University of Alberta

Irreducible Characters of $SL_k(\mathbb{Z}/p^n\mathbb{Z})$

by

Trevor Lee Pasanen

A thesis submitted to the Faculty of Graduate Studies and Research
in partial fulfillment of the requirements for the degree of

Masters of Science
in
Pure Mathematics

Department of Mathematical and Statistical Sciences

Fall, 2009
Edmonton, Alberta

Examining Committee

Dr. Gerald Cliff, Mathematical and Statistical Sciences

Dr. David McNeilly, Mathematical and Statistical Sciences

Dr. Lorna Stewart, Computing Science

Abstract

In this paper we find irreducible characters of $G = SL_k(\mathbb{Z}/p^n\mathbb{Z})$, where $n \geq 2$, $k = 2, 3$ and, p is an odd prime. In the case $k = 2$ we give a construction for every irreducible character of G without calculating the character values. Our method is based on finding a normal subgroup of G and applying Clifford theory.

Acknowledgements

I would like to thank Dr. Gerald Cliff, my supervisor, for his constant support during this research. I am also thankful to my fellow student Qianglong Wen for his comments and suggestions. I should also mention that my graduate studies in Canada were supported in part by NSERC. Of course, I am grateful to my wife and parents for their patience and love. Without them this work would never have come into existence.

Contents

List of Tables

List of Symbols

$M_n(R)$	The $n \times n$ matrices over R
$tr(A)$	The trace of a matrix A
A_{ij}	The i, j^{th} entry of a matrix A
$A \bmod m$	The matrix $A \in M_n(\mathbb{Z})$ with each entry reduced mod m
I	The identity matrix
I_n	The $n \times n$ identity matrix
C_n	The cyclic group of order n
&	Logical AND
inj	The natural injective map
$\lceil x \rceil$	The *ceiling* of a real number
ϕ_H	The restriction of a map ϕ to the subgroup H
$\phi\|_H$	The restriction of a map ϕ to the subgroup H

Chapter 1

Introduction

1.1 Understanding $SL_k(\mathbb{Z}/p^n\mathbb{Z})$

Definition 1.1.1. Given a commutative ring with unity $\mathbf{R}$, the *general linear group* $GL_k(\mathbf{R})$ is the group of invertible $k \times k$ matrices with entries in $\mathbf{R}$, under the group operation of matrix multiplication.

From linear algebra over a field $\mathbf{F}$ we know a matrix M with entries in $\mathbf{F}$ is invertible $\Leftrightarrow$ $\det M \neq 0$. More generally if we consider linear algebra over a commutative ring with unity $\mathbf{R}$ there is an analogous result shown below. The determinant of a square matrix M over a commutative ring with unity can be defined exactly as for a square matrix over a field, and the usual elementary properties of determinants carry over. We make use of the following facts carried over from standard linear algebra:

(i) $A, B \in M_k(\mathbf{R}) \Rightarrow \det AB = \det A \det B$

(ii) $M \in M_k(\mathbf{R}) \Rightarrow M \cdot \operatorname{adj}(M) = \operatorname{adj}(M) \cdot M = \det M \cdot I_k$, where $\operatorname{adj}(M)$ is the transpose of the matrix of cofactors.

Proposition 1.1.2. *Let* $\mathbf{R}$ *be a commutative ring with unity, and let* $M \in M_k(\mathbf{R})$*. Then* M *is invertible* $\Leftrightarrow \det M \in \mathbf{R}^\times$

Proof. " $\Rightarrow$ "

Let $M \in M_k(\mathbf{R})$be invertible

$\Rightarrow M \cdot N = I_k$ for some $N \in M_k(\mathbf{R})$

$\Rightarrow \det(M \cdot N) = \det I_k$

$\Rightarrow \det M \cdot \det N = 1$ using (i)

$\Rightarrow \det M \in \mathbf{R}^\times$ since $(\det M)^{-1} = \det N$ in $\mathbf{R}$.

