FIELDS GENERATED BY CHARACTERS OF FINITE LINEAR GROUPS

MADELINE LOCUS DAWSEY, KEN ONO*, AND IAN WAGNER

ABSTRACT. In previous work [2], the authors confirmed the speculation of J. G. Thompson that certain multiquadratic fields are generated by specified character values of sufficiently large alternating groups A_n. Here we address the natural generalization of this speculation to the finite general linear groups $\mathrm{GL}_m(\mathbb{F}_q)$ and $\mathrm{SL}_2(\mathbb{F}_q)$.

1. Introduction and Statement of Results

Let G be a finite group, and let $K(G)$ denote the field generated over $\mathbb{Q}$ by the character values of G. G. R. Robinson and J. G. Thompson [6] proved for alternating groups A_n that the $K(A_n)$ are generally large multiquadratic extensions of $\mathbb{Q}$. For $n > 24$, they proved that

$$K(A_n) = \mathbb{Q}\left(\{\sqrt{p^*} \ : \ p \leq n \text{ an odd prime with } p \neq n-2\}\right),$$

where $m^* := (-1)^{\frac{m-1}{2}} m$ for any odd integer m.

In a letter [9] to the second author in 1994, Thompson asked whether a refinement of this result exists that is analogous to the Kronecker–Weber Theorem and the theory of complex multiplication, where abelian extensions are generated by the values of suitable functions at arguments which determine the ramified primes. Instead of adjoining special values of analytic functions to number fields, which is the substance of *Hilbert's 12th Problem* [5], Thompson suggested adjoining character values of A_n.

The authors recently answered this question [2]. Let $\pi := \{p_1, p_2, \dots, p_t\}$ be a set of $t \geq 2$ distinct odd primes[1] listed in increasing order. A π-*number* is a positive integer whose prime factors belong to π. Thompson's prediction was that in general $K_\pi(A_n)$, the field generated over $\mathbb{Q}$ by the values of A_n-characters restricted to elements σ of A_n with π-number order, should be the field $\mathbb{Q}(\sqrt{p_1^*}, \sqrt{p_2^*}, \dots, \sqrt{p_t^*})$. Although counterexamples exist for each π, the authors proved [2], for sufficiently large n, that

$$K_\pi(A_n) = \mathbb{Q}\left(\sqrt{p_1^*}, \sqrt{p_2^*}, \dots, \sqrt{p_t^*}\right).$$

In this note we consider Thompson's problem for the finite general linear groups $\mathrm{GL}_m(\mathbb{F}_q)$ and $\mathrm{SL}_2(\mathbb{F}_q)$, where $\mathbb{F}_q$ is a finite field. Throughout, we let p be a prime, and let $q := p^n$. Let ζ_n denote the nth root of unity $\zeta_n := e^{2\pi i/n}$, and let $\mathbb{Z}_n^\times := (\mathbb{Z}/n\mathbb{Z})^\times$. Thanks to classical work of Green [4], it is not difficult to determine the number fields generated by the $\mathrm{GL}_m(\mathbb{F}_q)$-character values. To ease notation, for positive integers $d, r \in \mathbb{Z}^+$, we let

$$\omega_d(r) := \sum_{k=0}^{d-1} \zeta_{q^d-1}^{rq^k}. \tag{1.1}$$

2010 *Mathematics Subject Classification.* 20B30, 20C30, 11R20.

Key words and phrases. Hilbert's 12th Problem, group characters.

*This author thanks the generous support of the Asa Griggs Candler Fund at Emory University, the Thomas Jefferson Fund at the University of Virginia, and the NSF (DMS-1601306).

[1]The phenomenon cannot hold when $t = 1$ for any $n \not\equiv 0, 1 \pmod{p}$.

Theorem 1.1. *If $m \geq 2$, then we have*

$$K\left(\mathrm{GL}_m\left(\mathbb{F}_q\right)\right) = \mathbb{Q}\left(\left\{\omega_d(r) \ : \ 1 \leq d \leq m \text{ and } r \in \mathbb{Z}_{q^d-1}^{\times}\right\}\right).$$

Turning to Thompson's speculation, we determine the subfields of $K\left(\mathrm{GL}_m\left(\mathbb{F}_q\right)\right)$ generated by the character values of elements of prime power order ℓ^r. Confirming Thompson's speculation, we find that these fields systematically correspond to subfields with ramification only at ℓ. Let ℓ be prime, and let $r \geq 1$ be an integer. Define $K_{\ell^r}\left(\mathrm{GL}_m\left(\mathbb{F}_q\right)\right)$ to be the field generated over $\mathbb{Q}$ by the values of $\mathrm{GL}_m\left(\mathbb{F}_q\right)$-characters evaluated at elements of order ℓ^r. For primes $\ell \neq p$, we let $\mathrm{ord}_{\ell^r}(q)$ denote the multiplicative order of q modulo ℓ^r.

Theorem 1.2. *Suppose that $\ell \neq p$ is an odd prime. If there is an element of order ℓ^r in $\mathrm{GL}_m\left(\mathbb{F}_q\right)$, then $K_{\ell^r}\left(\mathrm{GL}_m\left(\mathbb{F}_q\right)\right)$ is the unique subfield of $\mathbb{Q}\left(\zeta_{\ell^r}\right)$ of degree $\frac{\ell^{r-1}(\ell-1)}{\mathrm{ord}_{\ell^r}(q)}$ over $\mathbb{Q}$.*

Remark. *If $\tau_q \in \mathrm{Gal}\left(\mathbb{Q}\left(\zeta_{\ell^r}\right)/\mathbb{Q}\right)$ satisfies $\tau_q\left(\zeta_{\ell^r}\right) = \zeta_{\ell^r}^q$, then $K_{\ell^r}\left(\mathrm{GL}_m\left(\mathbb{F}_q\right)\right) = \mathbb{Q}\left(\zeta_{\ell^r}\right)^{\langle\tau_q\rangle}$.*

