Ann. Sci. Math. Québec **34** (2010), no 1, 37–61

RECIPROCITY LAWS FOR REPRESENTATIONS OF FINITE GROUPS

SUNIL CHEBOLU, JÁN MINÁČ AND CLIVE REIS

Dedicated to Professor Paulo Ribenboim who inspired us to read the masters and to dream.

RÉSUMÉ. Beaucoup d'articles ont été écrits sur les lois de réciprocité de la théorie des nombres et leurs liens avec les représentations des groupes. Dans cet article, nous poursuivrons l'étude de ces liens. En complète analogie avec les lois classiques de réciprocité de la théorie des nombres, nous obtenons une « loi de réciprocité » pour certaines représentations de produits semi-directs de deux groupes cycliques. En fait, nous montrons que la célèbre loi de réciprocité quadratique est une conséquence directe de notre théorème appliqué à un certain groupe spécifique. Une autre conséquence de notre théorème principal est de recouvrer un théorème classique de Sylvester. Le focus principal de cet article porte sur les constructions explicites de représentations sur des corps suffisamment petits. Nos recherches procurent une évidence supplémentaire qu'il y a encore des zones grises à explorer sur les ponts qui existent entre la théorie des nombres et les représentations des groupes, et ce, même à un niveau élémentaire.

ABSTRACT. Much has been written on reciprocity laws in number theory and on their connections with group representations. In this paper we explore more on these connections. We prove a "reciprocity law" for certain specific representations of semidirect products of two cyclic groups which is in complete analogy with classical reciprocity laws in number theory. In fact, we show that the celebrated quadratic reciprocity law is a direct consequence of our main theorem applied to a specific group. As another consequence of our main theorem we also recover a classical theorem of Sylvester. Our main focus is on explicit constructions of representations over sufficiently small fields. These investigations give further evidence that there is still much unexplored territory in connections between number theory and group representations, even at an elementary level.

1. Introduction

Let p and s be odd primes. Then the quadratic reciprocity law tells us how to find all finite fields $\mathbb{F}_s$ of s elements for which $\sqrt{p} \in \mathbb{F}_s$. (To anticipate the generalization we have in mind, we might say that $\sqrt{p}$ is *realizable* over $\mathbb{F}_s$.) Remarkably, whether or not $\sqrt{p}$ is realizable over $\mathbb{F}_s$ can be decided modulo $4p$ thus reducing a question concerning infinitely many fields to one which can be decided using only finitely many operations, namely, squarings. (See [Gau], [Ser1] or [Ser2].)

Reçu le 15 octobre 2009 et, sous forme définitive, le 26 décembre 2009.

It is known that reciprocity laws are intimately connected with representations of finite groups (see for example [Art], [Lan], [Tat].) However, we were unable to find in the literature a development of reciprocity laws for representations of finite groups themselves. In a recent preprint [BH], an extremely interesting connection between division algebras with involutions and automorphism groups associated with Shimura varieties is uncovered and used. Certain constructions employed in this paper have a similar flavor as in [BH]. Also, in [Lem], the field of definition of some representations of finite groups was studied in order to deduce statements about the ranks of class groups.

The main goal of this paper is to provide reciprocity laws for certain representations of a restricted family of metacyclic groups. More precisely, we define certain specific representations $\rho_s : G \to \operatorname{Aut} V_s$, where G is a fixed metacyclic group and V_s is a vector space over $\overline{\mathbb{F}}_s$, the algebraic closure of $\mathbb{F}_s$. We then show that the question of the realizability of ρ_s over a given finite extension field of $\mathbb{F}_s$ can be decided entirely in terms of the invariants of G and depends only on a finite number of computations. This provides a straightforward analogy to the classical reciprocity laws. Indeed, in Section 3 below, it will be seen that a judicious choice of group G and corresponding representation $\rho(G)$ yields the usual quadratic reciprocity law.

The connection between the representation $\rho(G)$ and the quadratic reciprocity law was discovered by D. R. Corro (see [Jac, pp. 320-325]). However this is used only to evaluate the square of Gauss's sum which is only part of the proof. To complete that part of the proof in which the reduction to a finite number of primes is achieved, a classical method due to Jacobi is used. This part is not difficult and is actually worked out in a simple way in [Ser2]. However the evaluation of the square of Gauss's sum though important, does not, on its own, accomplish the reduction from infinitely many to finitely many primes.

Some of the results we obtain could be arrived at using the notion of the Schur index of a representation which is always 1 when the field in question is finite and of characteristic coprime to $|G|$ (see [Dor]). However our approach has the merit of being quite elementary and, more importantly, constructive. Except for Section 4, the basic notions of representation theory as can be found in [Ser1] are more than enough. For Section 4 we refer the reader to [Rei]. All other background material concerning finite fields, Vandermonde and companion matrices and characteristic polynomials should be understandable to a good advanced undergraduate.

In this paper we believe that we have merely scratched the surface of a possibly rather general theory of reciprocity in the representations of finite groups. The style of this paper is influenced by Ribenboim's writing, and after his urging to read Euler, also writing of Euler which are full of examples, "naive questions" and exploration spirit.

2. Main results – Galois, Vandermonde and field of definition

Throughout we shall be concerned with split semidirect products of two cyclic groups. Thus in terms of generators and relations

$$G = \langle a, b \mid a^m = 1 = b^n, b^{-1}ab = a^k \rangle,$$

where the order of $k \pmod m$ divides n. Let s be an odd prime relatively prime to m and let ζ be a primitive m-th root of unity in $\overline{\mathbb{F}}_s$, the algebraic closure of the field $\mathbb{F}_s$ of s elements. We shall focus attention on the representation ρ^G induced from the representation $\rho : \langle a \rangle \to \overline{\mathbb{F}}_s^*$ defined by $\rho(a) = \zeta$. We first prove a simple proposition which, among other things, tells us under what circumstances ρ^G is irreducible over $\overline{\mathbb{F}}_s$.

Proposition 2.1. (1) *Let G, ρ and ρ^G be as above. Then ρ^G is irreducible over $\overline{\mathbb{F}}_s$ if and only if $|k|_m$, the order of k in the multiplicative group of units $\bmod m$, is equal to the order of b.*

(2) *If $|k|_m = t \neq n, n = tr$ and $(r, s) = 1$, then $\rho^G \approx \rho_0 + \rho_1 + \cdots + \rho_{r-1}$, where the ρ_i are irreducible pairwise inequivalent representations over $\overline{\mathbb{F}}_s$ and, relative to an appropriate basis $\mathcal{B}_i$,*

$$[\rho_i(a)]_{\mathcal{B}_i} = \begin{pmatrix} \zeta & 0 & \dots & 0 \\ 0 & \zeta^k & \dots & 0 \\ \vdots & \vdots & \ddots & \vdots \\ 0 & 0 & \dots & \zeta^{k^{t-1}} \end{pmatrix}; \quad [\rho_i(b)]_{\mathcal{B}_i} = \begin{pmatrix} 0 & 0 & 0 & \cdots & 0 & \eta_i^{-1} \\ 1 & 0 & 0 & \cdots & 0 & 0 \\ 0 & 1 & 0 & \cdots & 0 & 0 \\ \vdots & \vdots & \vdots & \ddots & \vdots & \vdots \\ 0 & 0 & 0 & \cdots & 1 & 0 \end{pmatrix}.$$

Here $\eta_i = \eta^i$, with $i = 0, 1, \dots, r-1$, and η is a primitive r-th root of unity in $\overline{\mathbb{F}}_s$.

Proof. Since $a = b^{-n}ab^n = a^{k^n}$, it follows that $k^n \equiv 1 \pmod m$ and so $|k|_m \mid n$. Let $M = \overline{\mathbb{F}}_s$ be the representation space of ρ and let $H = \langle a \rangle$. Then the representation space of ρ^G is $V = \overline{\mathbb{F}}_s G \otimes_{\overline{\mathbb{F}}_s H} M$. The set

$$\{b^i \otimes 1 \mid i = 0, 1, ..., n-1\}$$

is a basis of V. Setting $e_i = b^i \otimes 1$, for $i = 0, ..., n-1$, we have $be_i = e_{i+1}$, where the indices are taken modulo n, and

$$ae_i = ab^i \otimes 1 = b^i \otimes (a^{k^i} \cdot 1) = \zeta^{k^i} e_i.$$

We prove the sufficiency of (1) first. Assume therefore that $|k|_m = n$. Then $\{\zeta, \zeta^k, ..., \zeta^{k^{n-1}}\}$ is a set of n distinct elements. Let $\zeta_i = \zeta^{k^i}$ and let W be a nonzero G-invariant subspace of V. Let

$$f = c_v e_v + \cdots + c_{n-1} e_{n-1},$$

with $c_v \neq 0$, be a nonzero vector of W such that v is largest subject to $c_v \neq 0$ and $c_0 = c_1 = \cdots = c_{v-1} = 0$. Then $c_{n-1} \neq 0$, otherwise

$$bf = c_v e_{v+1} + \cdots + c_{n-2} e_{n-1} \in W - \{0\},$$

contradicting the maximality of v. Now

$$\zeta_v f = \sum_{j=v}^{n-1} \zeta_v c_j e_j \quad \text{and} \quad af = \sum_{j=v}^{n-1} \zeta_j c_j e_j,$$

and assume $v < n-1$. Then

$$af - \zeta_v f = \sum_{j=v+1}^{n-1} c_j(\zeta_j - \zeta_v) e_j$$

is a nonzero vector of W since $c_{n-1}(\zeta_{n-1}-\zeta_v)\neq 0$, contradicting maximality of v. Thus $v=n-1$ and so $e_{n-1}\in W$. It follows that $b^ie_{n-1}\in W$ for all i and so $W=V$, proving the irreducibility of V.

Next we prove (2) and indicate that the existence of one of the direct summands constructed does not depend on the existence of a primitive r-th root of unity in $\overline{\mathbb{F}}_s$. This will then also prove the necessity of (1).