"$\Leftarrow$"

Let $M \in M_k(\mathbf{R})$ with $\det M \in \mathbf{R}^\times$

$\Rightarrow (\det M)^{-1} \cdot M \cdot \text{adj }(M) = (\det M)^{-1} \cdot \text{adj }(M) \cdot M$

$= (\det M)^{-1} \cdot \det M \cdot I_k$ multiplying (ii) by $(\det M)^{-1}$

$\Rightarrow M \cdot \big((\det M)^{-1} \cdot \text{adj }(M)\big) = \big((\det M)^{-1} \cdot \text{adj }(M)\big) \cdot M = I_k$

$\Rightarrow M$ is invertible.

□

So, now

$$GL_k(\mathbf{R}) = \{M \in M_k(\mathbf{R}) \mid \det M \in \mathbf{R}^\times\},$$

and we can define $GL_k(\mathbf{R})$'s subgroup of interest:

Definition 1.1.3. Given a commutative ring with unity $\mathbf{R}$, the *special linear group* $SL_k(\mathbf{R})$ is a subgroup of $GL_k(\mathbf{R})$ with matrices having determinant 1.

Proposition 1.1.4. *Let* $\mathbf{R}$ *be a commutative ring with unity, there is a short exact sequence:*

$$1 \to SL_k(\mathbf{R}) \xrightarrow{inj} GL_k(\mathbf{R}) \xrightarrow{\det} \mathbf{R}^\times \to 1$$

Proof. To prove this we show the map det is surjective and image inj $=$ ker det ([3],p.379). The fact image inj $=$ ker det follows directly form the definition of $SL_k(\mathbf{R})$, so we are left to show: det is surjective. Let $x \in \mathbf{R}^\times$

$$\Rightarrow \begin{vmatrix} x & 0 & \dots & 0 \\ 0 & 1 & \dots & 0 \\ \vdots & \vdots & \ddots & \vdots \\ 0 & 0 & \dots & 1 \end{vmatrix} = x$$

$$\Rightarrow \begin{bmatrix} x & 0 & \dots & 0 \\ 0 & 1 & \dots & 0 \\ \vdots & \vdots & \ddots & \vdots \\ 0 & 0 & \dots & 1 \end{bmatrix} = M \in GL_k(\mathbf{R}), \text{ by Proposition 1.1.2.}$$

So we have $\det(M) = x$ and det is surjective. □

Applying the first isomorphism theorem to this short exact sequence gives the following corollary:

Corollary 1.1.5. *Given a commutative ring with unity* $\mathbf{R}$ *we have:*

$$SL_k(\mathbf{R}) \trianglelefteq GL_k(\mathbf{R}) \text{ and,}$$

$$GL_k(\mathbf{R})/SL_k(\mathbf{R}) \simeq \mathbf{R}^\times.$$

Chapter 2

Preliminary Results

2.1 The Size of $SL_k(\mathbb{Z}/p^n\mathbb{Z})$

In the following proof we use the fact ([1],p.11):

$$|GL_k(\mathbb{Z}/p^n\mathbb{Z})| = p^{k^2(n-1)} \prod_{t=1}^{k} \left(p^k - p^{(t-1)} \right).$$

Proposition 2.1.1.

$$| SL_k(\mathbb{Z}/p^n\mathbb{Z}) |= \frac{p^{(k^2-1)(n-1)} \prod_{t=1}^{k} \left(p^k - p^{(t-1)} \right)}{p-1}.$$

Proof. From 1.1.5 we have:

$$\begin{aligned}
&GL_k(\mathbb{Z}/p^n\mathbb{Z})/SL_k(\mathbb{Z}/p^n\mathbb{Z}) \simeq (\mathbb{Z}/p^n\mathbb{Z})^\times \\
&\Rightarrow \frac{| GL_k(\mathbb{Z}/p^n\mathbb{Z}) |}{| SL_k(\mathbb{Z}/p^n\mathbb{Z}) |} =| (\mathbb{Z}/p^n\mathbb{Z})^\times | \\
&\Rightarrow | SL_k(\mathbb{Z}/p^n\mathbb{Z}) |= \frac{p^{k^2(n-1)} \prod_{t=1}^{k} \left(p^k - p^{(t-1)} \right)}{p^{n-1}(p-1)}
\end{aligned}$$

□

Corollary 2.1.2.

$$| SL_2(\mathbb{Z}/p^n\mathbb{Z}) |= p^{3n-2}(p^2-1)$$

$$| SL_3(\mathbb{Z}/p^n\mathbb{Z}) |= p^{8n-5}(p^3-1)(p^2-1)$$

2.2 Quadratic Residues of $\mathbb{Z}/p^n\mathbb{Z}$ and the Subgroup S

In the last section of chapter 3 we will need the following preliminary results detailed in this section.