Remark. *If $\ell = p$, then $K_{\ell}\left(\mathrm{GL}_m\left(\mathbb{F}_q\right)\right) = \mathbb{Q}$, as shown in Section 3. The proof of Theorem 1.2 also shows that $K_2\left(\mathrm{GL}_m\left(\mathbb{F}_q\right)\right) = \mathbb{Q}$ and that*

$$K_4\left(\mathrm{GL}_m\left(\mathbb{F}_q\right)\right) = \begin{cases} \mathbb{Q}(i) & q \equiv 1 \pmod 4 \\ \mathbb{Q} & \text{otherwise.} \end{cases}$$

If $\ell^r = 2^r$ for $r > 2$, then it is not always clear which fields are generated by character values at elements of order 2^r, since $\mathrm{Gal}\left(\mathbb{Q}\left(\zeta_{2^r}\right)/\mathbb{Q}\right)$ is no longer cyclic.

Now we turn to the case of the groups $\mathrm{SL}_2\left(\mathbb{F}_q\right)$.

Theorem 1.3. *Assuming the notation above, we have that*

$$K\left(\mathrm{SL}_2\left(\mathbb{F}_q\right)\right) = \begin{cases} \mathbb{Q}\left(\zeta_{q-1} + \zeta_{q-1}^{-1}, \zeta_{q+1} + \zeta_{q+1}^{-1}\right) & \text{if } p = 2, \\ \mathbb{Q}\left(\sqrt{q^*}, \zeta_{q-1} + \zeta_{q-1}^{-1}, \zeta_{q+1} + \zeta_{q+1}^{-1}\right) & \text{if } p > 2. \end{cases}$$

Regarding Thompson's speculation for these groups, we obtain the following result.

Theorem 1.4. *If there is an element of order ℓ^r in $\mathrm{SL}_2\left(\mathbb{F}_q\right)$, then the following are true.*

(1) If $p = 2$, then we have that

$$K_{\ell^r}\left(\mathrm{SL}_2\left(\mathbb{F}_q\right)\right) = \begin{cases} \mathbb{Q}\left(\zeta_{\ell^r} + \zeta_{\ell^r}^{-1}\right) & \text{if } q \equiv \pm 1 \pmod{\ell^r}, \\ \mathbb{Q} & \text{if } q \equiv 0 \pmod{\ell^r}. \end{cases}$$

(2) If $p > 2$, then we have that

$$K_{\ell^r}\left(\mathrm{SL}_2\left(\mathbb{F}_q\right)\right) = \begin{cases} \mathbb{Q}\left(\zeta_{\ell^r} + \zeta_{\ell^r}^{-1}\right) & \text{if } q \equiv \pm 1 \pmod{\ell^r}, \\ \mathbb{Q}\left(\sqrt{q^*}\right) & \text{if } q \equiv 0 \pmod{\ell^r}. \end{cases}$$

Remark. *C. Bonnafé [1] and T. Shoji [7, 8] gave a method for computing the characters of $\mathrm{SL}_m(\mathbb{F}_q)$ when $m \geq 3$. We ask whether Theorems 1.3 and 1.4 can be extended using their work.*

This paper is organized as follows. In Section 2, we recall some classic facts from the representation theory of $\mathrm{GL}_2\left(\mathbb{F}_q\right)$ and $\mathrm{SL}_2\left(\mathbb{F}_q\right)$. These facts allow us to deduce Theorems 1.3 and 1.4, and Theorems 1.1 and 1.2 when $m = 2$. In Section 3, we recall essential features of the classical work of Green [4] on the representation theory of $\mathrm{GL}_m\left(\mathbb{F}_q\right)$, which we then use to prove Theorems 1.1 and 1.2 for ranks $m \geq 3$.

Acknowledgements

The authors thank John Duncan, John G. Thompson and Pham Tiep for helpful conversations.

2. Rank 2 Finite Linear Groups

In Section 2.1 we establish the rank 2 cases of Theorems 1.1 and 1.2, and we prove Theorems 1.3 and 1.4 in Section 2.2.

2.1. **The $\mathrm{GL}_2(\mathbb{F}_q)$ cases.** For completeness, we recall the construction of the character tables of $\mathrm{GL}_2(\mathbb{F}_q)$ following the treatment in [3]. It is well-known that $\mathbb{F}_{q^2}^\times$ is isomorphic to a large cyclic subgroup of $\mathrm{GL}_2(\mathbb{F}_q)$. When q is odd, we make this isomorphism explicit by choosing a generator ϵ of $\mathbb{F}_q^\times$ and a square root $\sqrt{\epsilon}$ in $\mathbb{F}_{q^2}^\times$. Then 1 and $\sqrt{\epsilon}$ form a basis for $\mathbb{F}_{q^2}^\times$ as a vector space over $\mathbb{F}_q$. We therefore make the identification

$$\left\{ \begin{pmatrix} x & \epsilon y \\ y & x \end{pmatrix} \right\} \cong \mathbb{F}_{q^2}^\times, \qquad \begin{pmatrix} x & \epsilon y \\ y & x \end{pmatrix} \longleftrightarrow \zeta = x + \sqrt{\epsilon}\, y. \tag{2.1}$$

When q is even, we let d_ζ denote the matrix that is identified with the element $\zeta \in \mathbb{F}_{q^2}^\times$ as above. In particular, the order of d_ζ in $\mathrm{GL}_2(\mathbb{F}_q)$ is equal to the order of ζ in $\mathbb{F}_{q^2}^\times$.

The conjugacy classes of $\mathrm{GL}_2(\mathbb{F}_q)$ are given in the table below.