Let $\mathcal{B}=\{e_0,e_1,...,e_{n-1}\}$, where the e_i are defined as above. Then we have a matrix of r blocks

$$[\rho^G(a)]_{\mathcal{B}}=\begin{pmatrix} A & 0 & \dots & 0\\ 0 & A & \dots & 0\\ \vdots & \vdots & \ddots & \vdots\\ 0 & 0 & \dots & A\end{pmatrix}\quad\text{with}\quad A=\begin{pmatrix}\zeta_0 & 0 & \dots & 0\\ \dots & \zeta_1 & \dots & 0\\ \vdots & \vdots & \ddots & \vdots\\ 0 & 0 & \dots & \zeta_{t-1}\end{pmatrix};$$

moreover,

$$[\rho^G(b)]_{\mathcal{B}}=\begin{pmatrix}0 & 0 & \cdots & 0 & 1\\ 1 & 0 & \cdots & 0 & 0\\ 0 & 1 & \cdots & \vdots & \vdots\\ \vdots & \vdots & \ddots & 0 & 0\\ 0 & 0 & \cdots & 1 & 0\end{pmatrix}.$$

Let η be a primitive r-th root of unity in $\overline{\mathbb{F}}_s$ and, for $0\leq i\leq r-1$ and $0\leq j\leq t-1$, let

$$v_{ij}=\sum_{\ell=0}^{r-1}\eta^{i\ell}e_{j+\ell t},$$

and set

$$W_i=\operatorname{span}\mathcal{B}_i,\quad\text{with }\mathcal{B}_i=\{v_{i0},v_{i1},\dots,v_{i,t-1}\}.$$

Now, for $0\leq j\leq t-2$,

$$\begin{cases} av_{ij} &= \zeta_j v_{ij},\\ bv_{ij} &= v_{i,j+1},\end{cases}$$

and

$$bv_{i,t-1}\;=\;\sum_{\ell=0}^{r-1}\eta^{i\ell}be_{t-1+\ell t}\;=\;\sum_{\ell=0}^{r-1}\eta^{i\ell}e_{t(\ell+1)}\;=\;\eta^{-i}\sum_{\ell=0}^{r-1}\eta^{i(\ell+1)}e_{t(\ell+1)}\;=\;\eta^{-i}v_{i0}.$$

It follows that W_i is a G-invariant subspace of V and the matrix representation of the restriction ρ_i of ρ^G to W_i relative to the basis $\mathcal{B}_i$, is given by

$$[\rho_i(a))]_{\mathcal{B}_i}=\begin{pmatrix}\zeta_0 & 0 & \dots & 0\\ 0 & \zeta_1 & \dots & 0\\ \vdots & \vdots & \ddots & \vdots\\ 0 & 0 & \dots & \zeta_{t-1}\end{pmatrix};\quad [\rho_i(b)]_{\mathcal{B}_i}=\begin{pmatrix}0 & 0 & \cdots & 0 & \eta^{-i}\\ 1 & 0 & \cdots & 0 & 0\\ 0 & 1 & \cdots & \vdots & \vdots\\ \vdots & \vdots & & 0 & 0\\ 0 & 0 & \cdots & 1 & 0\end{pmatrix}.$$

There are n vectors in $\cup\mathcal{B}_i$ and so, if we can prove they are linearly independent we shall have the decomposition $V=W_0\oplus W_1\oplus\cdots\oplus W_{r-1}$ into G-spaces.

Let $\sum_{i,j} \alpha_{ij} v_{ij}$. Then

$$\sum_{i,j,\ell} \alpha_{ij} \eta^{i\ell} e_{j+\ell t} = 0.$$

For all j and ℓ, we have

$$\sum_{i=0}^{r-1} \alpha_{ij} (\eta^{\ell})^i = 0.$$

Fixing j and letting ℓ vary, we obtain a system of r equations in r unknowns with matrix of coefficients the Vandermonde matrix

$$\begin{pmatrix} 1 & 1 & 1 & \dots & 1 \\ 1 & \eta & \eta^2 & \dots & \eta^{r-1} \\ 1 & \eta^2 & \eta^4 & \dots & \eta^{2(r-1)} \\ \vdots & \vdots & \vdots & \ddots & \vdots \\ 1 & \eta^{r-1} & \eta^{2(r-1)} & \dots & \eta^{(r-1)(r-1)} \end{pmatrix}.$$

Since η is a primitive r-th root of unity, this matrix is nonsingular, whence $\alpha_{ij} = 0$ for all i. Letting j vary we obtain $\alpha_{ij} = 0$ for all i and j. Observe that the $\overline{\mathbb{F}}_s G$-module W_0 exists whether or not $(r, s) = 1$ and so the necessity of (1) is proved.

The irreducibility of each W_i is proved in a manner entirely similar to that used to prove the sufficiency of (1). Finally, we observe that the characteristic polynomial of $\rho_i(b)$ is $X^t - \eta^{-i}$, whence the elements $\rho_0, \rho_1, \dots \rho_{r-1}$ are mutually inequivalent. □

Using the notation established in the foregoing, we now proceed by a series of lemmas to prove our main theorem.

Lemma 2.2. *Let ζ be a primitive m-th root of unity in $\overline{\mathbb{F}}_s$ and k be a positive integer with $|k|_m = n$. Then the Frobenius automorphism τ on $\overline{\mathbb{F}}_s$ defined by $\tau(x) = x^q$, where q is a power of s, permutes the elements of*

$$\mathcal{P} = \left\{\zeta, \zeta^k, \dots, \zeta^{k^{n-1}}\right\}$$

if and only if $q \equiv k^i \pmod{m}$ for some i, with $0 \leq i \leq n-1$.

Proof. If τ permutes the elements of $\mathcal{P}$, then $\zeta^q \in \mathcal{P}$ and so $\zeta^q = \zeta^{k^i}$ for some $i,\ 0 \leq i \leq n-1$. Hence $q \equiv k^i \pmod{m}$. Conversely, if $q \equiv k^i \pmod{m}$ then $(\zeta^{k^j})^q = \zeta^{k^{i+j}} \in \mathcal{P}$ whence τ permutes the elements of $\mathcal{P}$. □

The following is the cornerstone of our main result.

Lemma 2.3. *Let K be a field and let α be an automorphism of K with fixed field F. Let $a_0, a_1, \dots, a_{n-1}$ be elements of K which are cyclically permuted by α, say $\alpha(a_i) = a_{i+1}$, where the indices are taken modulo n. Let $f(x) = \prod_{i=0}^{n-1} (x - a_i) \in F[x]$*

and let $C = (c_{ij})$ be the $n \times n$ matrix with $c_{i,i-1} = 1$ if $2 \leq i \leq n$, $c_{1n} = 1$ and $c_{ij} = 0$ otherwise. Let V be the $n \times n$ Vandermonde matrix defined by

$$V = \begin{pmatrix} 1 & a_0 & a_0^2 & \cdots & a_0^{n-1} \\ 1 & a_1 & a_1^2 & \cdots & a_1^{n-1} \\ \vdots & \vdots & \vdots & \ddots & \vdots \\ 1 & a_{n-1} & a_{n-1}^2 & \ldots & a_{n-1}^{n-1} \end{pmatrix}.$$

Then $V^{-1}CV \in M_n(F)$, where $M_n(F)$ denotes the algebra of $n \times n$ matrices over F.

Proof. For $i = 0, 1, \ldots, n-1$, define

$$g_i(x) = \frac{f(x)}{(x - a_i)f'(a_i)},$$

where $f'(a_i)$ is the formal derivative of f evaluated at a_i. Let

$$g_i(x) = d_{0i} + d_{1i}x + \cdots + d_{(n-1)i}x^{n-1}$$

and let

$$D = \begin{pmatrix} d_{00} & d_{01} & \ldots & d_{0n-1} \\ d_{10} & d_{11} & \ldots & d_{1n-1} \\ \vdots & \vdots & \ddots & \vdots \\ d_{n-1,0} & d_{n-1,1} & \ldots & d_{n-1,n-1} \end{pmatrix},$$

i.e., D is the matrix whose columns are the coefficients of the g_i's. Since $g_i(a_j) = \delta_{ij}$, the Kronecker delta, we have $VD = I$ and so $D = V^{-1}$. Now

$$V^{-1}C = \begin{pmatrix} d_{01} & d_{02} & \cdots & d_{0n-1} & d_{00} \\ d_{11} & d_{12} & \cdots & d_{1n-1} & d_{10} \\ \vdots & \vdots & & \vdots & \vdots \\ d_{n-1,1} & d_{n-1,2} & \cdots & d_{n-1,n-1} & d_{n-1,0} \end{pmatrix}$$

and so it is easily seen that the $(j+1)$-st column of $V^{-1}CV$ consists of the coefficients of the polynomial

$$h_j(x) = (a_0)^j g_1(x) + (a_1)^j g_2(x) + \cdots + (a_{n-2})^j g_{n-1}(x) + (a_{n-1})^j g_0(x).$$

Now $g_i(x) = \frac{f(x)}{(x-a_i)f'(a_i)}$ and so applying the automorphism α and bearing in mind the fact that $f(x) \in F[x]$ we get, if $0 \leq i \leq n-2$,

$$\alpha(g_i(x)) = \frac{f(x)}{(x - a_{i+1})f'(a_{i+1})} = g_{i+1}(x)$$

while

$$\alpha(g_{n-1}(x)) = \frac{f(x)}{(x - a_0)f'(a_0)} = g_0(x).$$

Thus $\alpha(h_j(x)) = (a_1)^j g_2(x) + \cdots + (a_{n-1})^j g_0(x) + (a_0)^j g_1(x) = h_j(x)$. Since the fixed field of α is F, it follows that $V^{-1}CV \in M_n(F)$. □

Remark. The referee of our paper found the following nice, less computational proof of Lemma 2.3. Let $\beta = \alpha^{-1}$. Then β naturally acts element-wise on the matrices in $M_n(K)$, and we have $\beta(V) = CV$. Hence

$$\beta(V^{-1}) = (\beta(V))^{-1} = (CV)^{-1} = V^{-1}C^{-1}.$$

Thus

$$\beta(V^{-1}CV) = \beta(V^{-1})\beta(C)\beta(V) = V^{-1}C^{-1}CCV = V^{-1}CV$$

and again we can conclude that $V^{-1}CV \in M_n(F)$.

In the next lemma we use the hypothesis that the Frobenius automorphism τ on $\overline{\mathbb{F}}_s$ is transitive on the set $\mathcal{P} = \left\{\zeta, \zeta^k, \ldots, \zeta^{k^{n-1}}\right\}$. Observe that this simply means that $q \pmod m$ and $k \pmod m$ generate the same subgroups of $(\mathbb{Z}/m\mathbb{Z})^*$.