Definition 2.2.1. Let a, m be relatively prime integers. If there exists an integer x that satisfies

$$x^2 \equiv a \pmod{m}$$

then a is said to be a *quadratic residue* of m. Otherwise, a is called a *quadratic nonresidue* of m.

In the group $(\mathbb{Z}/p\mathbb{Z})^\times$ there are exactly $\frac{p-1}{2}$ quadratic residues of p. In this section we prove a corresponding result for $\mathbb{Z}/p^n\mathbb{Z}$, along with another result which will help calculate the size of an important subgroup of $SL_k(\mathbb{Z}/p^n\mathbb{Z})$.

Proposition 2.2.2. *In the group $(\mathbb{Z}/p^n\mathbb{Z})^\times$ there are exactly $\frac{p^n-p^{n-1}}{2}$ quadratic residues of p^n.*

Proof. Let $a \in (\mathbb{Z}/p^n\mathbb{Z})^\times$. Our first step is to show the equation $x^2 \equiv a \bmod p^n$ has exactly 0 or 2 solutions. To do this we show the equation $x^2 \equiv a \bmod p^n$ can not have a unique solution and has at most 2 solutions.

• Let $x \in (\mathbb{Z}/p^n\mathbb{Z})^\times$ be a solution so that, $x^2 \equiv a \bmod p^n$. Then $(-x)^2 \equiv a \bmod p^n$ so, $-x$ is also a solution. Now if there is to be exactly one solution to $x^2 \equiv a \bmod p^n$ we must have $-x \equiv x \bmod p^n$. But,

$$-x \equiv x \bmod p^n \;\Rightarrow\; 2x \equiv 0 \bmod p^n \overset{\text{p odd}}{\Rightarrow} x \equiv 0 \bmod p^n \;\Rightarrow\; x \notin (\mathbb{Z}/p^n\mathbb{Z})^\times$$

is a contradiction. Therefore, there can not be exactly one solution to $x^2 \equiv a \bmod p^n$.

• Let $x_1, x_2 \in (\mathbb{Z}/p^n\mathbb{Z})^\times$ be solutions to $x^2 \equiv a \bmod p^n$. First note, $p \nmid (x_1 - x_2)$ or $p \nmid (x_1 + x_2)$ since: $p \nmid 2x_1 = (x_1 - x_2) + (x_1 + x_2)$. Now

$$\Rightarrow x_1^2 \equiv x_2^2 \bmod p^n$$

$$\Rightarrow x_1^2 - x_2^2 \equiv (x_1 - x_2)(x_1 + x_2) \equiv 0 \bmod p^n$$

$$\Rightarrow p^n \mid (x_1 - x_2)(x_1 + x_2)$$

$$\Rightarrow p^n \mid (x_1 - x_2) \quad \text{or} \quad p^n \mid (x_1 + x_2) \qquad\qquad \text{since: } p \nmid (x_1 - x_2) \text{ or } p \nmid (x_1 + x_2)$$

$$\Rightarrow x_1 \equiv x_2 \bmod p^n \quad \text{or} \quad x_1 \equiv -x_2 \bmod p^n.$$

Therefore there can not be three (or more) solutions to $x^2 \equiv a \bmod p^n$ and our first step has been shown.

