J. Sci. I. R. Iran

Vol.9 No.2
Spring 1998

THE RATIONAL CHARACTER TABLE OF SPECIAL LINEAR GROUPS

H. Behravesh

Department of Mathematics, University of Urmia, Urmia, Islamic Republic of Iran

Abstract

In this paper we will give the character table of the irreducible rational representations of $G=SL(2, q)$ where $q=p^n$, p prime, $n>0$, by using the character table and the Schur indices of $SL(2, q)$.

Introduction

Let G be a finite group and χ be an irreducible complex character of G. Let $m_Q(\chi)$ denote the Schur index of χ over Q. †Let $\Gamma(\chi)$ be the Galois group $Q(\chi)$ over Q. It is known that

$$\Sigma_{\alpha\in\Gamma(\chi)} m_Q(\chi)\chi^{\alpha} \qquad (*)$$

is a character of an irreducible Q (G)-module [4, Corollary 10.2(b)]. So, by knowing the character table of a group and Schur indices we can find the rational character table of that group.

In this paper we will give the character table of the irreducible rational representations of $G=SL(2, q)$ where $q=p^n$, p prime, $n>0$, by using the character table and the the Schur indices of $SL(2, q)$.

Background

We begin with a brief summary of facts relevant to the irreducible complex characters and Schur indices of special linear groups.

Theorem 2.1. Let F be the finite field of $q=p^n$ elements, p an odd prime, and let v be a generator of the cyclic group of $F^*=F-\{0\}$.
Denote

$$1=\begin{pmatrix}1&0\\0&1\end{pmatrix}, z=\begin{pmatrix}-1&0\\0&-1\end{pmatrix},$$
$$c=\begin{pmatrix}1&0\\1&1\end{pmatrix}, d=\begin{pmatrix}1&0\\v&1\end{pmatrix}, a=\begin{pmatrix}v&0\\0&v^{-1}\end{pmatrix}$$

in $G = SL(2, F)$. G contains an element b of order $q+1$.

For any $x\in G$, let (x) denote the conjugacy class of G containing x. Then G has exactly $q+4$ conjugacy classes (1), (z), (c), (d), (zc), (zd), (a), (a^2),..., $(a^{\frac{q-3}{2}})$, (b), (b^2),...,$(b^{\frac{q-1}{2}})$, for $1\leq l\leq (q-3)/2$, $1\leq m\leq (q-1)/2$ (See Table 1).
Denote $\varepsilon=(-1)^{(q-1)/2}$. Let $\rho\in$ C be a primitive $(q-1)$-th root of 1, $\sigma\in$ C a primitive $(q+1)$-th root of 1. Then the complex character table of G for $1\leq i\leq (q-3)/2$, $1\leq j\leq (q-1)/2$, $1\leq l\leq (q-3)/2$, $1\leq m\leq (q-1)/2$ is given in Table 2. (The columns for the classes (zc) and (zd) are missing in this table. These values are obtained from the relations

$$\chi(zc)=\frac{\chi(z)}{\chi(1)}\chi(c),\ \chi(zd)=\frac{\chi(z)}{\chi(1)}\chi(d),$$

for all irreducible characters χ of G.)

Proof. See [2, 38.1].

Theorem 2.2. Let F be the finite field of $q=2^n$ elements,

Keywords: Rational character table; Special linear groups

Table 1. Table of conjugacy classes of $SL(2, p^n)$

x	1	z	c	d	zc	zd	a^l	b^m
$\|(x)\|$	1	1	$\frac{1}{2}(q^2-1)$	$\frac{1}{2}(q^2-1)$	$\frac{1}{2}(q^2-1)$	$\frac{1}{2}(q^2-1)$	$q(q+1)$	$q(q-1)$