Representative	# elements	# classes
$a_x = \left(\begin{smallmatrix} x & 0 \\ 0 & x \end{smallmatrix}\right)$	1	$q-1$
$b_x = \left(\begin{smallmatrix} x & 1 \\ 0 & x \end{smallmatrix}\right)$	q^2-1	$q-1$
$c_{x,y} = \left(\begin{smallmatrix} x & 0 \\ 0 & y \end{smallmatrix}\right),\ \ x \neq y$	q^2+q	$\dfrac{(q-1)(q-2)}{2}$
$d_\zeta,\ \zeta \in \mathbb{F}_{q^2} \setminus \mathbb{F}_q$	q^2-q	$\dfrac{q(q-1)}{2}$

Table 1. Conjugacy classes of $\mathrm{GL}_2(\mathbb{F}_q)$

We now turn to the construction of the character table. The group $\mathbb{F}_q^\times = \{1, a, \ldots, a^{q-2}\}$ has $q-1$ characters, say $\alpha_k : \mathbb{F}_q^\times \longrightarrow \mathbb{C}^\times$, defined by $\alpha_k(a) := \zeta_{q-1}^{k-1}$ for $1 \leq k \leq q-1$. Similarly, the multiplicative group $\mathbb{F}_{q^2}^\times$ has q^2-1 characters which we denote by ϕ_n, for $1 \leq n \leq q^2-1$.

We employ these characters to describe $\mathrm{Irr}(\mathrm{GL}_2(\mathbb{F}_q))$, the q^2-1 irreducible representations of $\mathrm{GL}_2(\mathbb{F}_q)$. The permutation representation of $\mathrm{GL}_2(\mathbb{F}_q)$ on $\mathbb{P}^1(\mathbb{F}_q)$ has dimension $q+1$ and contains the trivial representation. The complementary q-dimensional representation is irreducible and will be denoted by V. There are also $q-1$ irreducible one-dimensional representations U_k given by $U_k(g) = \alpha_k(\det(g))$. Note that $\det(d_\zeta) = N_{\mathbb{F}_{q^2}/\mathbb{F}_q}(\zeta) = \zeta^{q+1}$. The $q-1$ representations given by $V_k = V \otimes U_k$ are also irreducible. For each pair α_j, α_k of characters of $\mathbb{F}_q^\times$, there is a character ψ of the subgroup B, the Borel subgroup consisting of upper triangular matrices, such that

$$\psi : \begin{pmatrix} a & b \\ 0 & d \end{pmatrix} \longmapsto \alpha_j(a)\alpha_k(d).$$

Let $W_{j,k}$ be the representation of $\mathrm{GL}_2(\mathbb{F}_q)$ induced from the representation of B associated to ψ. Note that $W_{j,j} \cong U_j \oplus V_j$ and $W_{j,k} \cong W_{k,j}$, and that there are $(q-1)(q-2)/2$ representations $W_{j,k}$ of dimension $q+1$ for $j \neq k$. It can be shown that the final $q(q-1)/2$ irreducible

representations arise from the characters ϕ of $\mathbb{F}_{q^2}^\times$ with $\phi \neq \phi^q$ and $\phi|_{\mathbb{F}_q^\times} = \alpha_k$ for some k. We denote these representations by X_ϕ. To summarize, we have the following table.

$\mathrm{GL}_2(\mathbb{F}_q)$	$a_x = \begin{pmatrix} x & 0 \\ 0 & x \end{pmatrix}$	$b_x = \begin{pmatrix} x & 1 \\ 0 & x \end{pmatrix}$	$c_{x,y} = \begin{pmatrix} x & 0 \\ 0 & y \end{pmatrix}$, $x \neq y$	d_ζ, $\zeta \in \mathbb{F}_{q^2} \setminus \mathbb{F}_q$
U_k	$\alpha_k(x^2)$	$\alpha_k(x^2)$	$\alpha_k(xy)$	$\alpha_k(\zeta^{q+1})$
V_k	$q\alpha_k(x^2)$	0	$\alpha_k(xy)$	$-\alpha_k(\zeta^{q+1})$
$W_{j,k}$	$(q+1)\alpha_j(x)\alpha_k(x)$	$\alpha_j(x)\alpha_k(x)$	$\alpha_j(x)\alpha_k(y) + \alpha_j(y)\alpha_k(x)$	0
X_ϕ	$(q-1)\phi(x)$	$-\phi(x)$	0	$-(\phi(\zeta) + \phi(\zeta^q))$

Table 2. Character table of $\mathrm{GL}_2(\mathbb{F}_q)$

We now describe the character values of $\mathrm{GL}_2(\mathbb{F}_q)$ based on the group orders. To this end, we first determine these orders. It is clear that the order of a_x in $\mathrm{GL}_2(\mathbb{F}_q)$ is equal to the order of x in $\mathbb{F}_q^\times$. Therefore, for each $d \mid (q-1)$, there are $\varphi(d)$ conjugacy classes $[a_x]$ consisting of elements of order d, where φ denotes Euler's totient function. Notice that

$$b_x^n = \begin{pmatrix} x^n & nx^{n-1} \\ 0 & x^n \end{pmatrix},$$

so in order for b_x^n to be the identity matrix, we must have that the order of x divides n and $n \equiv 0 \pmod{p}$. Since the order of x is coprime to p, we have that for each $d \mid (q-1)$, there are $\varphi(d)$ conjugacy classes $[b_x]$ consisting of elements of order pd. The order of $c_{x,y}$ is the least common multiple of the order of x and the order of y. Therefore, for each $d > 1$ with $d \mid (q-1)$, there are $\varphi(d)\left(d - \frac{\varphi(d)+1}{2}\right)$ conjugacy classes $[c_{x,y}]$ consisting of elements of order d. Finally, for each $d \mid (q^2-1)$ with $d \nmid (q-1)$, there are $\varphi(d)/2$ conjugacy classes $[d_\zeta]$ consisting of elements of order d.