Now consider the set of all the squares in $(\mathbb{Z}/p^n\mathbb{Z})^\times$:

$$\left\{x_1^2, x_2^2, \ldots, x_{p^n-p^{n-1}}^2\right\},$$

and of course for each i: x_i above is a solution to $x^2 \equiv a \bmod p^n$ (letting $a \equiv x_i^2 \bmod p^n$). Therefore each square in $(\mathbb{Z}/p^n\mathbb{Z})^\times$ is equivalent to exactly two choices of x_i^2, in other words we can write our set in the form:

$$\left\{x_{i_1}^2 = x_{i_2}^2,\ x_{i_3}^2 = x_{i_4}^2,\ \ldots\ , x_{i_{p^n-p^{n-1}-1}}^2 = x_{i_{p^n-p^{n-1}}}^2\right\},$$

with exactly $\frac{p^n-p^{n-1}}{2}$ distinct elements. Meaning $(\mathbb{Z}/p^n\mathbb{Z})^\times$ has exactly $\frac{p^n-p^{n-1}}{2}$ quadratic residues of p^n.

□

Proposition 2.2.3. *Let $a \in (\mathbb{Z}/p^n\mathbb{Z})^\times$. a is a quadratic residue of p^n $\Leftrightarrow$ a is a quadratic residue of p. Equivalently in terms of the Legendre symbol:*

$$\left(\frac{a}{p^n}\right) = \left(\frac{a}{p}\right).$$

Proof. To prove this result, we show the inductive step: a is a quadratic residue of p^n $\Leftrightarrow$ a is a quadratic residue of p^{n+1}.

"$\Rightarrow$" Assume a is a quadratic residue of p^n, so we can pick $x_1 \in \mathbb{Z}$ with $x_1^2 \equiv a \bmod p^n$. This means $x_1^2 + mp^n = a$ for some $m \in \mathbb{Z}$. Now, $p \nmid a \Rightarrow p \nmid x_1 \Rightarrow x_1 \bmod p^{n+1}$ is a unit in $\mathbb{Z}/p^{n+1}\mathbb{Z}$ gives:

$$(x_1 + x_1^{-1}2^{-1}mp^n)^2 \equiv x_1^2 + mp^n + lp^{n+1} \equiv a \bmod p^{n+1}$$

for some integer l. Therefore, a is a quadratic residue of p^{n+1}

"$\Leftarrow$" If a is a quadratic residue of p^{n+1} then we can pick $x_1 \in \mathbb{Z}$ so:

$$x_1^2 \equiv a \bmod p^{n+1} \Rightarrow x_1^2 \equiv a \bmod p^n.$$

Therefore, a is a quadratic residue of p^n. □

With the help of the two results above we investigate the size of an important subgroup of $G = SL_2(\mathbb{Z}/p^n\mathbb{Z})$. Let ε be a quadratic nonresidue of p and define:

$$S = \left\{ \begin{bmatrix} a & b\varepsilon \\ b & a \end{bmatrix} \in G \,\middle|\, a, b \in \mathbb{Z}/p^n\mathbb{Z} \right\}.$$

Proposition 2.2.4. *S is an abelian subgroup of $SL_2(\mathbb{Z}/p^n\mathbb{Z})$*

Proof. Given $s, s' \in S$ we have:

$$s \cdot s' = \begin{bmatrix} a & b\varepsilon \\ b & a \end{bmatrix} \cdot \begin{bmatrix} c & d\varepsilon \\ d & c \end{bmatrix} = \begin{bmatrix} ac + bd\varepsilon & (ad+bc)\varepsilon \\ ad + bc & ac + bd\varepsilon \end{bmatrix} = \begin{bmatrix} c & d\varepsilon \\ d & c \end{bmatrix} \cdot \begin{bmatrix} a & b\varepsilon \\ b & a \end{bmatrix} = s' \cdot s \in S,$$

so S is an abelian subgroup of $SL_2(\mathbb{Z}/p^n\mathbb{Z})$. □

Proposition 2.2.5. $\mid S \mid = (p+1)p^{n-1}$.