Table 2. Character table of $SL(2, p^n)$

	1	z	c	d	a^l	b^m
1_G	1	1	1	1	1	1
ψ	q	q	0	0	1	-1
χ_i	$q+1$	$(-1)^i(q+1)$	1	1	$\rho^{il}+\rho^{-il}$	0
θ_j	$q-1$	$(-1)^j(q-1)$	-1	-1	0	$-(\sigma^{jm}+\sigma^{-jm})$
ξ_1	$\frac{1}{2}(q+1)$	$\frac{1}{2}\varepsilon(q+1)$	$\frac{1}{2}(1+\sqrt{\varepsilon q})$	$\frac{1}{2}(1-\sqrt{\varepsilon q})$	$(-1)^l$	0
ξ_2	$\frac{1}{2}(q+1)$	$\frac{1}{2}\varepsilon(q+1)$	$\frac{1}{2}(1-\sqrt{\varepsilon q})$	$\frac{1}{2}(1+\sqrt{\varepsilon q})$	$(-1)^l$	0
η_1	$\frac{1}{2}(q-1)$	$-\frac{1}{2}\varepsilon(q-1)$	$\frac{1}{2}(-1+\sqrt{\varepsilon q})$	$\frac{1}{2}(-1-\sqrt{\varepsilon q})$	0	$(-1)^{m+1}$
η_2	$\frac{1}{2}(q-1)$	$-\frac{1}{2}\varepsilon(q-1)$	$\frac{1}{2}(-1-\sqrt{\varepsilon q})$	$\frac{1}{2}(-1+\sqrt{\varepsilon q})$	0	$(-1)^{m+1}$

and let ν be a generator of the cyclic group $F^*= F-\{0\}$. Denote

$$1=\begin{pmatrix}1&0\\0&1\end{pmatrix}, c=\begin{pmatrix}1&0\\1&1\end{pmatrix}, a=\begin{pmatrix}\nu&0\\0&\nu^{-1}\end{pmatrix}$$

in $G= SL(2, F)$. G contains an element b of order $q+1$.

For any $x \in G$, let (x) denote the conjugacy class of G containing x. Then G has exactly $q+1$ conjugacy classes (1), (c), (a), (a^2),…,$(a^{(q-2)/2})$, (b), (b^2),…,$(b^{q/2})$, where (See Table 3).
for $1 \leq l \leq (q-2)/2$, $1 \leq m \leq q/2$.

Let $\rho \in \mathbf{C}$ be a primitive $(q-1)$-th root of 1, $\sigma \in \mathbf{C}$ a primitive $(q+1)$-th root of 1. Then the character table of G over $\mathbf{C}$ for $1 \leq i \leq (q-2)/2$, $1 \leq j \leq q/2$, $1 \leq l \leq (q-2)/2$, $1 \leq m \leq q/2$ is given in Table 4.

Table 3. Table of conjugacy classes of $SL(2, 2^n)$

x	1	c	a^l	b^m
$\|(x)\|$	1	(q^2-1)	$q(q+1)$	$q(q-1)$

Proof. See [2, 38.2].

Table 4. Character table of $SL(2, 2^n)$

	1	c	a^l	b^m
1_G	1	1	1	1
ψ	q	0	1	-1
χ_i	$q+1$	1	$\rho^{il}+\rho^{-il}$	0
θ_j	$q-1$	-1	0	$-(\sigma^{jm}+\sigma^{-jm})$

Theorem 2.3. Let $G = SL(2, q)$. If q is a power of 2, then the Schur index of any irreducible character of G over the rational numbers $\mathbf{Q}$ is 1. If q is a power of an odd prime p, then the Schur indices of the irreducible characters of G

over the rational numbers **Q** are as follows: (See Table 5).

Table 5. Table of Schur indices

	q ≡ 1 mod 4	q ≡ 3 mod 4
1_G	1	1
ψ	1	1
χ_i	2 (*i odd*)	2 (*i odd*)
	1 (*i even*)	1 (*i even*)
θ_j	2 (*j odd*)	2 (*j odd*)
	1 (*j even*)	1 (*j even*)
ξ_1	1	1
ξ_2	1	1
η_1	2	1
η_2	2	1

Proof. See [5].

Character Table of Irreducible Rational Representations of $G = SL(2,q)$

Lemma 3.1. Let ξ be a primitive n-th root of unity. Then $\xi+\xi^{-1}$ is rational if and only if $n = 1,2,3,4,6$. The values which occur are as follows:

Table 6.

n	1	2	3	4	6
$\xi+\xi^{-1}$	2	-2	-1	0	1

Proof. The result is clear for $n = 1$ or $n = 2$ so that we may assume that $n \geq 3$.

As $x^2-(\xi+\xi^{-1})x+1 = (x-\xi)(x-\xi^{-1})$, the index $(\mathbf{Q}(\xi): \mathbf{Q}(\xi+\xi^{-1})) = 2$ unless $\xi \in \mathbf{Q}$, that is, unless $n = 1$ or 2. It follows that $\xi + \xi^{-1} \in \mathbf{Q}$ if and only if $\phi(n) = (\mathbf{Q}(\xi): \mathbf{Q}) = 2$. Examination of the possibilities shows that $\phi(n) = 2$ if and only if $n = 3,4$ or 6.