Lemma 2.4. *Let $G = \langle a, b \mid a^m = 1 = b^n, b^{-1}ab = a^k\rangle$, where $|k|_m = n$. Let ζ be a primitive m-th root of unity in $\overline{\mathbb{F}}_s$ and let q be a power of s. Assume that the Frobenius automorphism $\tau(x) = x^q$, with $x \in \overline{\mathbb{F}}_s$, is transitive on $\mathcal{P} = \left\{\zeta, \zeta^k, \ldots, \zeta^{k^{n-1}}\right\}$ and let $\rho : \langle a\rangle \to \overline{\mathbb{F}}^*$ be the representation defined by $\rho(a) = \zeta$. Then the induced representation ρ^G is realizable over $\mathbb{F}_q$.*

Proof. By assumption, $\zeta, \zeta^q, \ldots, \zeta^{q^{n-1}}$ are distinct and $\zeta^{q^n} = \zeta$ whence $|q|_m = n$. By Lemma 2.2, $q \equiv k^i \pmod m$ for some i. Since $|q|_m = |k|_m$, it follows that $(i, n) = 1$. Hence, letting $c = b^i$ we have $G = \langle a, c \mid a^m = 1 = c^n,\ c^{-1}ac = a^q\rangle$. The induced representation ρ^G using the coset representatives $1, c, c^2, \ldots, c^{n-1}$ is given by

$$\rho^G(c) = \begin{pmatrix} 0 & 0 & \ldots & 0 & 1 \\ 1 & 0 & \ldots & 0 & 0 \\ 0 & 1 & \ldots & 0 & 0 \\ \vdots & \vdots & \ddots & \vdots & \vdots \\ 0 & 0 & \ldots & 1 & 0 \end{pmatrix}; \quad \rho^G(a) = \begin{pmatrix} \zeta & 0 & 0 & \ldots & 0 \\ 0 & \zeta^q & 0 & \ldots & 0 \\ 0 & 0 & \zeta^{2q} & \ldots & 0 \\ \vdots & \vdots & \vdots & \ddots & \vdots \\ 0 & 0 & 0 & \ldots & \zeta^{q^{n-1}} \end{pmatrix}.$$

Set $\rho^G(c) = C$, $\rho^G(a) = A$ and let

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

Since $\tau(f(x)) = f(x)$ it follows that $f(x) \in \mathbb{F}_q[x]$, say $f(x) = a_0 + a_1x + \cdots + x^n$.

Let W be an n-dimensional vector space over $\overline{\mathbb{F}_s}$ and let

$$\mathcal{A} = \{v_0, v_1, v_2, \ldots, v_{n-1}\}$$

be a basis of W. Let $L : W \to W$ be the linear transformation with $[L]_{\mathcal{A}} = A$. Let $\zeta_i = \zeta^{q^i}, 0 \le i \le n-1$ and let

$$\begin{cases} w_0 &= v_0 + v_1 + \cdots + v_{n-1}, \\ w_1 &= \zeta_0 v_0 + \zeta_1 v_1 + \cdots + \zeta_{n-1} v_{n-1}, \\ \vdots & \vdots \qquad\qquad \vdots \\ w_{n-1} &= \zeta_0^{n-1} v_0 + \zeta_1^{n-1} v_1 + \cdots + \zeta_{n-1}^{n-1} v_{n-1}. \end{cases}$$

Then $Lw_i = w_{i+1}$, with $0 \leq i \leq n-2$ and

$$Lw_{n-1} = \zeta_0^n v_0 + \zeta_1^n v_1 + \cdots + \zeta_{n-1}^n v_{n-1}.$$

But $a_0 + a_1\zeta_i + a_2\zeta_i^2 + \cdots + \zeta_i^n = 0$ for all i and so

$$Lw_{n-1} = -a_0 w_0 - a_1 w_1 - \cdots - a_{n-1} w_{n-1}.$$

Let $\mathcal{B} = \{w_1, w_1, \ldots, w_{n-1}\}$. Then

$$[L]_{\mathcal{B}} = \begin{pmatrix} 0 & 0 & \ldots & 0 & -a_0 \\ 1 & 0 & \ldots & 0 & -a_1 \\ 0 & 1 & \ldots & 0 & -a_2 \\ \vdots & \vdots & \ddots & \vdots & \vdots \\ 0 & 0 & \ldots & 1 & -a_{n-1}. \end{pmatrix},$$

the companion matrix of $f(x)$. Let V be the Vandermonde matrix

$$V = \begin{pmatrix} 1 & \zeta_0 & \zeta_0^2 & \cdots & \zeta_0^{n-1} \\ 1 & \zeta_1 & \zeta_1^2 & \cdots & \zeta_1^{n-1} \\ \vdots & \vdots & \vdots & \ddots & \vdots \\ 1 & \zeta_{n-1} & \zeta_{n-1}^2 & \cdots & \zeta_{n-1}^{n-1} \end{pmatrix}.$$

We have that

$$V^{-1}AV = [L]_{\mathcal{B}} \in M_n(\mathbb{F}_q)$$

and by Lemma 2.3, since the fixed field of $\langle\tau\rangle$ is $\mathbb{F}_q$,

$$V^{-1}CV \in M_n(\mathbb{F}_q).$$

Hence ρ^G is realizable over $\mathbb{F}_q$. □

We are now ready to prove our main result.

Theorem 2.5. *Let*

$$G = \left\langle a, b \mid a^m = 1 = b^n, b^{-1}ab = a^k \right\rangle,$$

where $|k|_m = n$. As above, let ρ be the representation of $\langle a\rangle$ defined by $\rho(a) = \zeta$, where ζ is a primitive m-th root of 1 in $\overline{\mathbb{F}_s}$, with $(s, m) = 1$. Let q be a power of s. Then the induced representation ρ^G is realizable over $\mathbb{F}_q$ if and only if $q \equiv k^i \pmod m$ for some i, with $0 \leq i \leq n-1$.

Proof. Assume that ρ^G is realizable over $\mathbb{F}_q$. Then since

$$\rho^G(a) = \begin{pmatrix} \zeta & 0 & \ldots & 0 \\ 0 & \zeta^k & \ldots & 0 \\ \vdots & \vdots & \ddots & \vdots \\ 0 & 0 & \ldots & \zeta^{k^{n-1}} \end{pmatrix},$$

it follows that

$$f(x) = \prod_0^{n-1} (x - \zeta^{k^i}),$$

the characteristic polynomial of $\rho^G(a)$, is in $\mathbb{F}_q[x]$. Hence the Frobenius automorphism τ defined above permutes the elements of the set

$$\mathcal{P} = \left\{\zeta, \zeta^k, \ldots, \zeta^{k^{n-1}}\right\}.$$

By Lemma 2.2, $q \equiv k^i \pmod{m}$ for some i.

Conversely, assume $q \equiv k^j \pmod{m}$ for some j. Again by Lemma 2.2, τ permutes the elements of

$$\mathcal{P} = \left\{\zeta, \zeta^k, \ldots, \zeta^{k^{n-1}}\right\}.$$

Since $\langle\tau\rangle$ acts regularly on $\mathcal{P}$, the orbits of $\langle\tau\rangle$ are all of the same size. Let there be u orbits of size v each so that $uv = n$. Now $|q|_m = v$ and since $q \equiv k^j \pmod{m}$ we have $1 \equiv q^v \equiv k^{vj} \pmod{m}$. Thus $uv \mid vj$ whence $u \mid j$ and so $j = u\alpha$, say. Since $|k^u|_m = v = |q|_m$, it follows that $(\alpha, v) = 1$. Therefore $|b^{u\alpha}| = v$. Set $c = b^{u\alpha}$ and let $H = \langle a, c\rangle$. Then $c^{-1}ac = a^{k^{u\alpha}} = a^q$. Now $\langle\tau\rangle$ acts transitively on $\left\{\zeta, \zeta^q, \ldots, \zeta^{q^{v-1}}\right\}$ and so, by Lemma 2.4, ρ^H is realizable over $\mathbb{F}_q$. Hence $(\rho^H)^G$ is realizable over $\mathbb{F}_q$. But, by transitivity of induction, $(\rho^H)^G$ is equivalent to ρ^G whence ρ^G is realizable over $\mathbb{F}_q$. □

We now proceed to give a specific example of what happens when $|k|_m \neq n$ (see Theorem 2.1). It turns out that this example mirrors faithfully the situation which obtains in the case of the class of generalized quaternion groups Q_{4m}, m odd.

Example 2.6. Let

$$Q_{12} = \left\langle a, b \mid a^3 = 1 = b^4, b^{-1}ab = a^2\right\rangle.$$

In this case $|k|_3 = 2 \neq |b|$. The conjugacy classes of Q_{12} are

$$\{1\}, \quad \{b^2\}, \quad \{a, a^2\}, \quad \{b, ab, a^2b\}, \quad \{b^3, ab^3, a^2b^3\} \quad \text{and} \quad \{ab^2, a^2b^2\}.$$

Hence, over $\overline{\mathbb{F}_s}$, there are six irreducible representations, of which there are clearly four of degree one and two of degree two. Letting i be one of the square roots of -1 we obtain the following character table:

	1	a	b^2	b	b^3	ab^2
χ_1	1	1	1	1	1	1
χ_2	1	1	-1	i	$-i$	-1
χ_3	1	1	-1	$-i$	i	-1
χ_4	1	1	1	-1	-1	1
χ_5	2	-1	2	0	0	-1
χ_6	2	-1	-2	0	0	1

It happens that χ_5 is afforded by the representation

$$\rho_5(a) = \begin{pmatrix} 0 & -1 \\ 1 & -1 \end{pmatrix}, \quad \rho_5(b) = \begin{pmatrix} 1 & -1 \\ 0 & -1 \end{pmatrix},$$

while χ_6 is afforded by

$$\rho_6(a) = \begin{pmatrix} \zeta & 0 \\ 0 & \zeta^2 \end{pmatrix}, \quad \rho_6(b) = \begin{pmatrix} 0 & -1 \\ 1 & 0 \end{pmatrix}.$$

The representation ρ^G which is induced by $\rho : \langle a \rangle \to \langle \zeta \rangle$, where ζ is a primitive third root of 1, verifies

$$\rho^G(a) = \begin{pmatrix} \zeta & 0 & 0 & 0 \\ 0 & \zeta^2 & 0 & 0 \\ 0 & 0 & \zeta & 0 \\ 0 & 0 & 0 & \zeta^2 \end{pmatrix} \qquad \text{and} \qquad \rho^G(b) = \begin{pmatrix} 0 & 0 & 0 & 1 \\ 1 & 0 & 0 & 0 \\ 0 & 1 & 0 & 0 \\ 0 & 0 & 1 & 0 \end{pmatrix},$$

and this is easily seen to be equivalent to $\rho_5 + \rho_6$, defined by

$$a \mapsto \begin{pmatrix} 0 & -1 & 0 & 0 \\ 1 & 0 & 0 & 0 \\ 0 & 0 & \zeta & 0 \\ 0 & 0 & 0 & \zeta^2 \end{pmatrix} \qquad \text{and} \qquad b \mapsto \begin{pmatrix} 0 & 1 & 0 & 0 \\ 1 & 0 & 0 & 0 \\ 0 & 0 & 0 & -1 \\ 0 & 0 & 1 & 0 \end{pmatrix}.$$

Thus to find an explicit matrix representation of ρ^G over some $\mathbb{F}_q$, we need only realize ρ_6 over $\mathbb{F}_q$. We do this in full generality for Q_{4m}, m odd.