Proof. In ([1],p.12) the size of a very similar subgroup

$$S' = \left\{ \begin{bmatrix} a & b\varepsilon \\ b & a \end{bmatrix} \in GL_2(\mathbb{Z}/p^n\mathbb{Z}) \,\middle|\, a, b \in \mathbb{Z}/p^n\mathbb{Z} \right\},$$

is calculated as: $(p^2-1)p^{2n-2}$. Naturally we pick the homomorphism $\det : S' \longrightarrow (\mathbb{Z}/p^n\mathbb{Z})^\times$ and use the first isomorphism theorem to show: $S'/S \simeq (\mathbb{Z}/p^n\mathbb{Z})^\times$. We need to show det is surjective, to do this we start by considering the case $n = 1$ and let $\mathbb{F}_{p^2} = \mathbb{Z}/p\mathbb{Z}(\sqrt{\varepsilon})$, and $\mathbb{F}_p = \mathbb{Z}/p\mathbb{Z}$. Now we have a Galois extension $\mathbb{F}_{p^2}/\mathbb{F}_p$ of degree 2 ([3], page: 566) so $Gal(\mathbb{F}_{p^2}/\mathbb{F}_p) = \{1, \sigma\}$. Define the norm map:

$$\begin{aligned} N : \mathbb{F}_{p^2} &\longrightarrow \mathbb{F}_p \\ x = a + b\sqrt{\varepsilon} &\longmapsto a^2 - \varepsilon b^2 = (a + b\sqrt{\varepsilon})(a - b\sqrt{\varepsilon}) = x \cdot \sigma(x), \end{aligned}$$

here the Galois automorphism σ is defined by $\sqrt{\varepsilon} \longmapsto -\sqrt{\varepsilon}$. We can also consider $x \longmapsto x^p$ which defines an automorphism of $\mathbb{F}_{p^2}$ fixing $\mathbb{F}_p$ therefore it is the nontrivial element of $Gal(\mathbb{F}_{p^2}/\mathbb{F}_p) =$

$\{1, \sigma\}$. Thus we can also write $\sigma(x) = x^p$. Now pick v a generater of the cyclic group $\mathbb{F}_{p^2}^\times$ so $< v^{p+1} >= \mathbb{F}_p^\times$. Finally pick an arbitrary $(v^{p+1})^i \in \mathbb{F}_p^\times$ and we have:

$$N(v^i) = v^i\sigma(v^i) = v^i(v^i)^p = (v^{p+1})^i$$

and so the norm map N is surjective. This shows when $n = 1$ the map det is surjective. For the case $n > 1$ consider $z \in (\mathbb{Z}/p^n\mathbb{Z})^\times$. We know from the case $n = 1$ we can write $z = a^2 - \varepsilon b^2 + pn_*$ for some a, b, n_*. By using 2.2.3 we can pick $y \in (\mathbb{Z}/p^n\mathbb{Z})^\times$ so that $y^2 = a^2 + pn_*$ and we have:

$$\begin{vmatrix} y & b\varepsilon \\ b & y \end{vmatrix} = y^2 - b^2\varepsilon = a^2 + pn_* - b^2\varepsilon = z.$$

Therefore det is surjective and we conclude:

$$\mid S \mid = \frac{\mid S' \mid}{\mid (\mathbb{Z}/p^n\mathbb{Z})^\times \mid} = \frac{(p^2-1)p^{2n-2}}{p^n - p^{n-1}} = (p+1)p^{n-1}.$$

$\square$

2.3 Cubic Residues of $\mathbb{Z}/p^n\mathbb{Z}$ and the Subgroup S

In the last section of chapter 4 we will need the subgroup S (defined below) in this section we calculate its size. In this section we let $p > 3$.

Definition 2.3.1. Let a, m be relatively prime integers. If there exists an integer x that satisfies

$$x^3 \equiv a \pmod{m}$$

then a is said to be a *cubic residue* of m. Otherwise, a is called a *cubic nonresidue* of m.

An irreducible polynomial $x^3 - cx^2 - bx - a \in \mathbb{Z}/p\mathbb{Z}[x]$ was chosen in ([1],p.13) to define:

$$B = \begin{bmatrix} 0 & 0 & a \\ 1 & 0 & b \\ 0 & 1 & c \end{bmatrix}.$$

We define B in the same way but we are very careful of which irreducible polynomial we pick as the following cases illustrate:

- If $p \equiv 1 \pmod 3$ then let a be a cubic nonresidue $b = 0, c = 0$
- If $p \equiv 2 \pmod 3$ then choose a, b and $c = 0$ so $x^3 - bx - a$ is irreducible.

