx)^{-1},$$
$$T(x) = L(x)^{-1}R(x).$$

Direct calculations shows that the image of an element of Q of the from $(g,0)$ under any of the above generators is an element of the form $(h^{-1}gh,0)$. Thus the subset of Q of elements $(g,0)$ splits into conjugacy classes C_{io} where $C_{io}=\{(g,0),\ g\epsilon C_i,\ C_i$ a conjugacy class of G. If z is an element of Q of the form (g,1) the following describes the action of the above generators on z.

x	y	$zR(x,y)$	$zL(x,y)$
$(h,0)$	$(k,0)$	$k^{-1}h^{-1}khg,1)$	$(ghkh^{-1}k^{-1},1)$
$(h,0)$	$(k,1)$	$(hgkh^{-1}k^{-1},1)$	$k^{-1}h^{-1}kgh,1)$
$(h,1)$	$(k,0)$	$h^{-1}k^{-1}ghk,1)$	$(khgk^{-1}h^{-1},1)$
$(h,1)$	$(k,1)$	$k^{-1}h^{-1}kgh,1)$	$(hgkh^{-1}k^{-1},1)$.

Under the action of $T(x)$ the image of z is always of the form $(h^{-1}gh,1)$.

Thus the subset of Q of elements of the form $(g,1)$ splits into classes each having $|G|$ elements and descibed by

$C_g=\{(gg',1): g'\in G'\}$. Hence the total number of classes of Q is $t + |G/G'|$ where t is the class number of G.

Theorem 3.3. Let G be any finite group, let $Q = G^F$. The basic characters of Q are described as follows.

(a) Linear characters. Each linear character is obtained via the homomorphism $G^F \longrightarrow (G/G')^F$ by the "pullback" operation described in [7].

(b) Non-linear characters. To each non-linear character χ of G there corresponds a basic χ^* of Q with $\chi^*(g,0) = 2^{1/2}\chi(g)$ and $\chi^*(g,1) = 0$. All the non-linear characters of Q are obtained in this way.

Proof. The number of basic characters of Q is equal to the number of conjugacy classes (see[5]). Since the existence of the linear characters in (a) follows from the results in [7] and the fact that (G/G') is abelian the theorem will follow if it can be shown that the characters χ^* as described in (b) are basic characters and are all distinct.

As in the proof of Proposition 3.2, to each irreducible character χ of G there corresponds a unique irreducible factor φ_α of det $(Y+Z^*)$, and thus to χ there corresponds a factor φ of $\det(Y+Z^*)$. By Lemma 3.1. φ is an irreducible factor of Θ_Q. In [4] it is shown that each irreducible factor of Θ_Q corresponds to a unique basic character of Q. Denote the basic character corresponding to φ by χ^*. If in φ the variable z_i is set equal to 0 for all i then the factorisation reduces to that of the group matrix Y_G and thus $(\varphi_\chi)^{\deg(\chi)}$ is obtained where φ_χ is the irreducible factor of $\det(Y_G)$ which corresponds to χ in Frobenius' theory. Hence $\chi^*(g,0) = m\chi(g)$, m constant. This shows that distinct irreducible χ give rise to distinct χ^*.

We now compute the value of χ^* on an element of the form $(g,1)$. Each of the $2|G/G'|$ elements of G described in (a) has norm 1 on each element of Q. Therefore

$$\sum_{\psi \text{ linear}} |\psi(g,1)|^2 = 2|G/G'|.$$

But for fixed $(g,1)$ the normalization of the columns of the character table of Q gives

$$\sum_{\chi^* \in \mathrm{Bas}(Q)} |\chi^*(g,1)|^2 = |Q|/|G'| = 2|G/G'|.$$

This implies that if χ^* is a non-linear character as described in (b) then $\chi^*(g,1) = 0$. By the normalization of the rows of the character table of Q, $\chi^*(g,0) = (2)^{1/2}\chi(g)$. The theorem proved. ∎

4. The construction of the canonical factors of Θ_Q for an arbitrary loop Q

The correspondence between the basic characters of a loop Q and the canonical factors of Θ_Q is described in [4] and may be summarised as follows. If $\Gamma_1,\ldots,\Gamma_t$ are the conjugacy classes of Q and the reduced loop matrix X_R of Q is obtained by replacing x_g by x_{γ_i} whenever g lies in Γ_i, the determinant Θ_Q of X_R splits into linear factors, and there is a 1:1 correspondence between basic characters of Q and distinct linear factors of Θ_R. If φ is an irreducible factor of Θ_Q the corresponding factor φ_R of Θ_R is a power of a linear factor. The canonical factor φ_χ of Θ_Q which corresponds to basic character χ of Q consists of the product of those factors φ for which φ_R has the same linear factor. In fact this factor may be obtained directly from χ as $\sum[|\Gamma_i|\chi(\gamma_i)/(\deg(\chi))^{1/2}]x_\gamma$, the sum being over all classes Γ_i.