Corollary 3.2. Let ξ be a primitive n-th root of unity. Let $1 \leq j \leq n$. Then $\xi^j + \xi^{-j}$ is rational if and only if $n = j, 2j, 3j, 4j, 6j, \frac{3}{2}j, \frac{4}{3}j, \frac{6}{5}j$.

Proof. Let (j, n) denote the greatest common divisor of j and n. Write $j = a(j, n)$ and $n = b(j, n)$ so that a and b are coprime and $0 < \frac{a}{b} \leq 1$.

As ξ^j is a primitive b-th root of unity, Lemma 3.1 shows that $\xi^j + \xi^{-j}$ is rational if and only if $b = 1,2,3,4$ or 6. For these values of b, the corresponding possibilities for $\frac{a}{b}$ are $1, \frac{1}{2}, \frac{1}{3}, \frac{2}{3}, \frac{1}{4}, \frac{3}{4}, \frac{1}{6}$, and $\frac{5}{6}$. As $j = \frac{a}{b}n$, the result follows.

Corollary 3.3. Let ξ be a primitive n-th root of unity and $n \neq 2$. Then $(\mathbf{Q}(\xi) : \mathbf{Q}(\xi + \xi^{-1})) = 2$ and $(\mathbf{Q}(\xi + \xi^{-1}) : \mathbf{Q}) = \frac{1}{2}\varphi(n)$.

Proof. This follows from the fact that $(x-\xi)(x-\xi^{-1}) = x^2-(\xi + \xi^{-1})x+1$ and $(\mathbf{Q}(\xi) : \mathbf{Q}) = \varphi(n)$.

Lemma 3.4. Let ξ be a primitive n-th root of unity, $i \in \mathbf{Z}$ and $d_i = (i, n)$. If $n > 2d_i$, then $(\mathbf{Q}(\xi^i + \xi^{-i}) : \mathbf{Q}) = \frac{1}{2}\varphi(\frac{n}{d_i})$.

Proof. Since $n > 2d_i$, so $n \neq 2$. If $i = 1$, then the result follows from Corollary 3.3. So let $i \neq 1$. By Corollary 3.2, $\xi^i + \xi^{-i} \in \mathbf{Q}$ if and only if $\frac{n}{d_i} = 1,2,3,4,6, \frac{3}{2}, \frac{4}{3}$ and $\frac{6}{5}$. Since $\frac{n}{d_i} \in \mathbf{Z}$ and $n \neq d_i, 2d_i$ so $\xi^i + \xi^{-i} \in \mathbf{Q}$ if and only if, $\frac{n}{d_i} = 3,4,6$. But $\varphi(3) = \varphi(4) = \varphi(6) = 2$ and $(\mathbf{Q}(\xi^i + \xi^{-i}) : \mathbf{Q}) = 1$in these cases, so the result follows for the case $\xi^i + \xi^{-i} \in \mathbf{Q}$.

Now let $\xi^i + \xi^{-i} \notin \mathbf{Q}$. Since ξ^i is a primitive $\frac{n}{d_i}$ - th root of unity, so by Corollary 3.3 $(\mathbf{Q}(\xi^i) : \mathbf{Q}(\xi^i + \xi^{-i})) = 2$. Therefore $(\mathbf{Q}(\xi^i + \xi^{-i}): \mathbf{Q}) = \frac{1}{2}\varphi(\frac{n}{d_i})$.

Corollary 3.5. Let ξ be a primitive n-th root of unity and $1 \leq i < \frac{n}{2}$. Then $(\mathbf{Q}(\xi^i + \xi^{-i}): \mathbf{Q}) = \frac{1}{2}\varphi(\frac{n}{d_i})$

where $d_i = (i, n)$

Proof. This follows from Lemma 3.4.

Let M be a field of characteristic zero and let K be a subfield of M. Suppose that M is a finite and normal extension of K with Galois group $\Gamma = \Gamma(M:K)$. For any $a \in M$ define the trace

$$\mathrm{Tr}_{M\to K}(a) = \Sigma_{\alpha\in\Gamma} a^{\alpha}.$$

Lemma 3.6. Let $K \leq L \leq M$ be fields and let M be a finite and normal extension of K. Then

$$\mathrm{Tr}_{L\to K}(\mathrm{Tr}_{M\to L}(x)) = \mathrm{Tr}_{M\to K}(x)$$

where $x \in M$.

Proof. It is obvious.