Proposition 2.7. *Let*

$$Q_{4m} = \left\langle a, b \mid a^m = 1 = b^4, b^{-1}ab = a^{-1} \right\rangle$$

and let $\rho : \langle a \rangle \to \overline{\mathbb{F}_s}$ be the representation defined by $\rho(a) = \zeta$, where ζ is a primitive m-th root of unity. Then ρ^G is the direct sum of the representations σ and τ, where

$$\sigma(a) = \begin{pmatrix} \zeta & 0 \\ 0 & \zeta^{-1} \end{pmatrix}, \quad \sigma(b) = \begin{pmatrix} 0 & 1 \\ 1 & 0 \end{pmatrix}$$

and

$$\tau(a) = \begin{pmatrix} \zeta & 0 \\ 0 & \zeta^{-1} \end{pmatrix}, \quad \tau(b) = \begin{pmatrix} 0 & -1 \\ 1 & 0 \end{pmatrix}.$$

Proof. The elements σ and τ are both irreducible since $\sigma(a)$ and $\sigma(b)$ (respectively, $\tau(a)$ and $\tau(b)$) have no common eigenvector. Also, by Frobenius reciprocity,

$$\begin{aligned} (\rho^G, \sigma) &= (\rho, \sigma_{\langle a \rangle}) \\ &= \frac{1}{m}\left[2 + \zeta(\zeta + \zeta^{-1}) + \zeta^2(\zeta^2 + \zeta^{-2}) + \cdots + \zeta^{m-1}(\zeta^{m-1} + \zeta^{-(m-1)})\right] \\ &= 1, \end{aligned}$$

since $\left\langle \zeta^2 \right\rangle = \langle \zeta \rangle$ (because m is odd). Similarly, $(\rho^G, \tau) = 1$. Thus, since

$$\deg\ \sigma = \deg\ \tau = 2 \quad \text{and} \quad \deg\ \rho^G = 4,$$

it follows that $\rho^G = \sigma + \tau$. □

Remark. The representation σ is a representation of

$$Q_{4m}/\left\langle b^2 \right\rangle \approx \left\langle a, c \mid a^m = 1 = c^2, c^{-1}ac = a^{-1} \right\rangle$$

and can be dealt with using Theorem 2.5 (see also Theorem 3.6). We are thus left with the computation of an explicit form for τ over $\mathbb{F}_q$, where, as usual, q is a power of the prime s. Naturally, if τ is realizable over $\mathbb{F}_q$, then $\zeta + \zeta^{-1} \in \mathbb{F}_q$. Moreover, $\zeta + \zeta^{-1} \in \mathbb{F}_q$ if and only if $q \equiv \pm 1 \pmod{m}$ (see Theorem 3.6). Thus, given that

$\theta = \zeta + \zeta^{-1} \in \mathbb{F}_q$, we construct an explicit representation over $\mathbb{F}_q$ which is equivalent to τ.

We may assume $\zeta \notin \mathbb{F}_q$, otherwise τ itself is an $\mathbb{F}_q$-representation. Clearly the irreducible polynomial of ζ over $\mathbb{F}_q$ is $f = x^2 - \theta x + 1$ and so $\zeta = \frac{\theta + \sqrt{\theta^2 - 4}}{2}$ where we have taken a specific square root of $\theta^2 - 4$ in $\overline{\mathbb{F}_q}$.

Choose $\alpha, \beta \in \mathbb{F}_q$ such that $\alpha^2 + \beta^2 = \theta^2 - 4$. Since $\zeta \notin \mathbb{F}_q$ it follows that $\beta \neq 0$. Let

$$A = \begin{pmatrix} \alpha & \beta \\ \beta & -\alpha \end{pmatrix} \quad \text{and} \quad \tilde{A} = \frac{\theta}{2} + \frac{1}{2}A.$$

By our choice of α and β, we have $A^2 = (\theta^2 - 4)I$ and so the minimum polynomial of $\tilde{A}$ is $f = x^2 - \theta x + 1$ since $\tilde{A}$ is not diagonal. The mapping $\varphi : \mathbb{F}_q[\zeta] \to M_2(\mathbb{F}_q)$ defined by

$$\varphi(g(\zeta)) = g(\tilde{A})$$

is well-defined since the irreducible polynomial of ζ over $\mathbb{F}_q$ is the same as the minimum polynomial of $\tilde{A}$, and so embeds $\mathbb{F}_q[\zeta]$ in $M_2(\mathbb{F}_q)$.

Let $B = \begin{pmatrix} 0 & -1 \\ 1 & 0 \end{pmatrix}$. Then $B^{-1}AB = -A$ and so $B^{-1}\tilde{A}B = \frac{\theta}{2}I - \frac{1}{2}A = \tilde{A}^{-1}$. The map $\mu : Q_{4m} \to M_2(\mathbb{F}_q)$ defined by

$$\mu(a) = \tilde{A} \quad \text{and} \quad \mu(b) = B$$

is clearly a faithful irreducible representation of Q_{4m}. We show that $tr\tilde{A}^t = \zeta^t + \zeta^{-t}$. Define $\gamma_1 = \theta$, $\gamma_0 = 1$ and, for $j \geq 2$, let $\gamma_j = \theta\gamma_{j-1} - \gamma_{j-2}$. We claim that $\zeta^t = \gamma_{t-1}\zeta - \gamma_{t-2}$ for all $t \geq 2$. Indeed, when $t = 2, \zeta^2 = \theta\zeta - 1 = \gamma_1\zeta - \gamma_0$. Assume the result true for t. Then

$$\zeta^{t+1} = \gamma_{t-1}\zeta^2 - \gamma_{t-2}\zeta = \gamma_{t-1}(\theta\zeta - 1) - \gamma_{t-2}\zeta = (\theta\gamma_{t-1} - \gamma_{t-2})\zeta - \gamma_{t-1} = \gamma_t\zeta - \gamma_{t-1}.$$

By induction, the result follows. In a similar fashion we have $\zeta^{-t} = \gamma_{t-1}\zeta^{-1} - \gamma_{t-2}$. Now $\tilde{A}^t = \gamma_{t-1}\tilde{A} - \gamma_{t-2}I$, and so $tr(\tilde{A}^t) = \theta\gamma_{t-1} - 2\gamma_{t-1}$, since $tr(\tilde{A}) = \theta$. But $\zeta^t + \zeta^{-t} = \theta\gamma_{t-1} - 2\gamma_{t-1} = tr\tilde{A}^t$.

It is easily checked that $tr(\tilde{A}^t B^j) = 0$ if j is odd and $tr(\tilde{A}^t B^2) = -\zeta^t - \zeta^{-t}$. Hence the character afforded by μ is identical to that afforded by τ. Since each is irreducible, it follows that μ and τ are equivalent.

Returning again to the case $Q_{12} = \langle a, b \mid a^3 = 1 = b^4,\ b^{-1}ab = a^{-1} \rangle$, let $\mathbb{F}_q = \mathbb{F}_5$. Since $5 \equiv -1 \pmod 3$, it follows that $\zeta + \zeta^{-1} \in \mathbb{F}_5$ where ζ is a primitive third root of unity. Indeed, since $x^2 + x + 1$ is the irreducible polynomial of ζ over $\mathbb{F}_5$, we have $\zeta + \zeta^{-1} = -1 = \theta$. Hence $\theta^2 - 4 = -3$. Choose $\alpha^2 + \beta^2 = -3$, say $\alpha = 1 = \beta$. Then

$$A = \begin{pmatrix} 1 & 1 \\ 1 & -1 \end{pmatrix}$$

and

$$\tilde{A} = \frac{-I}{2} + \frac{1}{2}\begin{pmatrix} 1 & 1 \\ 1 & -1 \end{pmatrix} = 2I + 3\begin{pmatrix} 1 & 1 \\ 1 & -1 \end{pmatrix} = \begin{pmatrix} 0 & 3 \\ 3 & -1 \end{pmatrix}.$$

It now follows from the general theory above that the representation

$$a \mapsto \begin{pmatrix} \zeta & 0 \\ 0 & \zeta^{-1} \end{pmatrix}, \quad b \to \begin{pmatrix} 0 & -1 \\ 1 & 0 \end{pmatrix},$$

is equivalent to

$$a \mapsto \begin{pmatrix} 0 & 3 \\ 3 & -1 \end{pmatrix}, \quad b \to \begin{pmatrix} 0 & -1 \\ 1 & 0 \end{pmatrix}.$$

3. Applications related to the quadratic reciprocity law

By choosing special groups in Theorem 2.5 we are able to obtain some interesting number-theoretic relations. In particular, we shall recover the classical quadratic reciprocity laws as well as an interesting property concerning "values of cosine". (See [Syl]. This property was also re-discovered and generalized in [M-R].) It is clear that many other interesting facts can be established by choosing appropriate groups. This is left to the interested reader, and authors who are certainly interested.

Example 3.1 (The quadratic reciprocity law). Let p and s be distinct odd primes, g be a primitive root modulo p and ζ be a primitive p-th root of unity in $\overline{\mathbb{F}_s}$. Let

$$G = G(p) = \left\langle a, b \mid a^p = 1 = b^{\frac{p-1}{2}}, b^{-1}ab = a^{g^2} \right\rangle$$

(see [Jac, Section 5.15]). Since $|g^2|_p = |b|$, we are in a position to apply Theorem 2.5. Thus let $\rho = \rho(p) : \langle a \rangle \to \overline{\mathbb{F}_s}$ be defined by $\rho(a) = \zeta$ and let (s/p) be the usual Legendre symbol. Then we have the following three results.

Theorem 3.2. *ρ^G is realizable over $\mathbb{F}_s$ if and only if* $\left(\dfrac{s}{p}\right) = 1$.

Proof. By Theorem 2.5, ρ^G is realizable over $\mathbb{F}_s$ if and only if $s \equiv g^{2i} \pmod{p}$ for some i, with $0 \le i \le \frac{p-3}{2}$. That is, ρ^G is realizable over $\mathbb{F}_s$ if and only if s is a square modulo p. □

Theorem 3.3. *Let $p^* = (-1)^{\frac{p-1}{2}} p$. Then ρ^G is realizable over $\mathbb{F}_s$ if and only if* $\left(\dfrac{p^*}{s}\right) = 1$.

Proof. By Theorem 3.2, if ρ^G is realizable over $\mathbb{F}_s$, then the Frobenius automorphism $x \to x^s$ on $\overline{\mathbb{F}}_s$ permutes the elements of the set $\{\zeta, \zeta^{g^2}, \ldots, \zeta^{g^{p-3}}\}$. But then

$$\sum_{i=0}^{(p-3)/2} \zeta^{g^{2i}} \in \mathbb{F}_s.$$

Otherwise, by [Jac, Section 5.15], we have

$$\sum_{i=0}^{(p-3)/2} \zeta^{g^{2i}} = \frac{-1 \pm \sqrt{p^*}}{2},$$

whence $\sqrt{p^*} \in \mathbb{F}_s$ and so $\left(\frac{p^*}{s}\right) = 1$.