Define $K_d(G) := \mathbb{Q}(\{\chi(g) : g \in G \text{ has order } d \text{ and } \chi \in \mathrm{Irr}(G)\})$. We have the following lemma relating character values at elements of order d to those at elements of order pd.

Lemma 2.1. *If $d \mid (q-1)$, then $K_d(\mathrm{GL}_2(\mathbb{F}_q)) = K_{pd}(\mathrm{GL}_2(\mathbb{F}_q)) = \mathbb{Q}(\zeta_d)$.*

Proof. The conjugacy classes $[a_x]$ and $[c_{x,y}]$ may contain elements of order $d \mid (q-1)$. It suffices to restrict our attention to the values of the character U_k at elements in the conjugacy classes $c_{x,1}$, where x has order d. The value of U_2 is $\alpha_2(xy) = \alpha_2(x) = \zeta_{q-1}^t$ for some $0 \leq t \leq q-2$. Since the order of x is d, we must have that $\zeta_{q-1}^t = \zeta_d^r$ for some r coprime to d. In fact, cycling through all of the characters α_k shows that every dth root of unity actually appears as a character value for $d \mid (q-1)$.

We now turn to the conjugacy classes $[b_x]$ with elements of order pd. For such elements b_x, the corresponding element x of $\mathbb{F}_q^\times$ must have order d. Therefore, the desired dth roots of unity arise as the values of the characters $W_{j,1}$, $1 \leq j \leq q-1$, and the values of X_ϕ. □

Lemma 2.2. *Suppose that $d \mid (q^2-1)$ but $d \nmid (q-1)$. Then*

$$K_d(\mathrm{GL}_2(\mathbb{F}_q)) = \mathbb{Q}(\{\zeta_d^r + \zeta_d^{qr} : 1 \leq r \leq d\}).$$

Proof. The only conjugacy classes containing elements of order $d \mid (q^2-1)$ with $d \nmid (q-1)$ are the classes $[d_\zeta]$, where $\zeta = x + \sqrt{\epsilon}\, y$ has order d in $\mathbb{F}_{q^2}^\times$. It is then clear that the desired sums $\zeta_d^r + \zeta_d^{qr}$ arise from the values of the characters X_ϕ at these elements. □

It is natural to ask which fields are generated by the sums of roots of unity appearing in Lemma 2.2. Here we make some initial observations for small values of d. In order for the conditions of Lemma 2.2 to hold, we must have that $q^2 \equiv 1 \pmod{d}$ and $q \not\equiv 1 \pmod{d}$. For some small values of d, the only solutions to this pair of congruences are $q \equiv -1 \pmod{d}$. In these special cases, we can identify the fields in question. For example, if $d = 3, 4, 6$ and $q \equiv -1 \pmod{d}$, then $\zeta_d^r + \zeta_d^{-r} \in \mathbb{Z}$, and so $K_d(\mathrm{GL}_2(\mathbb{F}_q)) = \mathbb{Q}$. If $d = 5$ and $q \equiv -1 \pmod{d}$, then $\zeta_5^r + \zeta_5^{-r} = \frac{1}{2}\left(-1 + \left(\frac{r}{5}\right)\sqrt{5}\right)$, and so $K_5(\mathrm{GL}_2(\mathbb{F}_q)) = \mathbb{Q}(\sqrt{5})$. If $d = 8$ and $q \equiv -1 \pmod{d}$, then a similar argument implies that

$$K_8(\mathrm{GL}_2(\mathbb{F}_q)) = \begin{cases} \mathbb{Q}(\zeta_8) & \text{if } q \equiv 1 \pmod 8, \\ \mathbb{Q}\left(\sqrt{-2}\right) & \text{if } q \equiv 3 \pmod 8, \\ \mathbb{Q}(i) & \text{if } q \equiv 5 \pmod 8, \\ \mathbb{Q}\left(\sqrt{2}\right) & \text{if } q \equiv 7 \pmod 8. \end{cases}$$

For general orders d, Lemmas 2.1 and 2.2 imply the following two theorems, which are restatements of Theorems 1.1 and 1.2 for $m = 2$.

Theorem 2.3. *We have that*

$$K(\mathrm{GL}_2(\mathbb{F}_q)) = \mathbb{Q}\left(\zeta_{q-1}, \left\{\zeta_{q^2-1}^r + \zeta_{q^2-1}^{qr} \ : \ 1 \le r \le \frac{q^2-1}{2}\right\}\right).$$

The previous theorem, and the following theorem addressing Thompson's speculation, prove the rank 2 cases of Theorems 1.1 and 1.2.

Theorem 2.4. *Suppose that ℓ is an odd prime and that there is an element of order ℓ^r in $\mathrm{GL}_2(\mathbb{F}_q)$. Then we have that*

$$K_{\ell^r}(\mathrm{GL}_2(\mathbb{F}_q)) = \begin{cases} \mathbb{Q}(\zeta_{\ell^r}) & \text{if } q \equiv 1 \pmod{\ell^r}, \\ \mathbb{Q}\left(\zeta_{\ell^r} + \zeta_{\ell^r}^{-1}\right) & \text{if } q \equiv -1 \pmod{\ell^r}, \\ \mathbb{Q} & \text{if } q \equiv 0 \pmod{\ell^r}. \end{cases}$$

Remark. The number field $\mathbb{Q}\left(\zeta_{\ell^r} + \zeta_{\ell^r}^{-1}\right)$ is the maximal totally real subfield of the cyclotomic field $\mathbb{Q}(\zeta_{\ell^r})$ and has degree $\frac{\ell^{r-1}(\ell-1)}{2}$ over $\mathbb{Q}$.