Now X_Q may be decomposed as $X_Q = \sum \pi_i x_{q_i}$, where π_i is the permutation matrix obtained from X_Q by substituting $x_{q_i}=1$, $x_{q_j}=0$ for $i \neq j$. The π_i correspond to the right maps of a loop Q^* which is not in general isotopic to Q but which has the property that $M(Q^*) \approx M(Q)$ as permutation groups. Now the π_i may be decomposed into block diagonal matrices according to the decomposition of the natural representation of $M(Q)$ into irreducible representations ψ_j. Thus there exists a non-singular matrix P such that

$$P^{-1}X_Q P = \begin{pmatrix} B_0 & & & \\ & B_1 & & 0 \\ 0 & & \ddots & \\ & & & B_t \end{pmatrix},$$

where B_j is a square matrix of size $\deg(\psi_j)$. Further, if the substitution $x_q = x_{\gamma_i}$ where $q \in \Gamma_i$ is made in B_j to produce $(B_j)_R$,

$$\det[B_j)_R] = (\Sigma\ \lambda(\gamma_i)x_{\gamma_i})^f, \tag{4.1}$$

where f the degree of ψ_j, and $\lambda(\gamma_i) = |\Gamma_i|\chi_j(\gamma_i)/f$. (This means that λ is the association scheme character corresponding to χ_j). The decomposition (4.1) ensures that $\det(B_j) = \varphi_j$ is the canonical factor of Θ_Q corresponding to ψ_j.

The following algorithm constructs the canonical factor $\det(B_j)$ from the character ψ_j and set $\{\pi_1,\ldots\pi_n\}$. For simplicity the subscript j is omitted. Let σ be an element of S_k. Write σ as a product of disjoint cycles

$$\sigma = (a_1\ldots a_{k_1})(b_1\ldots b_{k_2})(c_1\ldots c_{k_3})\ldots ,$$

where 1-cycles are included. Define the <u>trace function</u> $T_\sigma : M_f(\mathbf{C}) \longrightarrow \mathbf{C}$ by

$$T_\sigma(X_1,\ldots,X_k) = T(X_{a_1}\ldots X_{a_{k_1}})T(X_{b_1}\ldots X_{b_{k_2}})T(X_{c_1}\ldots X_{c_{k_3}})\ \ldots \tag{4.2}$$

where T is the usual trace. Define

$$\psi(\pi_1,\ldots,\pi_k) = \sum_{\sigma\in S} \operatorname{sign}(\sigma)T_\sigma(\psi(\pi_1),\ldots,\psi(\pi_k)). \tag{4.3}$$

Then

$$f!\varphi_\chi = \Sigma\ \psi(\pi_{i_1},\ldots,\pi_{i_f})x_{q_{i_1}}\ldots x_{q_{i_f}}$$

where the sum is over all f-tuples of $(q_{i_1},\ldots,q_{i_f})$ of Q.

This construction is similar to Frobenius' initial construction of the irreducible factors of a group determinant, but whereas in the group case the φ_χ factorises as the *f*th power of an irreducible factor in general the factorisation of φ_χ is more complicated.

REFERENCES

[1] E. Bannai, T. Ito: Algebraic Combinatorics I. Benjamin/ Cummings, Menlo Park, California 1984.

[2] G. Frobenius: Uber die Primfaktoren der Gruppen-determinante, S, Ber Akad. Wiss. Berlin (1896) 1343-1382.

[3] K. W. Johnson: Latin square determinants, in Algebraic, Extermal and Metric Combinatorics 1986, L.M.S. Lecture Notes 131 (1988) 146-154.

[4] K. W. Johnson: Latin square determinants II. Submitted for publication.

[5] K. W. Johnson, J. D. H. Smith: Characters of finite quasigroups, European J. Combinatorics 5, 1 (1984).

[6] K. W. Johnson, J. D. H. Smith: Characters of finite quasigroups II: induced characters, European J. Combinatorics 7 (2) (1984) 131-138.

[7] K. W. Johnson, J. D. H. Smith: Characters of finite quasigroups III, Quotients and fusion, European J. Combinatorics 10 (1989) 47-56.

[8] K. W. Johnson, J. D. H. Smith: Characters of finite quasigroups IV: products and superschemes, European J. Combinatorics 10 (1989) 257-263.

[9] K. W. Johnson, J. D. H. Smith: Characters of finite quasigroups V: linear characters, European J. Combinatorics 10 (1989) 449-456.

THE PENNSYLVANIA STATE UNIVERSITY, OGONTZ CAMPUS
Current address:
DEPARTMENT OF MATHEMATICS, IOWA STATE UNIVERSITY, 400 CARVER HALL, AMES, IA 50011, USA.
Received November 8, 1989.