Conversely, assume that $\left(\frac{p^*}{s}\right) = 1$. Then, as above,

$$\sum_{i=0}^{(p-3)/2} \zeta^{g^{2i}} \in \mathbb{F}_s.$$

We show that the Frobenius automorphism $\varphi : x \to x^s$ on $\overline{\mathbb{F}_s}$ permutes the elements of the set

$$\left\{\zeta, \zeta^{g^2}, \zeta^{g^4}, \ldots, \zeta^{g^{p-3}}\right\}.$$

Then using Theorem 2.5 we conclude that ρ^G is realizable over $\mathbb{F}_s$.

To do this, it is sufficient by Lemma 2.2 to show that $\varphi(\zeta) = \zeta^{g^{2j}}$ for some j in $\left\{0, 1, \ldots, \frac{p-3}{2}\right\}$. Now

$$1 + \sum_{i=0}^{(p-3)/2} \zeta^{g^{2i}} + \sum_{i=0}^{(p-3)/2} \zeta^{g^{2i+1}} = 0.$$

If $\phi(\zeta) = \zeta^{g^{2j+1}}$, then

$$\sum_{i=0}^{(p-3)/2} \zeta^{g^{2i}} = \sum_{i=0}^{(p-3)/2} \zeta^{g^{2i+1}},$$

whence

$$1 + 2\sum_{i=0}^{(p-3)/2} \zeta^{g^{2i}} = \pm\sqrt{p^*} = 0.$$

Thus $p^* = 0$, contradicting the hypothesis that p and s are distinct primes. Therefore, ρ^G is realizable over $\mathbb{F}_s$ and Corollary 3.4 follows immediately. □

Corollary 3.4 (The quadratic reciprocity law [Gau]**).** *We have*

$$\left(\frac{s}{p}\right) = \left(\frac{p^*}{s}\right).$$

Remark. The realizability of ρ^G over $\mathbb{F}_s$ depends entirely on $s \pmod p$.

Remarks. (1) The method of evaluation $\sum_{i=0}^{\frac{p-3}{2}} \zeta^{g^{2i}}$ given in [Jac, Section 5.15] can be simplified and clarified as follows: let Q be the set of nonzero quadratic residues modulo p and let N be the set of nonquadratic residues modulo p. If ζ is a primitive p-th root of unity in $\overline{\mathbb{F}_s}$ we have:

(i) For $p \equiv 1 \pmod 4$,

$$\sum_{x\in Q} \zeta^{-x} = \sum_{x\in Q} \zeta^{x} \qquad \text{and} \qquad \sum_{x\in N} \zeta^{x} = \sum_{x\in N} \zeta^{-x}.$$

(ii) For $p \equiv -1 \pmod 4$,

$$\sum_{x\in Q} \zeta^{-x} = \sum_{x\in N} \zeta^{x} \qquad \text{and} \qquad \sum_{x\in N} \zeta^{-x} = \sum_{x\in Q} \zeta^{x}.$$

Now let $c = \sum_{x \in Q} \zeta^x$ and let $G = \left\langle a, b \mid a^p = 1 = b^{\frac{p-1}{2}}, b^{-1}ab = a^{g^2} \right\rangle$, where g is a primitive root modulo p. Let ρ_1 and ρ_2 be the representations of $H = \langle a \rangle$ defined by $\rho_1(a) = \zeta$ and $\rho_2(a) = \zeta^g$ and let χ_1 and χ_2 denote their respective characters. Since $|g^2|_p = \frac{p-1}{2} = |b|$, it follows by Proposition 2.1 (1) that ρ_1^G and ρ_2^G are irreducible. Moreover, since $\rho_1^G(a)$ and $\rho_2^G(a)$ have different eigenvalues, they are inequivalent. Hence by Schur's Lemma and Frobenius reciprocity we have

$$0 = \left(\chi_2^G, \chi_1^G\right) = \left(\chi_2, (\chi_1^G)_H\right).$$

But

$$(\chi_2, (\chi_1^G)_H) = \frac{1}{|H|}\left(\frac{p-1}{2} + \zeta^g \sum_{x \in Q} \zeta^{-x} + \zeta^{g^2} \sum_{x \in N} \zeta^{-x} + \zeta^{g^3} \sum_{x \in Q} \zeta^{-x} + \cdots + \zeta^{g^{p-1}} \sum_{x \in N} \zeta^{-x}\right).$$

Case (i). Let $p \equiv 1 \pmod 4$. By (i) above we have

$$0 = \frac{p-1}{2} + \zeta^g c + \zeta^{g^2}(-1-c) + \zeta^{g^3} c + \cdots + \zeta^{g^{p-1}}(-1-c).$$

Hence

$$\frac{1-p}{2} = c(-1-c) + c(-1-c)$$

and so

$$4c^2 + 4c + 1 - p = 0.$$

Therefore

$$c = \frac{-1 \pm \sqrt{p}}{2}.$$

Case (ii). Let $p \equiv -1 \pmod 4$. By (ii) above we have

$$0 = \frac{p-1}{2} + \zeta^g(-1-c) + \zeta^{g^2} c + \cdots + \zeta^{g^{p-1}} c.$$

Hence

$$\frac{p-1}{2} + (-1-c)^2 + c^2 = 0,$$

yielding

$$4c^2 + 4c + p + 1 = 0.$$

Therefore

$$c = \frac{-1 \pm \sqrt{-p}}{2}.$$

We may combine the two solutions by setting $p^* = (-1)^{p-1/2}p$. Then $c = \frac{-1 \pm \sqrt{p^*}}{2}$.

(2) Assume that p is an odd prime such that $p \equiv 1 \pmod n$. Let g be a primitive root modulo p and let

$$G(p,n) = \left\langle a, b \mid a^p = 1 = b^{(p-1)/n}, b^{-1}ab = a^{g^n} \right\rangle.$$

The group $G(p)$ of the previous example is the group $G(p,2)$ in this notation. Observe that $|g^n|_p = \frac{p-1}{n} = |b|$ and so, once again, Theorem 2.5 is applicable. We find immediately that the representation $\rho^{G(p,n)}$ is realizable over $\mathbb{F}_s$ if and only if s has an n-th

root in $\mathbb{F}_p$. In this case again we see a connection with higher reciprocity laws (see, for example [I-R] and [Ank]) which we plan to investigate in a subsequent paper.

Example 3.5. In [Syl], Sylvester discovered that if ζ is a primitive m-th root of unity in $\overline{\mathbb{F}_s}$, $(s,m)=1$, then $2\cos\frac{2\pi}{m} := \zeta+\zeta^{-1}$ belongs to $\mathbb{F}_s$ if and only if $s \equiv \pm 1 \pmod{m}$. Sylvester's formulation of his result differs somewhat from that just stated, but is equivalent to it. In the paper [M-R] this result was re-discovered, generalized and applied to some questions concerning extensions of degree 2^l.

Here we shall strengthen Sylvester's result by applying our Theorem 2.5 to the dihedral group. As usual, set $D_{2m} = \langle a, b \mid a^m = 1 = b^2, b^{-1}ab = a^{-1}\rangle$, with $m \in \mathbb{N}$ and $m \geq 3$. Then $|-1|_m = 2 = |b|$ and so our theorem is applicable.

Theorem 3.6. *The 2-dimensional representation ρ of D_{2m} given by*

$$\rho(a) = \begin{pmatrix} \zeta & 0 \\ 0 & \zeta^{-1} \end{pmatrix} \quad \text{and} \quad \rho(b) = \begin{pmatrix} 0 & 1 \\ 1 & 0 \end{pmatrix},$$

where ζ is a primitive m-th root of unity is realizable over the field $\mathbb{F}_q$, with q a power of the odd prime s, if and only if $q \equiv \pm 1 \pmod{m}$. Moreover, in the case when ρ is realizable over $\mathbb{F}_q$, we can write the corresponding matrices with entries in $\mathbb{F}_q$ explicitly. Indeed, we have:

(1) *If $q \equiv 1 \pmod{m}$, then $\zeta \in \mathbb{F}_q$ and the original matrices lie in $\mathbb{F}_q$;*

(2) *If $q \equiv -1 \pmod{m}$, then $\zeta \notin \mathbb{F}_q$, but $t = \zeta + \zeta^{-1} \in \mathbb{F}_q$ and ρ is equivalent to the representation θ given by*

$$\theta(a) = \begin{pmatrix} 0 & 1 \\ 1 & t \end{pmatrix} \quad \text{and} \quad \theta(b) = \begin{pmatrix} 1 & t \\ 0 & -1 \end{pmatrix}.$$

One can find the matrices over $\mathbb{F}_q$ following the proof of Theorem 2.5. From the explicit form of the matrices we deduce immediately that $\zeta + \zeta^{-1} \in \mathbb{F}_q$ if and only if $q \equiv \pm 1 \pmod{m}$ which is indeed a generalization of Sylvester's result. This theorem does give us additional information, namely, that if $q \equiv \pm 1 \pmod{m}$, then, not only is $\zeta + \zeta^{-1} \in \mathbb{F}_q$, but the whole representation ρ is realizable over $\mathbb{F}_q$ and moreover, explicit formulas for the matrices $\rho(g)$ and g in D_{2m} can be computed.

4. Connections with cross-products

The methods used in the previous sections are of an elementary nature but may appear somewhat mysterious to the reader. The veil of mystery lifts however and we gain considerable insight into our computations once we establish a connection with cross-products (see for example [Her] or [Rei]). Moreover, guided by this connection with cross-products we are able to obtain a stronger result concerning complete realizability (*cf.* Definition 4.5).

Roughly speaking, cross-products intervened in the following manner. We consider a finite field $F = \mathbb{F}_q$ over which we want to construct a representation module M for our group G which realizes a given component ρ_i, with $i = 0, 1, \ldots, r-1$ of ρ^G (see Proposition 2.1). More precisely, we want to verify that for $L = F(\zeta)$, where ζ is a

primitive m-th root of unity, the action of $a, b \in G$ on $L \otimes_F M$ has the required form described in Proposition 2.1 (2) with respect to a suitable basis of $L \otimes_F M$.

Now a hint on how to construct the required representation module M is obtained via the cross-product $A = (L/F, \mathcal{G}, f)$ with a trivial factor set f (see [Her, Chapter 4] and Example 4.1 below) in the case where $[L : F] = t, q \equiv k \pmod m$, $q \equiv 1 \pmod r$, and $(r, m) = 1$ (in the notation of Proposition 2.1).

Then the idea is to choose $M \cong L$ as F-vector spaces and use two facts:

(1) We can embed our group G into A.