The case when $\ell = 2$ is more complicated than the cases described above. In this case, it is possible that $q \equiv 2t + 1 \pmod{2^r}$ for any $0 \le t \le 2^{r-1} - 1$. However, there are still a few congruence classes of q that yield simple fields. For example, if $q \equiv \pm 1 \pmod{2^r}$, then the conclusion of Theorem 2.4 holds. If $q \equiv 2^{r-1} \pm 1 \pmod{2^r}$, then we have that

$$K_{2^r}(\mathrm{GL}_2(\mathbb{F}_q)) = \begin{cases} \mathbb{Q}\left(\zeta_{2^{r-1}} + \zeta_{2^{r-1}}^{-1}, \zeta_{2^r} - \zeta_{2^r}^{-1}\right) & \text{if } q \equiv 2^{r-1} - 1 \pmod{2^r}, \\ \mathbb{Q}(\zeta_{2^{r-1}}) & \text{if } q \equiv 2^{r-1} + 1 \pmod{2^r}. \end{cases}$$

2.2. **Proof of Theorems 1.3 and 1.4.** As in the previous subsection, the proofs follow from the explicit description of the character tables of $\mathrm{SL}_2(\mathbb{F}_q)$. We consider the cases where q is odd (resp. even) separately.

2.2.1. *The case when q is odd.* When q is odd, the conjugacy class $[b_1]$ in $\mathrm{GL}_2(\mathbb{F}_q)$ splits into two conjugacy classes $[b_{1,1}]$ and $[b_{1,\epsilon}]$ in $\mathrm{SL}_2(\mathbb{F}_q)$, and the conjugacy class $[b_{-1}]$ splits into $[b_{-1,1}]$ and $[b_{-1,\epsilon}]$. These split conjugacy classes are given by the following table.

Representative	# elements	# classes
$\left(\begin{smallmatrix}1&0\\0&1\end{smallmatrix}\right)$	1	1
$\left(\begin{smallmatrix}-1&0\\0&-1\end{smallmatrix}\right)$	1	1
$b_{1,1}=\left(\begin{smallmatrix}1&1\\0&1\end{smallmatrix}\right)$	$\frac{q^2-1}{2}$	1
$b_{1,\epsilon}=\left(\begin{smallmatrix}1&\epsilon\\0&1\end{smallmatrix}\right)$	$\frac{q^2-1}{2}$	1
$b_{-1,1}=\left(\begin{smallmatrix}-1&1\\0&-1\end{smallmatrix}\right)$	$\frac{q^2-1}{2}$	1
$b_{-1,\epsilon}=\left(\begin{smallmatrix}-1&\epsilon\\0&-1\end{smallmatrix}\right)$	$\frac{q^2-1}{2}$	1
$c_x=\left(\begin{smallmatrix}x&0\\0&x^{-1}\end{smallmatrix}\right)$, $x\neq\pm1$	q^2+q	$\frac{q-3}{2}$
$d_\zeta=\left(\begin{smallmatrix}x&\epsilon y\\y&x\end{smallmatrix}\right)$, $x\neq\pm1$, $y\neq0$, $\zeta^{q+1}=1$	q^2-q	$\frac{q-1}{2}$

Table 3. Split conjugacy classes of $\mathrm{SL}_2(\mathbb{F}_q)$ for odd q

Define the set $C:=\left\{\zeta\in\mathbb{F}_{q^2}^{\times}:\zeta^{q+1}=1\right\}$. Here we give the restrictions of the representations of $\mathrm{GL}_2(\mathbb{F}_q)$ to $\mathrm{SL}_2(\mathbb{F}_q)$. All of the representations U_k restrict to the trivial representation U. The restriction V of V_k is also an irreducible representation. The restriction W_j of $W_{j,1}$ is irreducible if $\alpha_j^2\neq1$. It is also clear that $W_j\cong W_k$ if $j=\pm k$, and so there are $(q-3)/2$ irreducible representations W_j of dimension $q+1$. If τ is the nontrivial quadratic character of $\mathbb{F}_q^{\times}$, then $W_\tau=W'\oplus W''$, where both W' and W'' are irreducible representations. The restriction of X_ϕ is determined by the restriction of ϕ to C. The restrictions of ϕ and ϕ^{-1} to C yield the same character, so that if $\phi^2\neq1$, then there are $(q-1)/2$ irreducible representations of dimension $q-1$. If ψ is the nontrivial quadratic character of C, then $X_\psi=X'\oplus X''$, where both X' and X'' are irreducible. To complete the character table of $\mathrm{SL}_2(\mathbb{F}_q)$, it remains to identify the irreducible representations W',W'',X' and X''. By studying the index two subgroup $H\subset\mathrm{GL}_2(\mathbb{F}_q)$ of matrices with square determinant, one can show that W' and W'' are conjugate representations of dimension $(q+1)/2$, and X' and X'' are conjugate representations of dimension $(q-1)/2$. On non-split conjugacy classes, the character values of W',W'' and X',X'' are half the character values of W_j and X_ψ, respectively. On the split conjugacy classes, the character values can be determined from character relations.

The character table of $\mathrm{SL}_2(\mathbb{F}_q)$ in the case when q is odd is shown below. We note that $\tau(-1)=\psi(-1)=(-1)^{(q-1)/2}$ and $\tau(\epsilon)=-1$.