Lemma 3.7. Let ξ be a primitive n-th root of unity. Let $i \in \mathbf{Z}$ and $d_i = (i, n)$ and let $n \neq d_i, 2d_i$. Then

$$\Sigma_{\alpha\in\Gamma_i}(\xi^i + \xi^{-i})^{\alpha} = \mu\left(\frac{n}{d_i}\right)$$

where $\Gamma_i = \Gamma(\mathbf{Q}(\xi^i + \xi^{-i}) : \mathbf{Q})$ and μ is the Möbius function.

Proof. Let $A = \Sigma_{\alpha\in\Gamma_i}(\xi^i + \xi^{-i})^{\alpha} = \mathrm{Tr}_{\mathbf{Q}(\xi^i+\xi^{-i})\to\mathbf{Q}}(\xi^i + \xi^{-i})$ and let $B = \mathrm{Tr}_{\mathbf{Q}(\xi^i)\to\mathbf{Q}}(\xi^i + \xi^{-i})$.

Let $\xi^i + \xi^{-i} \notin \mathbf{Q}$. Then by [1, Lemma 3.4], $B = 2\mu\left(\frac{n}{d_i}\right)$ and by Lemma 3.6,

$$B = \mathrm{Tr}_{\mathbf{Q}(\xi^i+\xi^{-i})\to\mathbf{Q}}(\mathrm{Tr}_{\mathbf{Q}(\xi^i)\to\mathbf{Q}(\xi^i+\xi^{-i})}(\xi^i + \xi^{-i})) =$$

$$2\mathrm{Tr}_{\mathbf{Q}(\xi^i+\xi^{-i})\to\mathbf{Q}}(\xi^i + \xi^{-i}) = 2A$$

Therefore $A = \mu\left(\frac{n}{d_i}\right)$.

Now let $\xi^i + \xi^{-i} \in \mathbf{Q}$. By Lemma 3.4, $\xi^i + \zeta^{-i} \in \mathbf{Q}$ if and only if, $\frac{n}{d_i} = 3,4,6$. But in this case, $\xi^i + \xi^{-i} = \mu\left(\frac{n}{d_i}\right)$ and $A = \xi^i + \xi^{-i}$.

Lemma 3.8. Let ξ be a primitive n-th root of unity, $i \in \mathbf{Z}$, $d_i = (i, n)$ and $n \neq d_i, 2d_i$. Let $\Gamma = \Gamma(\mathbf{Q}(\xi + \xi^{-1}) : \mathbf{Q})$. Then

$$\Sigma_{\alpha\in\Gamma}(\xi^i + \xi^{-i})^{\alpha} = \frac{\varphi(n)}{\varphi\left(\frac{n}{d_i}\right)}\mu\left(\frac{n}{d_i}\right).$$

Proof. Let $L_i = \mathbf{Q}(\xi^i + \xi^{-i})$. Then by induction we can prove that $L_i \subseteq L_1$. By Lemma 3.4,

$$(L_i : \mathbf{Q}) = \frac{1}{2}\varphi\left(\frac{n}{d_i}\right).$$

So

$$(L_1 : L_i) = \frac{\varphi(n)}{\varphi\left(\frac{n}{d_i}\right)}.$$

Hence

$$\mathrm{Tr}_{L_1\to L_i}(\xi^i + \xi^{-i}) = \frac{\varphi(n)}{\varphi\left(\frac{n}{d_i}\right)}(\xi^i + \xi^{-i}).$$

Now apply Lemmas 3.6 and 3.7. So

$$\mathrm{Tr}_{L_1\to\mathbf{Q}}(\xi^i + \xi^{-i}) = (\mathrm{Tr}_{L_i\to\mathbf{Q}}(\mathrm{Tr}_{L_1\to L_i}(\xi^i + \xi^{-i})) =$$

$$\mathrm{Tr}_{L_i\to\mathbf{Q}}\left(\frac{\varphi(n)}{\varphi\left(\frac{n}{d_i}\right)}(\xi^i + \xi^{-i})\right) = \frac{\varphi(n)}{\varphi\left(\frac{n}{d_i}\right)}\mathrm{Tr}_{L_i\to\mathbf{Q}}(\xi^i + \xi^{-i}) =$$

$$\frac{\varphi(n)}{\varphi\left(\frac{n}{d_i}\right)}\mu\left(\frac{n}{d_i}\right)$$

Therefore $\Sigma_{\alpha\in\Gamma}(\xi^i + \xi^{-i})^{\alpha} = \frac{\varphi(n)}{\varphi\left(\frac{n}{d_i}\right)}\mu\left(\frac{n}{d_i}\right)$

Corollary 3.9. Let ξ be a primitive n-th root of unity and $1 \leq i < \frac{n}{2}$.
Let $\Gamma = \Gamma(\mathbf{Q}(\xi + \xi^{-1}) : \mathbf{Q})$. Then

$$\Sigma_{\alpha\in\Gamma}(\xi^i + \xi^{-i})^{\alpha} = \frac{\phi(n)}{\phi\left(\frac{n}{d_i}\right)}\mu\left(\frac{n}{d_i}\right)$$

where $d_i = (i, n)$.