(2) There exists an isomorphism $\varphi\colon A \to \mathrm{Hom}_F(L, L)$.

Then using φ restricted to G embedded in A, we obtain a representation G on M. Thus we can say that our cross-product A guides us to make the specific representation of G on M described in the first paragraph of our proof of Theorem 4.5.

We should point out, however, that we only use the cross-product construction as a guide for building a representation M, and our further exposition is logically independent of this construction. Nevertheless it seems to us worthwhile to include at least this idea, and to explain it in a detailed way in Example 4.1 below. One could say that if we were to follow C. F. Gauss's style of exposition, we would dismantle the scaffolding upon completion of the building. We have instead tried to follow L. Euler, by leaving the scaffolding intact.

We begin with an example which points the way in the general case.

Example 4.1. Let $G = \langle a, b \mid a^7 = 1 = b^9,\ b^{-1}ab = a^2 \rangle$. Let F be a finite field with q elements where $q \equiv 2 \pmod 7$ and $q \equiv 1 \pmod 3$ (for example, $q = 37$ would do). Let ζ be a primitive seventh root of unity in $\overline{F}$. In this case $|2|_7 = 3$ and so, using the notation established in Proposition 2.1, $r = t = 3$ and ρ^G is the direct sum of the representations

$$a \to \begin{pmatrix} \zeta & 0 & 0 \\ 0 & \zeta^2 & 0 \\ 0 & 0 & \zeta^4 \end{pmatrix} \quad \text{and} \quad b \to \begin{pmatrix} 0 & 0 & \eta \\ 1 & 0 & 0 \\ 0 & 1 & 0 \end{pmatrix}$$

as η varies over the third roots of unity in F. Let $L = F(\zeta)$. Then

$$\mathcal{G} = \mathrm{Gal}(L/F) = \langle \sigma \rangle ,$$

where $\sigma(\zeta) = \zeta^2$. Form the cross-product $A = (L/F, \mathcal{G}, f)$ with trivial factor set f (*cf.* [Her, Chapter 4]). Recall that A is a 3-dimensional algebra over L with basis $\{1 = u_1, u_\sigma, u_{\sigma^2}\}$ and multiplication defined according to the following:

(i) $u_\tau u_\nu = u_{\tau\nu}$;

(ii) $u_\tau \ell = \tau(\ell) u_\tau$.

It is easily checked ([Rei, Chapter 7, Section 29]) that the map $\varphi : A \to \mathrm{Hom}_F(L, L)$ defined by

$$[\varphi(\ell_0 + \ell_1 u_\sigma + \ell_2 u_{\sigma^2})](\lambda) = \ell_0\lambda + \ell_1\sigma(\lambda) + \ell_2\sigma^2(\lambda)$$

for all $\lambda \in L$ is an F-algebra isomorphism.

Now let η be a third root of unity in F and choose $z \in L$ such that $N_{L/F}(z) = \eta$. Here $N_{L/F}$ is the norm map from L down to F. Let $\psi : G \to A$ be the homomorphism defined by

$$\psi(a) = \zeta \quad \text{and} \quad \psi(b) = zu_{\sigma^2}.$$

Since $\zeta^7 = 1$, $(zu_{\sigma^2})^3 = \eta$ and $(zu_{\sigma^2})\zeta(zu_{\sigma^2})^{-1} = \zeta^4$ it follows that ψ is a well-defined homomorphism. (From the last identity it follows that $(zu_{\sigma^2})^{-1}\zeta(zu_{\sigma^2}) = \zeta^2$.)

Let $f = (x-\zeta)(x-\zeta^2)(x-\zeta^4) \in F[x]$. Then f is irreducible polynomial since $\mathcal{G}$ acts transitively on $\{\zeta, \zeta^2, \zeta^4\}$. Hence L is isomorphic with $M := \frac{F[x]}{(f)}$, where we send ζ to $\bar{x}$, the class of $x \pmod f$. We now define an action of G on M via ψ by

$$\begin{cases} ag(\overline{x}) &= \overline{x}g(\overline{x}), \\ bg(\overline{x}) &= z(\overline{x})g(\overline{x}^4), \end{cases}$$

where $z(\overline{x})$ corresponds to z. This clearly turns M into an FG-module since ψ is a homomorphism.

Let

$$M^L = L \otimes_F \frac{F[x]}{(f)} = \frac{L[x]}{(f)}.$$

We show that relative to an appropriate basis, M^L affords the matrix representation

$$a \mapsto \begin{pmatrix} \zeta & 0 & 0 \\ 0 & \zeta^2 & 0 \\ 0 & 0 & \zeta^4 \end{pmatrix} \quad \text{and} \quad b \mapsto \begin{pmatrix} 0 & 0 & \eta \\ 1 & 0 & 0 \\ 0 & 1 & 0 \end{pmatrix}.$$

Indeed, let

$$g_0 = \frac{(\overline{x}-\zeta^2)(\overline{x}-\zeta^4)}{(\zeta-\zeta^2)(\zeta-\zeta^4)}, \quad g_1 = \frac{z(\overline{x})(\overline{x}-\zeta)(\overline{x}-\zeta^4)}{(\zeta^2-\zeta)(\zeta^2-\zeta^4)}$$

and

$$g_2 = \frac{z(\overline{x})z(\overline{x}^4)(\overline{x}-\zeta)(\overline{x}-\zeta^2)}{(\zeta^4-\zeta)(\zeta^4-\zeta^2)}.$$

Using the equality $\bar{f} = 0$ in M, we see that

$$ag_0 = \zeta g_0, \quad ag_1 = \zeta^2 g_1 \quad \text{and} \quad ag_2 = \zeta^4 g_2.$$

Moreover,

$$bg_0(\overline{x}) = z(\overline{x})g_0(\overline{x}^4) = \frac{z(\overline{x})(\overline{x}^4-\zeta^2)(\overline{x}^4-\zeta^4)}{(\zeta-\zeta^2)(\zeta-\zeta^4)}.$$

But

$$\frac{(x^4-\zeta^2)(x^4-\zeta^4)}{(\zeta-\zeta^2)(\zeta-\zeta^4)} \quad \text{and} \quad \frac{(x-\zeta)(x-\zeta^4)}{(\zeta^2-\zeta)(\zeta^2-\zeta^4)}$$

evaluated at ζ, ζ^2 and ζ^4 both yield 0, 1, 0 respectively, showing that $bg_0 = g_1$. Similarly $bg_1 = g_2$ and $bg_2 = \eta g_0$ since $z(\overline{x})z(\overline{x}^4)z(\overline{x}^2) = \eta$. It follows that the given representation is realizable over F because M is our desired 3-dimensional representation space over F.

The above example is representative of the proof we are about to embark upon for the general case, except that, in the general case we need a technical maneuver to deal with the possibility that f is reducible over F and that conjugation of a by b does not reflect the action of the Galois group on ζ. In the example above f is irreducible over F and $b^{-1}ab = a^2$ reflects the fact that $\sigma(\zeta) = \zeta^2$.

Lemma 4.2. *Let F be a field and f a monic polynomial over F. Assume f has distinct roots $\zeta_1, \zeta_2, \ldots, \zeta_t$ in some splitting field and let d be a positive integer such that*

$$\{\zeta_1, \zeta_2, \ldots, \zeta_t\} = \{\zeta_1^d, \zeta_2^d, \ldots, \zeta_t^d\}.$$

Then $f(x) \mid f(x^d)$.

Proof. We have

$$f(x^d) = \prod_i (x^d - \zeta_i) = \prod_i (x^d - \zeta_i^d).$$

Clearly each ζ_i is a root of $f(x^d)$ and so $f(x) \mid f(x^d)$. □

Corollary 4.3. *With the same hypotheses and notation as above, if $g(x)$ and $h(x)$ are polynomials over F and $g(x) \equiv h(x) \pmod f$, then $g(x^d) \equiv h(x^d) \pmod f$.*

Proof. If $f(x) \mid (g(x) - h(x))$, then $f(x^d) \mid (g(x^d) - h(x^d))$. By the above lemma, we have $f(x) \mid (g(x^d) - h(x^d))$. □

The next lemma is the technical maneuver referred to above.

Lemma 4.4. *Let s be a prime, m be a positive integer with $(m, s) = 1$ and let q be a power of s. Let k be a positive integer and let ζ be a primitive m-th root of unity in $\overline{\mathbb{F}_s}$. Assume that $|k|_m = t$ and that $q \equiv k^j \pmod m$ for some j. Let*

$$f = (x - \zeta)(x - \zeta^k) \cdots (x - \zeta^{k^{t-1}})$$

and let $\eta \in F = \mathbb{F}_q$. Then there exists $z(x) \in F[x]$ such that

$$z(x)z(x^k) \cdots z(x^{k^{t-1}}) \equiv \eta \pmod f.$$

Proof. The set $\left\{\zeta, \zeta^k, \ldots, \zeta^{k^{t-1}}\right\}$ of roots of f in $L = F(\zeta)$ is invariant under the Frobenius automorphism $a \mapsto a^q$ since $q \equiv k^j \pmod m$. Hence $f \in F[x]$. Let $f = f_1 f_2 \cdots f_u$ be the factorization of f into irreducible factors over F and let S (resp. $\widehat{S}$) denote the set of roots of f_1 (resp. $f_2 f_3 \cdots f_u$). Assume that $\zeta \in S$. Let $\widehat{f_i} = f/f_i$, with $i = 1, 2, \ldots, u$. Since $(\widehat{f_i}, f_i) = 1$, there exists $h_i \in F[x]$ such that

$$h_i \widehat{f_i} \equiv 1 \pmod{f_i}.$$

Now $\frac{F[x]}{(f_1)}$ is isomorphic to L, where $\bar{x}$ (the element $x \pmod{f_1}$) plays the role of ζ. Further there exists $z \in L$ such that $N_{L/F}(z) = \eta$. Hence there exists $z_1(x) \in F[x]$ such that $\prod_{\xi \in S} z_1(\xi) = \eta$. Now let

$$z(x) = h_1(x)\widehat{f_1}(x)z_1(x) + h_2(x)\widehat{f_2}(x) + \cdots + h_u(x)\widehat{f_u}(x).$$

We observe that if α is a root of f_i, then $h_i(\alpha)\widehat{f}_i(\alpha) = 1$, while if α is a root of $\widehat{f}_i$, we have $h_i(\alpha)\widehat{f}_i(\alpha) = 0$. Now let δ be a root of f. We compute

$$z(\delta)z(\delta^k)\cdots z(\delta^{k^{t-1}}) = \prod_{\xi\in S} z(\xi)\prod_{\xi\in\widehat{S}} z(\xi).$$