$\mathrm{SL}_2(\mathbb{F}_q)$ q odd	2 $\begin{pmatrix}\pm1&0\\0&\pm1\end{pmatrix}$	$\frac{q^2-1}{2}$ $b_{x,y}=\begin{pmatrix}x&y\\0&x\end{pmatrix}$, $x\in\{\pm1\}$, $y\in\{1,\epsilon\}$	q^2+q $c_x=\begin{pmatrix}x&0\\0&x^{-1}\end{pmatrix}$, $x\neq\pm1$	q^2-q $d_\zeta=\begin{pmatrix}x&\epsilon y\\y&x\end{pmatrix}$, $x\neq\pm1$, $y\neq0$, $\zeta^{q+1}=1$
U	1	1	1	1
V	q	0	1	-1
W_k, $\alpha_k^2\neq1$	$(q+1)\alpha(\pm1)$	$\alpha_k(x)$	$\alpha_k(x)+\alpha_k(x^{-1})$	0
X_ϕ, $\phi^2\neq1$	$(q-1)\phi(\pm1)$	$-\phi(x)$	0	$-(\phi(\zeta)+\phi(\zeta^{-1}))$
W'	$[(q+1)/2]\,\tau(\pm1)$	$[\tau(x)/2]\,(1+\tau(y)\sqrt{q^*})$	$\tau(x)$	0
W''	$[(q+1)/2]\,\tau(\pm1)$	$[\tau(x)/2]\,(1-\tau(y)\sqrt{q^*})$	$\tau(x)$	0
X'	$[(q-1)/2]\,\psi(\pm1)$	$[\tau(x)/2]\,(-1+\tau(y)\sqrt{q^*})$	0	$-\psi(y)$
X''	$[(q-1)/2]\,\psi(\pm1)$	$[\tau(x)/2]\,(-1-\tau(y)\sqrt{q^*})$	0	$-\psi(\zeta)$

Table 4. Character table of $\mathrm{SL}_2(\mathbb{F}_q)$ for odd q

We see that $\pm I_2$ has order 1 or 2, and all the character values of $\pm I_2$ are integers. The matrix $b_{x,y}$ has order p when $x = 1$ and order $2p$ when $x = -1$, and some of the character values of $b_{x,y}$ include a factor of $\sqrt{q^*}$. For each $d \mid (q-1)$, there are matrices c_x and d_ζ of order d which yield character values of the form $\zeta_d^r + \zeta_d^{-r}$. This completes the proof of Theorems 1.3 and 1.4 when q is odd.

2.2.2. *The case when q is even.* When q is even, the conjugacy classes do not split as they do when q is odd. The conjugacy classes are given in the following table.

Representative	# elements	# classes
$\left(\begin{smallmatrix} 1 & 0 \\ 0 & 1 \end{smallmatrix}\right)$	1	1
$\left(\begin{smallmatrix} 1 & 1 \\ 0 & 1 \end{smallmatrix}\right)$	q^2-1	1
$c_x = \left(\begin{smallmatrix} x & 0 \\ 0 & x^{-1} \end{smallmatrix}\right)$, $x \neq \pm 1$	q^2+q	$\frac{q-2}{2}$
d_ζ, $\zeta^{q+1} = 1 \neq \zeta$	q^2-q	$\frac{q}{2}$

Table 5. Conjugacy classes of $\mathrm{SL}_2(\mathbb{F}_q)$ for even q

The restrictions of the representations are similar to those in the case when q is odd, except that W_j and X_ϕ no longer split at the nontrivial quadratic characters. We have the following character table.

$\mathrm{SL}_2(\mathbb{F}_q)$ q even	1 $\begin{pmatrix} 1 & 0 \\ 0 & 1 \end{pmatrix}$	q^2-1 $\begin{pmatrix} 1 & 1 \\ 0 & 1 \end{pmatrix}$	q^2+q $c_x = \begin{pmatrix} x & 0 \\ 0 & x^{-1} \end{pmatrix}$, $x \neq \pm 1$	q^2-q d_ζ, $\zeta^{q+1} = 1 \neq \zeta$
U	1	1	1	1
V	q	0	1	-1
W_j	$q+1$	1	$\alpha_j(x) + \alpha_j(x^{-1})$	0
X_ϕ	$q-1$	-1	0	$-(\phi(\zeta) + \phi(\zeta^{-1}))$

Table 6. Character table of $\mathrm{SL}_2(\mathbb{F}_q)$ for even q

The order of I_2 is 1, and the order of the element in the second column of the character table is 2. Both of these elements yield integer character values. For each $d \mid (q-1)$, there are matrices c_x and d_ζ of order d which yield character values of the form $\zeta_d^r + \zeta_d^{-r}$. This completes the proof of Theorems 1.3 and 1.4 when q is even.

3. $\mathrm{GL}_m(\mathbb{F}_q)$ for Dimensions $m \geq 3$

Here we define the notation required to describe the representation theory of $\mathrm{GL}_m(\mathbb{F}_q)$ for general rank $m \geq 3$, and we prove Theorems 1.1 and 1.2 for ranks $m \geq 3$.

3.1. **Proof of Theorem 1.1.** We first describe the conjugacy classes of $\mathrm{GL}_m(\mathbb{F}_q)$. Let $f(t)$ be the monic polynomial

$$f(t) = \sum_{i=0}^{d} a_i t^i \in \mathbb{F}_q[t]$$

with $a_d = 1$, and let $U_1(f)$ be the companion matrix of f. For any positive integer n, define the Jordan block matrix

$$U_n(f) := \begin{pmatrix} U_1(f) & I_d & 0 & \cdots & 0 \\ 0 & U_1(f) & I_d & \cdots & 0 \\ \vdots & \vdots & \ddots & \ddots & \vdots \\ \vdots & \vdots & \vdots & \ddots & I_d \\ 0 & 0 & 0 & \cdots & U_1(f) \end{pmatrix}.$$

For a partition $\lambda = (\lambda_1, \lambda_2, \dots, \lambda_k)$ of m, let $U_\lambda(f)$ be the matrix defined by

$$U_\lambda(f) := \operatorname{diag}\{U_{\lambda_1}(f), U_{\lambda_2}(f), \dots, U_{\lambda_k}(f)\} = \bigoplus_{i=1}^{k} U_{\lambda_i}(f).$$

Let $A \in \mathrm{GL}_m(\mathbb{F}_q)$ with characteristic polynomial

$$f_A = f_1^{k_1} f_2^{k_2} \cdots f_N^{k_N},$$

where $f_i \neq t$ are irreducible polynomials over $\mathbb{F}_q$. Then A is conjugate to its Jordan canonical form

$$\operatorname{diag}\{U_{\lambda_1}(f_1), U_{\lambda_2}(f_2), \dots, U_{\lambda_N}(f_N)\} = \bigoplus_{i=1}^{N} U_{\lambda_i}(f_i)$$

where λ_i is some partition of k_i.