Proof. This follows from Lemma 3.8.

Lemma 3.10. Let $G = SL(2, q)$ where $q = p^n$ for some odd prime p. Then the Galois orbit sums in $\mathrm{Irr}(G)$ are as follows:

(a) $\Sigma_{\alpha\in\Gamma}\chi_e^{\alpha}$ where $e = (i, q-1)$ and $1 \leq i \leq (q-3)/2$ and $\Gamma = \Gamma(\mathbf{Q}(\chi_i) : \mathbf{Q})$;
(b) $\Sigma_{\alpha\in\Gamma}\theta_f^{\alpha}$ where $f = (j, q+1)$ and $1 \leq j \leq (q-1)/2$ and $\Gamma = \Gamma(\mathbf{Q}(\theta_j) : \mathbf{Q})$;
(c) 1_G, ψ;
(d) $\xi_1 + \xi_2$ and $\eta_1 + \eta_2$ for odd n;
(e) ξ_1, ξ_2, η_1, and η_2 for even n.

Proof. Since (a) and (b) have similar proofs, we will prove only (a).

Fix an integer i, $1 \le i \le \frac{q-3}{2}$. Recall that ρ is a primitive (q-1)-th root of unity. Since $\Gamma(Q(\chi_i): Q) = \Gamma(Q(\rho^i + \rho^{-i}) : Q)$ and ρ^i is a primitive $\frac{q-1}{e}$-th root of unity where $e = (i, n)$, so $\Sigma_{\alpha \in \Gamma\chi_e} \alpha = \Sigma_{i \in A} \chi_i$ where A = $\{i : e = (i, n) \text{ and } 1 \le i \le \frac{q-3}{2}\}$.

(c), (d) and (e) follow from the character table of $SL(2, q)$ in Theorem 2.1.

Lemma 3.11. Let χ be a rational valued character of G and let $x, y \in G$ with $\langle x \rangle = \langle y \rangle$. Then $\chi(x) = \chi(y)$.

Proof. See [4, 5.22].

Lemma 3.12. Let $G = SL(2,q)$ where $q = p^n$ and p is an odd prime. Then $\langle c \rangle = \langle d \rangle$ if and only if n is odd.

Proof. Let $P = \{\begin{pmatrix} 1 & x \\ 0 & 1 \end{pmatrix} : x \in F\}$. Then P is a Sylow p-subgroup of G. Let N denote $N_G(P)$. It can be proved that $\begin{pmatrix} 1 & x \\ 0 & 1 \end{pmatrix}$ and $\begin{pmatrix} 1 & y \\ 0 & 1 \end{pmatrix}$ are conjugate in G if and only if they are conjugate in N and that $N = \{\mathrm{diag}(x, x^{-1}) : x \in F^*\}$.

Let $c = \begin{pmatrix} 1 & 1 \\ 0 & 1 \end{pmatrix}$ and $d = \begin{pmatrix} 1 & v \\ 0 & 1 \end{pmatrix}$ where v generates F*. It is easy to prove that

$$\mathrm{diag}(\lambda, \lambda^{-1}) \begin{pmatrix} 1 & x \\ 0 & 1 \end{pmatrix} \mathrm{diag}(\lambda^{-1}, \lambda) = \begin{pmatrix} 1 & \lambda^2 x \\ 0 & 1 \end{pmatrix}$$

where $\lambda \in F^*$ and $d^t = \begin{pmatrix} 1 & tv \\ 0 & 1 \end{pmatrix}$.