If $\xi \in \widehat{S}$, (say ξ is a root of f_j, with $j \neq 1$), then $z(\xi) = h_j(\xi)\widehat{f}_j(\xi) = 1$. Thus

$$z(\delta)z(\delta^k)\cdots z(\delta^{k^{t-1}}) = \prod_{\xi\in S} z(\xi).$$

But if $\xi \in S$, $z(\xi) = z_1(\xi)$ and so

$$z(\delta)z(\delta^k)\cdots z(\delta^{k^{t-1}}) = \prod_{\xi\in S} z_1(\xi) = \eta.$$

Hence $z(x)z(x^k)\cdots z(x^{k^{t-1}})$ evaluated at any root of f yields η. It follows that

$$z(x)z(x^k)\cdots z(x^{k^{t-1}}) \equiv \eta \pmod{f}. \qquad \square$$

Theorem 4.5. *Let*

$$G = \left\langle a, b \mid a^m = b^n = 1, b^{-1}ab = a^k \right\rangle$$

and let $|k|_m = t$ and $n = rt$. Let ζ be a primitive m-th root of unity in $\overline{\mathbb{F}_s}$, s a prime with $(s, m) = 1$. Let q be a power of s and assume $q \equiv k^j \pmod{m}$ for some j. Assume further that $F(= \mathbb{F}_q)$ contains a primitive r-th root of unity η. Then, for each integer c, the representation of G defined by

$$a \mapsto \begin{pmatrix} \zeta & 0 & \dots & 0 \\ 0 & \zeta^k & \dots & 0 \\ \vdots & \vdots & \ddots & \vdots \\ 0 & 0 & \dots & \zeta^{k^{t-1}} \end{pmatrix} \quad \text{and} \quad b \mapsto \begin{pmatrix} 0 & 0 & \dots & 0 & \eta^c \\ 1 & 0 & \dots & 0 & 0 \\ 0 & 1 & \dots & 0 & 0 \\ \vdots & \vdots & \ddots & \vdots & \vdots \\ 0 & 0 & \dots & 1 & 0 \end{pmatrix}$$

is realizable over F.

Proof. Let $f = (x-\zeta)(x-\zeta^k)\cdots(x-\zeta^{k^{t-1}})$. As in Lemma 4.4, $f \in F[x]$. Let $M = \frac{F[x]}{(f)}$ and turn M into an FG-module by defining

$$ag(\overline{x}) = \overline{x}g(\overline{x})$$

and

$$bg(\overline{x}) = z(\overline{x})g(\overline{x}^{\varphi(b^{-1})})$$

where $z(x)$ is chosen as in Lemma 4.4 with respect to η^c and $\varphi : \langle b\rangle \to \langle [k]_m\rangle$ is the homomorphism defined by $\varphi(b) = [k]_m$. Recall that by $[k]_m$ we mean $k \pmod{m}$ and naturally, by $\overline{x}^{[i]_m}$ we mean $\overline{x}^i$. This is independent of the representative of $[i]_m$ since $\overline{x}^m = \overline{1}$. Clearly the action of a is well-defined. That the action of b is well-defined follows from Corollary 4.3. Straightforward computation yields $b^n g(\overline{x}) = g(\overline{x})$ while it is obvious that $a^m g(\overline{x}) = g(\overline{x})$. In addition,

$$abg(\overline{x}) = \overline{x}z(\overline{x})g(\overline{x}^{\varphi(b^{-1})}),$$

while

$$ba^k g(\overline{x}) = b\overline{x}^k g(\overline{x}) = z(\overline{x})\overline{x}^{\varphi(b)\varphi(b^{-1})} g(\overline{x}^{\varphi(b^{-1})}) = \overline{x}z(\overline{x})g(\overline{x}^{\varphi(b^{-1})}).$$

It now follows that we have a well-defined action of G on M, thus turning M into an FG-module. Let $L = F(\zeta)$ and let

$$M^L = L \otimes_F M = \frac{L[x]}{(f)}.$$

Then M^L affords the same matrix representation as M relative to $\{1, \overline{x}, \ldots, \overline{x}^{t-1}\}$. We construct a basis $\mathcal{B}$ of $\frac{L[x]}{(f)}$ such that relative to $\mathcal{B}$, the matrix representation afforded by M^L is the given representation.

For $i = 0, 1, \ldots, t-1$, let

$$g_i(\overline{x}) = \frac{f(\overline{x})}{(\overline{x} - \zeta^{k^i}) f'(\zeta^{k^i})},$$

and define

$$\begin{cases} h_0(\overline{x}) &= g_0(\overline{x}), \\ h_1(\overline{x}) &= z(\overline{x}) g_1(\overline{x}), \\ h_2(\overline{x}) &= z(\overline{x}) z(\overline{x}^{\varphi(b^{-1})}) g_2(\overline{x}), \\ \quad \vdots & \quad \vdots \qquad\qquad \vdots \\ h_{t-1}(\overline{x}) &= z(\overline{x}) z(\overline{x}^{\varphi(b^{-1})}) \cdots z(\overline{x}^{\varphi(b^{-(t-2)})}) g_{t-1}(\overline{x}). \end{cases}$$

First observe that $(\overline{x} - \zeta^{k^i}) g_i(\overline{x}) = \overline{0}$ and so $\overline{x} g_i(\overline{x}) = \zeta^{k^i} g_i(\overline{x})$ whence

$$a h_i(\overline{x}) = \zeta^{k^i} h_i(\overline{x})$$

for $i = 0, 1, \ldots, t-1$. Consider now

$$b h_i(\overline{x}) = z(\overline{x}) h_i(\overline{x}^{\varphi(b^{-1})}) = z(\overline{x}) z(\overline{x}^{\varphi(b^{-1})}) \cdots z(\overline{x}^{\varphi(b^{-i})}) g_i(\overline{x}^{\varphi(b^{-1})}).$$

We show that $g_i(\overline{x}^{\varphi(b^{-1})}) = g_{i+1}(\overline{x})$ for all $0 \leq i \leq t-1$ where i is taken modulo t. Indeed,

$$g_i(\overline{x}^{\varphi(b-1)}) = \prod_{v \neq i} \left(\overline{x}^{k^{t-1}} - \zeta^{k^v} \right) / \prod_{v \neq i} \left(\zeta^{k^i} - \zeta^{k^v} \right).$$

Clearly $g_i(x^{\varphi(b-1)})$ vanishes for all ζ^{k^v} except $\zeta^{k^{i+1}}$ when its value is 1. The same holds for $g_{i+1}(x)$ and so we have $b h_i(\overline{x}) = h_{i+1}(\overline{x})$ provided $1 \leq i \leq t-2$. Moreover,

$$b h_{t-1}(\overline{x}) = z(\overline{x}) z(\overline{x}^k) \cdots z(\overline{x}^{k^{t-1}}) g_{t-1}(\overline{x}^{\varphi(b^{-1})}) = \eta^c h_0(\overline{x}).$$

Therefore, as claimed, M^L affords the same matrix representation as the original one. □

Remark. We have an algorithm to obtain the F-representation from the given $F(\zeta)$-representation (once we have found $z(x)$), namely, the matrix for a is the companion matrix of f; the $(i+1)$-st column of the matrix for b is computed as follows: write

$$z(x) x^{ik^{t-1}} = f(x) g(x) + r(x),$$

where $\deg\, r(x) < \deg\, f(x)$. Then the column vector formed by the coefficients of $r(x)$ (coefficient of constant term first) is the $(i+1)$-st column of the matrix for b.

Definition 4.6. Let L be an extension field of F and let ρ be an L-representation of a group G. We say ρ is *completely realizable* over F if ρ is equivalent to an F-representation of G, each of whose irreducible components over L is realizable over F.

Corollary 4.7. *Let the notation be as in Theorem 4.4 and let ρ be the representation $\langle a\rangle$ defined by $\rho(a) = \zeta$. Then ρ^G is completely realizable over $F(=\mathbb{F}_q)$ if and only if $q \equiv k^j \pmod m$ for some j and $q \equiv 1 \pmod r$.*

Proof. By Proposition 2.1, ρ^G is a sum of representations ρ_i of the form dealt with in Theorem 4.5. The sufficiency is thus established. For the necessity we observe first that if ρ^G is completely realizable over F, then F must contain a primitive r-th root of unity since (using the notation of Proposition 2.1 (2)) the characteristic polynomial of $\rho_1(b)$ is $x^t - \eta^{-1}$. In addition the characteristic polynomial of $\rho_1(a)$ remains invariant under the Frobenius automorphism $\tau : y \to y^q$ and so τ must permute the elements of the set $\{\zeta, \zeta^k, \ldots, \zeta^{k^{t-1}}\}$ and so $q \equiv k^j \pmod m$. □

We finish by applying the results obtained to compute a specific example.

Example 4.8. Let $G = \langle a, b \mid a^5 = 1 = b^8,\ b^{-1}ab = a^2\rangle$, with $s = q = 19$. In this case $|2|_5 = 4$, so $t = 4$ and $r = 2$. Also $f = x^4 + x^3 + x^2 + x + 1$. By the general theory, ρ^G is that direct sum of the two irreducible representations ρ_1 and ρ_2 defined by

$$\rho_1(a) = \begin{pmatrix} \zeta & 0 & 0 & 0 \\ 0 & \zeta^2 & 0 & 0 \\ 0 & 0 & \zeta^4 & 0 \\ 0 & 0 & 0 & \zeta^3 \end{pmatrix}, \quad \rho_1(b) = \begin{pmatrix} 0 & 0 & 0 & 1 \\ 1 & 0 & 0 & 0 \\ 0 & 1 & 0 & 0 \\ 0 & 0 & 1 & 0 \end{pmatrix}$$

and

$$\rho_2(a) = \begin{pmatrix} \zeta & 0 & 0 & 0 \\ 0 & \zeta^2 & 0 & 0 \\ 0 & 0 & \zeta^4 & 0 \\ 0 & 0 & 0 & \zeta^3 \end{pmatrix}, \quad \rho_2(b) = \begin{pmatrix} 0 & 0 & 0 & -1 \\ 1 & 0 & 0 & 0 \\ 0 & 1 & 0 & 0 \\ 0 & 0 & 1 & 0 \end{pmatrix}.$$

We first compute a matrix representation $\widehat{\rho}_1$ over $\mathbb{F}_{19}$ equivalent to ρ_1 using the algorithm established above. We know that

$$\widehat{\rho}_1(a) = \begin{pmatrix} 0 & 0 & 0 & -1 \\ 1 & 0 & 0 & -1 \\ 0 & 1 & 0 & -1 \\ 0 & 0 & 1 & -1 \end{pmatrix}.$$