Conjugacy classes in $\mathrm{GL}_m(\mathbb{F}_q)$ are defined by

$$(\{f_i\}, \{d_i\}, \{k_i\}, \{\lambda_i\})_{i=1}^{N},$$

where $f_i \neq t$ is an irreducible polynomial over $\mathbb{F}_q$ of degree d_i, λ_i is a partition of k_i, N is called the length of the conjugacy class, and

$$\sum_{i=0}^{N} k_i d_i = m.$$

We call a conjugacy class primary if $f_i = 1$ for all i except one. We say that two conjugacy classes

$$(\{f_i\}, \{d_i\}, \{k_i\}, \{\lambda_i\})_{i=1}^{N} \quad \text{and} \quad (\{g_i\}, \{e_i\}, \{w_i\}, \{\nu_i\})_{i=1}^{N'}$$

are of the same type if $N = N'$ and there is a permutation $\sigma \in S_m$ such that $e_{\sigma(i)} = d_i$, $w_{\sigma(i)} = k_i$, and $\nu_{\sigma(i)} = \lambda_i$, but the f_i and g_i are allowed to differ. When f_i and g_i have different roots, they yield two different conjugacy classes of the same type.

In [4], Green shows that the values of an irreducible character of $\mathrm{GL}_m(\mathbb{F}_q)$ on classes of the same type can be described by a single formula. Since f_i is irreducible of degree d_i, the roots of f_i are of the form $\alpha_i, \alpha_i^q, \dots, \alpha_i^{q^{d_i-1}}$ for some $\alpha_i \in \mathbb{F}_{q^{d_i}}^\times$, where α_i is not in $F_{q^\delta}^\times$ for any divisor δ of d_i. Elements in the conjugacy class $(\{f_i\}, \{d_i\}, \{k_i\}, \{\lambda_i\})_{i=1}^{N}$ have order given by $\operatorname{lcm}(\operatorname{ord}(\alpha_i))$, where $\operatorname{ord}(\alpha_i)$ is the order of α_i in $\mathbb{F}_{q^{d_i}}^\times$.

The values of the cuspidal characters are straightforward to describe. Let θ be a character of $\mathbb{F}_{q^m}^\times$, and denote its conjugate characters by $\theta_i = \theta^{q^i}$ for each $0 \leq i \leq m-1$. We say

that θ is non-decomposable if all of its conjugates are distinct. For an irreducible polynomial $f(t) \in \mathbb{F}_q[t]$ of degree $d = \deg(f)$ with roots $\alpha, \alpha^q, \ldots, \alpha^{q^{d-1}}$, define

$$\theta(f) = \sum_{k=0}^{d-1} \theta\left(\alpha^{q^k}\right).$$

If $d \mid m$, then we define the cuspidal character χ_θ to be the class function

$$\chi_\theta(g) = \begin{cases} \phi_f(q)\theta(f) & \text{if } [g] \text{ is the primary class associated to } f, \\ 0 & \text{otherwise,} \end{cases}$$

where $\phi_f(q) \in \mathbb{Z}$. If θ is a non-decomposable character of $\mathbb{F}_{q^m}^\times$, then $(-1)^{m-1}\chi_\theta$ is an irreducible character of $\mathrm{GL}_m(\mathbb{F}_q)$. In fact, Theorem 13 of [4] shows that χ is an irreducible character of $\mathrm{GL}_m(\mathbb{F}_q)$ if and only if it is a product of (possibly repeated) cuspidal characters such that the sum of the degrees of the associated polynomials is m. This proves Theorem 1.1.

3.2. **Proof of Theorem 1.2.** Recall that

$$|\mathrm{GL}_m(\mathbb{F}_q)| = q^{\frac{m(m-1)}{2}} \prod_{k=1}^{m} \Phi_k(q)^{\lfloor m/k \rfloor},$$

where Φ_k is the kth cyclotomic polynomial. Therefore, if there is an element of order ℓ^r in $\mathrm{GL}_m(\mathbb{F}_q)$, then either $\ell^r = p$ or $\ell^r \mid \Phi_k(q)$ for some $k \leq m$. It is clear from the description of the characters above that in the first case, if $\ell^r = p$, then all of the character values are integers. In the second case, if $k_r = \mathrm{ord}_{\ell^r}(q)$ is multiplicative order of q modulo ℓ^r, then $\ell^r \mid \Phi_{k_r}(q)$ and $\ell^r \nmid \Phi_{k_s}(q)$ for all $s < r$. Therefore, an element of order exactly ℓ^r must come from a conjugacy class associated to an irreducible polynomial of degree k_r.

The order of an element in $\mathrm{GL}_m(\mathbb{F}_q)$ is the least common multiple of the orders of the roots of the polynomials associated to its conjugacy class. For an element of order ℓ^r, these orders must be powers ℓ^a with $a \leq r$. Therefore, elements of order ℓ^r must come from conjugacy classes associated to an irreducible degree k_r polynomial and possibly also irreducible degree k_a polynomials with $a < r$. The character values at these elements are integer multiples of

$$\prod_{a=1}^{r} \left(\sum_{t=0}^{k_a-1} \theta_a\left(\alpha_a^{q^t}\right) \right) = \prod_{a=1}^{r} \left(\sum_{t=0}^{k_a-1} \zeta_{\ell^a}^{i_a q^t} \right),$$

where $i_r \in \mathbb{Z}_{\ell^r}^\times$ and $i_a \in \mathbb{Z}_{\ell^a}$ for $a < r$.