Let $l_\lambda = \mathrm{diag}(\lambda, \lambda^{-1}) \in N$. Since $\langle c \rangle$ and $\langle d \rangle$ are conjugate in G if and only if they are conjugate in N, so $\langle c \rangle$ and $\langle d \rangle$ are conjugate in N if and only if $l_\lambda c l_\lambda^{-1} = d^t$

Table 7. Character table of rational representations of $SL(2, p^n)$, p an odd prime, n even

	1	z	c and d	a^t	b^r
1_G	1	1	1	1	1
ψ	q	q	0	1	-1
χ_e	$(q+1)A(e)B(e)$	$(-1)^e(q+1)A(e)B(e)$	$A(e)B(e)$	$A(e)B(e)\tau_1(e, e')$	0
θ_f	$(q-1)C(f)B(f)$	$(-1)^f(q-1)C(f)B(f)$	$-C(f)B(f)$	0	$-C(f)B(f)\tau_2(f, f')$
ξ'_1	$\frac{1}{2}(q+1)$	$\frac{1}{2}(q+1)$	$\frac{1}{2}(1 \pm \sqrt{q})$	$(-1)^{e'}$	0
ξ'_2	$\frac{1}{2}(q+1)$	$\frac{1}{2}(q+1)$	$\frac{1}{2}(1 \mp \sqrt{q})$	$(-1)^{e'}$	0
η'_1	$\frac{1}{2}(q-1)E(q)$	$-\frac{1}{2}(q-1)E(q)$	$\frac{1}{2}(-1 \mp \sqrt{q})E(q)$	0	$(-1)^{f'+1}E(q)$
η'_2	$\frac{1}{2}(q-1)E(q)$	$-\frac{1}{2}(q-1)E(q)$	$\frac{1}{2}(-1 \mp \sqrt{q})E(q)$	0	$(-1)^{f'+1}E(q)$

(The columns for the classes (zc) and (zd) are missing in this table. These are obtained from the relations $\chi(zc) = \frac{\chi(z)}{\chi(1)}\chi(c)$, $\chi(zd) = \frac{\chi(z)}{\chi(1)}\chi(d)$ where χ is an irreducible character of G)

for some t and some λ, that is, if and only if $\lambda^2 = tv$ for some $\lambda \in F^*$, $t \in \mathbf{N}$.

Let $H = \langle v^2 \rangle$. Then the order of H is $(q-1)/2$.

If n is even, then $\frac{q-1}{2} = \frac{p^n-1}{2} = (p^{\frac{n}{2}}-1)\frac{p^{\frac{n}{2}}+1}{2}$ and $p-1 \mid (q-1)/2$. So $v \notin H$, as otherwise the order of v will be less than or equal to $(q-1)/2$. This shows that $tv \notin H$ for all $t \in \mathbf{N}$.

If n is odd, then $q-1 = p^n-1 = (p-1)(p^{n-1} + \dots + 1)$. But $p^{n-1} + \dots + 1$ is odd, so $p-1 \nmid (q-1)/2$. This shows that $v \in H$ and that there exists t and λ such that $\lambda^2 = tv$.

Theorem 3.13. The number of isomorphism types of irreducible $\mathbf{Q}G$-modules is equal to the number of conjugacy classes of cyclic subgroups of G.

Proof. See [3, 3.12]

Let d*(n) denote the number of divisors d of n such that $d < n/2$.

Lemma 3.14. The number of conjugacy classes of cyclic subgroups of $G = SL(2,q)$ where $q = p^n$, is equal to:
(a) $4+d^*(q-1)+d^*(q+1)$ if n is odd;
(b) $6+d^*(q-1)+d^*(q+1)$ if n is even.

Moreover, in case (a) the different conjugacy classes of cyclic subgroups of G are represented by (1), (z), (c), (zc), (a^l) where $l \mid q-1$ and $1 \le l < (q-1)/2$ and (b^m) where $m \mid q+1$ and $1 \le m < (q+1)/2$ and in case (b) the different conjugacy classes of cyclic subgroups of G are represented by (1), (z), (c), (d), (zc), (zd), (a^l) where $l \mid q-1$ and $1 \le l < (q-1)/2$ and (b^m) where $m \mid q+1$ and $1 \le m < (q+1)/2$.

Proof. In order to calculate the number of conjugacy classes of cyclic subgroups of G we apply Theorem 3.13 and Lemmas 3.11 and 3.12. By considering the values of ψ in each conjugacy class it is easy to see that (a^l) for all $l \mid q-1$ and $1 \le l < (q-1)/2$, and (b^m) for all $m \mid q+1$ and $1 \le m < (q+1)/2$, are different conjugacy classes of cyclic subgroups of G. Also, these conjugacy classes are different from (1), (z), (c), (d), (cz) and (dz), as we can see by considering the values of ψ. Hence the total number of different conjugacy classes of subgroups (a^l) is $d^*(q-1)$ and of different conjugacy classes of subgroups (b^m) is $d^*(q+1)$, as required.