To compute $\widehat{\rho}_1(b)$ we observe that in this case $k^{t-1} = 2^3 = 8$ and so we must find $1 \pmod f$, $x^8 \pmod f$, $x^{16} \pmod f$ and $x^{24} \pmod f$. Since $\overline{x}^5 = \overline{1}$ in $\frac{\mathbb{F}_{19}[x]}{(f)}$ we compute $1 \pmod f$, $x^3 \pmod f$, $x \pmod f$ and $x^4 \pmod f$. We get $1, x^3, x$ and

$-1-x-x^2-x^3$. Hence

$$\widehat{\rho}_1(b) = \begin{pmatrix} 1 & 0 & 0 & -1 \\ 0 & 0 & 1 & -1 \\ 0 & 0 & 0 & -1 \\ 0 & 1 & 0 & -1 \end{pmatrix}.$$

To compute a matrix representation $\widehat{\rho}_2$ over $\mathbb{F}_{19}$ equivalent to ρ_2 we must compute $z(x)$. We have $\zeta^4+\zeta^3+\zeta^2+\zeta+1=0$ and so $\zeta^2+\zeta^{-2}+\zeta+\zeta^{-1}+1=0$. But $(\zeta+\zeta^{-1})^2=\zeta^2+\zeta^{-2}+2$, whence $\zeta^2+\zeta^{-2}=(\zeta+\zeta^{-1})^2-2$. Letting $\omega=\zeta+\zeta^{-1}$ we get $\omega^2+\omega-1=0$. Hence

$$\omega = \frac{-1\pm\sqrt{5}}{2} = \frac{-1\pm 9}{2}.$$

Thus $\omega=4$ or $\omega=-5$ from which it follows that

$$x^4+x^3+x^2+x+1 = (x^2-4x+1)(x^2+5x+1).$$

We may assume ζ is a root of x^2-4x+1. Adopting the notation established above, we have $f=f_1f_2$, $\widehat{f_1}=x^2+5x+1$ and $\widehat{f_2}=x^2-4x+1$.

We must find an element $z\in\mathbb{F}_{19}(\zeta)$ whose norm is -1. Let $z=a_0+a_1\zeta$. We require $(a_0+a_1\zeta)(a_0+a_1\zeta^{-1})=-1$, *i.e.*, $a_0^2+a_0a_1(\zeta+\zeta^{-1})+a_1^2=-1$. But $\zeta+\zeta^{-1}=4$ and so $a_0^2+4a_0a_1+a_1^2+1=0$. Dividing by a_1^2 and setting $x=\frac{a_0}{a_1}$ we get

$$x^2+4x+\frac{a_1^2+1}{a_1^2}=0.$$

Solving for x we have $x=-2\pm\frac{\sqrt{3a_1^2-1}}{a_1}$. Let $a_1=2$. Then

$$x=-2\pm\frac{\sqrt{11}}{2}=-2\pm\frac{7}{2}=-2\pm 6.$$

Hence $x=-8$ or $x=4$. Taking $\frac{a_0}{2}=-8$ we get $a_0=3$. Hence $z=3+2\zeta$ and so $z_1(x)=2x+3$. A routine computation establishes that

$$1=(2x-8)(x^2+5x+1)+(-2x+9)(x^2-4x+1).$$

Hence $h_1(x)=(2x-8)$ and $h_2(x)=-2x+9$. It follows that

$$z(x)=(2x-8)(x^2+5x+1)(2x+3)+(-2x+9)(x^2-4x+1).$$

Taking $z(x)$ modulo f (by abuse of notation) we have $z(x)=4x^3-x$. Once again,

$$\widehat{\rho}_2(a) = \begin{pmatrix} 0 & 0 & 0 & -1 \\ 1 & 0 & 0 & -1 \\ 0 & 1 & 0 & -1 \\ 0 & 0 & 1 & -1 \end{pmatrix}.$$

Now

$$\begin{cases} b\cdot 1 &= 4\overline{x}^3-\overline{x}, \\ b\overline{x} &= (4\overline{x}^3-\overline{x})\overline{x}^8, \\ b\overline{x}^2 &= (4\overline{x}^3-\overline{x})\overline{x}^{16}, \\ b\overline{x}^3 &= (4\overline{x}^3-\overline{x})\overline{x}^{24}. \end{cases}$$

Reducing modulo f we get

$$\begin{cases} b \cdot 1 &= 4\overline{x}^3 - \overline{x}, \\ b\overline{x} &= \overline{x}^3 + \overline{x}^2 + 5\overline{x} + 1, \\ b\overline{x}^2 &= -4\overline{x}^3 - 5\overline{x}^2 - 4\overline{x} - 4, \\ b\overline{x}^3 &= 4\overline{x}^2 - 1. \end{cases}$$

Thus

$$b \to \begin{pmatrix} 0 & 1 & -4 & -1 \\ -1 & 5 & -4 & 0 \\ 0 & 1 & -5 & 4 \\ 4 & 1 & -4 & 0 \end{pmatrix}.$$

Remark. We have obtained necessary and sufficient conditions for the realizability of ρ^G over $\mathbb{F}_q$ in the case that $|b| = |k|_m$. Furthermore, in the case when $|b|$ does not necessarily coincide with $|k|_m$ and $q \equiv 1 \pmod{r}$, we have given the necessary and sufficient conditions for the complete realizability of ρ^G over $\mathbb{F}_q$. There remains the problem of the mere realizability of ρ^G over $\mathbb{F}_q$ when $|b| \neq |k|_m$. We observe in fact that the condition $q \equiv k^j \pmod{m}$ for some j is, even in this case, a necessary and sufficient condition for the realizability of ρ^G over $\mathbb{F}_q$ provided $(q, |G|) = 1$. (Observe that throughout we are tacitly assuming that $(m, q) = 1$ so that to require $(q, |G|) = 1$ we need only assume $(n, q) = 1$.) Indeed the necessity follows from looking at the characteristic polynomial of $\rho^G(a)$ while the sufficiency follows from the fact that ρ^G is completely realizable over $\mathbb{F}_q$ by Corollary 4.7. Alternatively one could possibly obtain the sufficiency from two facts, namely:

(i) if $q \equiv k^j \pmod{m}$, then $tr\rho^G(g) \in \mathbb{F}_q$ for all $g \in G$;

(ii) the Schur index of a representation over a finite field is 1 provided $(q, |G|) = 1$ [Dor, Theorem 24.10].

Nevertheless, the whole thrust of this paper is to explicitly construct the representations in question. This could not be done by merely appealing to the Schur index.

A number of new interesting problems arise from the paper. We end the paper by listing a few of them:

(1) Examine the case when $(n, q) \neq 1$.

(2) Find a reciprocity law for other finite and also algebraic groups.

(3) Extend reciprocity laws to cover fields which are not necessarily finite.

(4) Find further applications to and relations with number-theoretic reciprocity laws.

Acknowledgements. We thank Franz Lemmermeyer for his interest in this paper, and we thank the referee for his careful reading of our paper and for his valuable suggestions which helped us to improve our exposition. In particular we added the referee's alternate and nice proof of Lemma 2.3. The first author was supported in part by NFIG (New Faculty Initiative Grant) at ISU. The second author was supported in part by NSERC grant #0370A01.

REFERENCES

[Ank] N. C. Ankeny, *Criterion for rth power residuacity*, Pacific J. Math. **10** (1960), no. 4, 1115–1124.

[Art] E. Artin, *Zur Theorie der L-Reihen mit allgemeinen Gruppencharakteren,* Abh. Math. Sem. Univ. Hamburg **8** (1930), 292–306. (Emil Artin, collected papers, Edited by S. Lang and J. Tate, Springer-Verlag, New York 1965.)

[BH] M. Behrens and M. J. Hopkins, *Higher real K-theories and topological automorphic forms*, preprint 2009.

[Dor] L. Dornhoff, *Group representation theory*, in Part A: Ordinary representation theory. Pure and Applied Mathematics **7**, Marcel Dekker, Inc., New York, 1971, vii+pp, 1–254.

[Gau] C.F. Gauss, *Disquisitiones arithmeticae*, Translated into English by Arthur A. Clarke, S. J. Yale University Press, New Haven, Conn.-London, 1966, xx+472 pp.

[Her] I.N. Herstein, *Noncommutative rings*, The Carus Mathematical Monographs, No. 15, Published by The Mathematical Association of America; distributed by John Wiley & Sons, Inc., New York, 1968, xi+199 pp.

[I-R] K.F. Ireland and M.I. Rosen, *A classical introduction to modern number theory*, in Revised edition of *Elements of number theory*, Graduate Texts in Mathematics, **84**, Springer-Verlag, New York-Berlin, 1982. xiii+341 pp.

[Jac] N. Jacobson, *Basic algebra II*, W. H. Freeman and Co., San Francisco, Calif., 1980. xix+666 pp.

[Lan] R.P. Langlands, *Problems in the theory of automorphic forms*, Lectures in modern analysis and applications, III, pp. 18–61, Lecture Notes in Math., Vol. 170, Springer, Berlin, 1970.

[Lem] F. Lemmermeyer, *Galois action on class groups*, J. Algebra **264** (2003), no. 2, 553–564.

[M-R] J. Mináč and C. Reis, *Trigonometry in finite fields*, Exposition. Math. **11** (1993), no. 2, 97–108.

[Rei] I. Reiner, *Maximal orders*, London Mathematical Society Monographs, No. 5, Academic Press [A subsidiary of Harcourt Brace Jovanovich, Publishers], London-New York, 1975, xii+395 pp.

[Ser1] J.-P. Serre, *Linear representations of finite groups*, Translated from the second French edition by Leonard L. Scott, Graduate Texts in Mathematics, Vol. 42, Springer-Verlag, New York-Heidelberg, 1977, x+170 pp.

[Ser2] J.-P. Serre, *A course in arithmetic*, Translated from the French, Graduate Texts in Mathematics, No. 7, Springer-Verlag, New York-Heidelberg, 1973, viii+115 pp.

[Syl] J.-J. Sylvester, *Sur les diviseurs des fonctions cyclotomiques*, Comptes Rendu, XC, 1880, 287–289, 345–347. (Also in *The collected mathematical papers of James Joseph Sylvester,* Vol. II, 428–432.)

[Tat] J. Tate, *Number theoretic background* in Automorphic forms, representations and L-functions (Proc. Sympos. Pure Math., Oregon State Univ., Corvallis, Ore., 1977), Part 2, pp. 3–26, Proc. Sympos. Pure Math. **XXXIII**, Amer. Math. Soc., Providence, R.I., 1979.

S. CHEBOLU, DEPT. OF MATH., ILLINOIS STATE U., NORMAL, IL, USA.
schebol@ilstu.edu

J. MINÁČ, DEPT. OF MATH., U. OF WESTERN ONTARIO, LONDON, ON, CANADA.
minac@uwo.ca

C. REIS, 222 B SAINT CHARLES ST., VICTORIA, BC, CANADA.
c.m.reis@shaw.ca