We define the following notation for the lemma below. Let $G_{\ell^r} := \mathrm{Gal}\left(\mathbb{Q}\left(\zeta_{\ell^r}\right)/\mathbb{Q}\right)$, so that $G_{\ell^r} \cong \mathbb{Z}_{\ell^r}^\times$. Define $\tau_q \in G_{\ell^r}$ to be the automorphism such that $\tau_q(\zeta_{\ell^r}) = \zeta_{\ell^r}^q$. Theorem 1.2 follows as a consequence of the following lemma.

Lemma 3.1. *We have that*

$$\mathbb{Q}\left(\prod_{a=1}^{r} \left(\sum_{t=0}^{k_a-1} \zeta_{\ell^a}^{i_a q^t} \right) \right) = \mathbb{Q}(\zeta_{\ell^r})^{\langle \tau_q \rangle},$$

with $i_r \in \mathbb{Z}_{\ell^r}^\times$, is the unique subfield of $\mathbb{Q}(\zeta_{\ell^r})$ of degree $\frac{\ell^{r-1}(\ell-1)}{k_r}$ over $\mathbb{Q}$.

Proof. For simplicity, we take $i_r = 1$. If $\tau \in G_{\ell^r}$, then $\tau(\zeta_{\ell^r}) = \zeta_{\ell^r}^s$ for some $s \in \mathbb{Z}_{\ell^r}^\times$, and so we have that

$$\tau\left(\prod_{a=1}^{r} \left(\sum_{t=0}^{k_a-1} \zeta_{\ell^a}^{i_a q^t} \right) \right) = \prod_{a=1}^{r} \left(\sum_{t=0}^{k_a-1} \zeta_{\ell^a}^{i_a s q^t} \right) \tag{3.1}$$

for some $s \in \mathbb{Z}_{\ell^r}^{\times}$. Since $\mathrm{ord}_{\ell^r}(q) = k_r$, multiplication by q in $\mathbb{Z}_{\ell^r}^{\times}$ can be described by $\frac{\phi(\ell^r)}{k_r}$ disjoint k_r-cycles. This implies that there are $\frac{\ell^{r-1}(\ell-1)}{k_r}$ sets of distinct exponents $\{s, sq, \dots, sq^{k_r-1}\}$ (mod ℓ^r) in the last term as s varies. Thus, as we range over all $\tau \in G_{\ell^r}$, we see that

$$\tau\left(\zeta_{\ell^r} + \zeta_{\ell^r}^{q} + \cdots + \zeta_{\ell^r}^{q^{k_r-1}}\right)$$

takes $\frac{\ell^{r-1}(\ell-1)}{k_r}$ distinct values. The products in equation (3.1) are all character values, so they are linearly independent. This means that the character value

$$\prod_{a=1}^{r}\left(\sum_{t=0}^{k_a-1}\zeta_{\ell^a}^{i_a q^t}\right)$$

has $\frac{\ell^{r-1}(\ell-1)}{k_r}$ distinct Galois conjugates, and so we have that

$$\left[\mathbb{Q}\left(\prod_{a=1}^{r}\left(\sum_{t=0}^{k_a-1}\zeta_{\ell^a}^{i_a q^t}\right)\right) : \mathbb{Q}\right] = \frac{\ell^{r-1}(\ell-1)}{k_r}.$$

On the other hand, we observe that

$$\left[\mathbb{Q}(\zeta_{\ell^r})^{\langle\tau_q\rangle} : \mathbb{Q}\right] = \frac{[\mathbb{Q}(\zeta_{\ell^r}) : \mathbb{Q}]}{[\mathbb{Q}(\zeta_{\ell^r}) : \mathbb{Q}(\zeta_{\ell^r})^{\langle\tau_q\rangle}]} = \frac{\ell^{r-1}(\ell-1)}{k_r}.$$

Since $G_{\ell^r} \cong \mathbb{Z}_{\ell^r}^{\times}$ is cyclic, there is a unique subfield of $\mathbb{Q}(\zeta_{\ell^r})$ of degree d over $\mathbb{Q}$ for each $d \mid \phi(\ell^r)$. Therefore, we must have that

$$\mathbb{Q}\left(\prod_{a=1}^{r}\left(\sum_{t=0}^{k_a-1}\zeta_{\ell^a}^{i_a q^t}\right)\right) = \mathbb{Q}(\zeta_{\ell^r})^{\langle\tau_q\rangle}.$$

This proves Lemma 3.1. □

References

[1] C. Bonnafé, *Sur les caractères des groupes réductif finis à centre non connexe: applications aux groupes spéciaux linéaires et unitaires*, Astérisque **306**, 2006.

[2] M. L. Dawsey, K. Ono, and I. Wagner. Multiquadratic fields generated by characters of A_n. *J. Algebra* **533** (2019), 339-343.

[3] W. Fulton and J. Harris. *Representation theory: A first course*, Springer, New York, 1999.

[4] J. A. Green. The characters of the finite general linear groups. *Trans. Amer. Math. Soc.* **80**: 2 (1955), 402-447.

[5] D. Hilbert. Mathematical problems. *Bull. Amer. Math. Soc.* **8** (1902), 437-479.

[6] G. R. Robinson and J. G. Thompson. Sums of squares and the fields $\mathbb{Q}_{A_n}$. *J. Algebra* **174** (1995), 225-228.

[7] T. Shoji, *Shintani descent for special linear groups*, J. Algebra **199** (1998), 175-228.

[8] T. Shoji, *Lusztig's conjecture for finite special linear groups*, Representation Th. **10** (2006), 164-222.

[9] J. G. Thompson. Personal letter to the second author, February 11, 1994.

Department of Mathematics, University of Texas at Tyler, Tyler, TX 75799
E-mail address: mdawsey@uttyler.edu

Department of Mathematics, University of Virginia, Charlottesville, VA 22904
E-mail address: ko5wk@virginia.edu

Department of Mathematics, Vanderbilt University, Nashville, TN 37212
E-mail address: ian.c.wagner@vanderbilt.edu