Notation (1). Let $G = SL(2, q)$ where $q = p^n$ for some prime $p \neq 2$.

e and e' denote divisors of $q-1$ such that $e < \frac{q-1}{2}$ and $e' < \frac{q-1}{2}$

f and f' denote divisors of $q+1$ such that $f < \frac{q+1}{2}$ and $f' < \frac{q+1}{2}$.

Table 8. Character table of rational representations of $SL(2, p^n)$, p an odd prime, n odd

	1	z	c	$a^{e'}$	$b^{f'}$
1_G	1	1	1	1	1
ψ	q	q	0	1	-1
χ_e	$(q+1)A(e)B(e)$	$(-1)^e(q+1)A(e)B(e)$	$A(e)B(e)$	$B(e)\tau_1(e, e')$	0
θ_f	$(q-1)C(f)B(f)$	$(-1)^f(q-1)C(f)B(f)$	$-C(f)B(f)$	0	$-B(f)\tau_2(f, f')$
ξ'	$q+1$	$\varepsilon(q+1)$	ε	$(-1)^{e'}2$	0
η'	$(q-1)E(q)$	$-\varepsilon(q-1)E(q)$	$-\varepsilon E(q)$	0	$(-1)^{f'+1}2E(q)$

(The column for the class (zc) is missing in this table. This is obtained from the relation $\chi(zc) = \frac{\chi(z)}{\chi(1)}\chi(c)$ where χ is an irreducible character of G)

ρ_e is a primitive $\frac{q-1}{e}$-th root of unity.

σ_f is a primitive $\frac{q+1}{f}$-th root of unity.

$1, z, c, d, a, b, \rho$ and σ are as in Theorem 2.1.

$$B(k) = \begin{cases} 1 & \text{if } k \text{ is even} \\ 2 & \text{otherwise} \end{cases}$$

$$E(q) = \begin{cases} 1 & \text{if } q \equiv 3 \bmod 4 \\ 2 & \text{otherwise} \end{cases}$$

$A(e) = \frac{1}{2}\,\varphi\left(\frac{q-1}{e}\right)$ and $C(f) = \frac{1}{2}\,\varphi\left(\frac{q+1}{f}\right)$.

$\tau_1(e, e') = \Sigma_{\alpha \in \Gamma} (\rho_e^{e'} + \rho_e^{-e'})^\alpha = \dfrac{\varphi\left(\frac{q-1}{e}\right)}{\varphi\left(\frac{q-1}{ee'}\right)}\,\mu\left(\frac{q-1}{ee'}\right)$ by Lemma 3.8 where $\Gamma = \Gamma(Q(\chi_e) : Q)$. [Note that $\Gamma = \Gamma(Q(\rho_e + \rho_e^{-1}) : Q)$].

$\tau_2(f, f') = \Sigma_{\alpha \in \Gamma_1} (\theta_f^{f'} + \theta_f^{-f'})^\alpha = \dfrac{\varphi\left(\frac{q+1}{f}\right)}{\varphi\left(\frac{q+1}{ff'}\right)}\,\mu\left(\frac{q+1}{ff'}\right)$

where $\Gamma_1 = \Gamma(Q(\theta_f) : Q)$. [Note that $\Gamma = \Gamma(Q + \sigma_f^{-1}) : Q)$].

χ_i and θ_j are irreducible characters of G as in Theorem 2.1.

Then $\Sigma_{\alpha \in \Gamma} \chi_i^\alpha$, where $\Gamma = \Gamma(Q(\chi_i): Q)$, and $\Sigma_{\alpha \in \Gamma_1} \theta_j^\alpha$, where $\Gamma_1 = \Gamma(Q(\theta_j) : Q)$, are rational valued characters of G.

$\chi_e = B(e)\, \Sigma_{\alpha \in \Gamma} \chi_i^\alpha$ where $e = (i, q\text{-}1)$.

$\theta_f = B(f)\, \Sigma_{\alpha \in \Gamma_1} \theta_j^\alpha$ where $f = (j, q\text{+}1)$.

ξ' and η' denote the irreducible characters of the rational representations of G arising from ξ_1 (or ξ_2) and η_1 (or η_2) respectively, where n is odd.

$\xi'_1, \xi'_2, \eta'_1, \eta'_2$ denote the irreducible characters of the rational representations of G arising from $\xi_1, \xi_2, \eta_1, \eta_2$ respectively, where n is even.

Lemma 3.15. In the notation (1), χ_e and θ_f are irreducible characters of rational representations of G and

(a)

$\chi_e(1) = A(e)\,B(e)\,(q+1);$

$\chi_e(z) = (-1)^e A(e)\,B(e)\,(q+1);$

$\chi_e(c) = \chi_e(d) = A(e)\,B(e);$

$\chi_e(a^{e'}) = B(e)\,\tau_1(e, e');$

$\chi_e(b^{f'}) = 0;$

(b)

$\theta_f(1) = C(f)\,B(f)\,(q-1);$

$\theta_f(z) = (-1)^f C(f)\,B(f)\,(q-1);$

$\theta_f(c) = \theta_f(d) = -C(f)\,B(f);$

$\theta_f(a^{e'}) = 0;$

$\theta_f(b^{f'}) = B(f)\,\tau_2(f, f').$

Proof. Since the proofs of (a) and (b) are similar, we will prove only part (a).

By Theorem 2.3, $B(e)$ is equal to the Schur index of χ_e over Q, so by (*) χ_e is the irreducible character of a rational representation of G.

Now ρ is a primitive (q-1)-th root of unity, so ρ_e is a primitive $\frac{q-1}{e}$-th root of unity where $e = (i, q\text{-}1)$. By Corollary 3.5,

$$(Q(\rho^i + \rho^{-i}) : Q) = (Q(\rho_e + \rho_e^{-1}) : Q) = A(e).$$

By Lemma 3.8 we have

$$\Sigma_{\alpha \in \Gamma(Q(\rho^i + \rho^{-i}) : Q)} (\rho^{ie'} + \rho^{-ie'})^\alpha =$$

$$\Sigma_{\alpha \in \Gamma(Q(\rho_e + \rho_e^{-1}) : Q)} (\rho_e^{e'} + \rho_e^{-e'})^\alpha = \tau_1(e, e').$$

Now the result follows from the character table of Theorem 2.1.

Theorem 3.16. In the above notation the character table of the irreducible rational representations of G are given in Tables 7 and 8.

Notation (2). Let $G = SL(2, q)$, where $q = 2^n$.

e and e' denote divisors of q-1 such that $e \leq \frac{q-1}{2}$ and $e' \leq \frac{q-1}{2}$.

f and f' denote divisors of q+1 such that $f \leq \frac{q+1}{2}$ and $f' \leq \frac{q+1}{2}$.

ρ_e is a primitive $\frac{q-1}{e}$-th root of unity.

σ_f is a primitive $\frac{q+1}{f}$-th root of unity.

$1, c, a, b, \rho$, and σ are as in Theorem 2.2.

The functions $\tau_1(e, e')$, $\tau_2(f, f')$, $A(e)$, $C(f)$ are as in Notation (1).

Lemma 3.17. The number of conjugacy classes of cyclic subgroups of $G= SL(2, q)$, where $q = 2^n$, is equal to $2+d^n(q-1)+d^n(q+1)$ and the different conjugacy classes of cyclic subgroups of G are represented by (1), (c), (a^e) and (b^f), and the irreducible characters of rational representations of G are 1_G, ψ, χ_e and θ_f.

Theorem 3.18. Let $G = SL(2,q)$ where $q=2_n$. In Notation (2) the character table of the irreducible rational representations of G is as follows:
(See Table 9).

Table 9. Character table of rational representations of $SL(2, 2^n)$

	1	c	$a^{e'}$	$b^{f'}$
1_G	1	1	1	1
ψ	q	0	1	-1
χ_e	$(q+1)A(e)$	$A(e)$	$_1(e,e')$	0
θ_f	$(q-1)C(f)$	$C(f)$	0	$-\tau_2(f,f')$

Acknowledgements

This paper is part of a Ph.D thesis submitted to the University of Manchester. The work was done under the supervision of Professor Brian Hartley (1992-94). I would also like to express my sincere gratitude to Dr. Robert Sandling for his help in preparing this paper.

References

1. Burns, J. M., Goldsmith, B., Hartley, B. and Sandling, R. On quasi-permutation representations of finite groups. *Glasgow Math. J.*, **36**, 301-308, (1994).
2. Dornhoff, L. *Group representation theory, part A*. Dekker, New York, (1971).
3. Huppert, B. and Blackburn, N. *Finite groups II*. Springer, Berlin, (1982).
4. Isaacs, I.M. *Character theory of finite groups*. Academic Press, New York, (1976).
5. Shahabi Shojaei, M.A. Schur indices of irreducible characters of $SL(2, q)$. *Arch. Math.*, **40**, 221-231, (1983).