With these choices we define:

$$S = \left\{ xI + yB + zB^2 \in SL_3(\mathbb{Z}/p^n\mathbb{Z}) \right\}.$$

The choices for a, b, c will make sense below when we calculate the size of S. The following gives the number of cubic residues in $(\mathbb{Z}/p^n\mathbb{Z})^\times$ (recall that we only consider $n \geq 2$).

Proposition 2.3.2.

$$\left| \left\{ x^3 \middle| x \in \mathbb{Z}/p^n\mathbb{Z} \right\} \right| = \begin{cases} p^n - p^{n-1} & p \equiv 2 \pmod 3 \\ \frac{p^n - p^{n-1}}{3} & p \equiv 1 \pmod 3 \end{cases}$$

Proof. We start by referencing ([8],p.218) where they prove the proposition for $n = 1$. So to prove our result as in 2.2.3, we show the inductive step: $a \in (\mathbb{Z}/p^n\mathbb{Z})^\times$ is a cubic residue of p^r $\Leftrightarrow$ a is a cubic residue of p^{r+1}. "$\Rightarrow$" Assume a is a cubic residue of p^r, so we can pick $x_1 \in \mathbb{Z}$ with $x_1^3 \equiv a \mod p^r$. This means $x_1^3 + mp^r = a$ for some $m \in \mathbb{Z}$. Now, $p \nmid a \Rightarrow p \nmid x_1 \Rightarrow x_1$ is a unit gives:

$$(x_1 + x_1^{-2}3^{-1}mp^r)^3 \equiv x_1^3 + mp^r + sp^{r+1} \equiv a \bmod p^{r+1}$$

for some integer s. Therefore a is a cubic residue of p^{r+1}. "$\Leftarrow$" is shown with the same method used in 2.2.3.

Now we can count the number of cubic residues in each case: when $p \equiv 2 \pmod 3$ we have $p-1$ cubic residues of p^n amongst each set: $\{ip+1, ip+2, \ldots, ip+(p-1)\}_i$ (by our inductive step), and there are p^{n-1} such sets in $(\mathbb{Z}/p^n\mathbb{Z})^\times$. Therefore there are $p^{n-1} \cdot (p-1) = p^n - p^{n-1}$, cubic residues of p^n. Similarly when $p \equiv 1 \pmod 3$ we have $\frac{p-1}{3}$ cubic residues of p^n amongst each set: $\{ip+1, ip+2, \ldots, ip+(p-1)\}_i$ so there are $p^{n-1} \cdot \frac{p-1}{3} = \frac{p^n - p^{n-1}}{3}$, cubic residues of p^n. $\square$

Proposition 2.3.3.

$$|S| = (p^2 + p + 1)p^{2n-2}$$

Proof. We use the same method from 2.2.5; so our goal is to calculate the image of det: $S' = \left\{xI + yB + zB^2 \in GL_3(\mathbb{Z}/p^n\mathbb{Z})\right\} \to (\mathbb{Z}/p^n\mathbb{Z})^\times$. We consider elements $xI + yB + zB^2 \in S'$ and look at their image:

$$\begin{array}{lll} (1) & x^3 \in Image(\det) & \text{letting } x \in (\mathbb{Z}/p^n\mathbb{Z})^\times, y = z = 0 \\ (2) & ay^3 \in Image(\det) & \text{letting } y \in (\mathbb{Z}/p^n\mathbb{Z})^\times, x = z = 0 \\ (3) & a^2z^3 \in Image(\det) & \text{letting } z \in (\mathbb{Z}/p^n\mathbb{Z})^\times, x = y = 0\ . \end{array}$$

Now we consider each case in our construction of B and use 2.3.2. When $p \equiv 2 \pmod 3$ all elements of $(\mathbb{Z}/p^n\mathbb{Z})^\times$ are cubic residues; so (1) gives $Image(\det) = (\mathbb{Z}/p^n\mathbb{Z})^\times$. When $p \equiv 1 \pmod 3$ we have chosen a to be a cubic nonresidue; so letting X be the subgroup of cubic residues $(1), (2), (3)$ respectively give the distinct coset $X, aX, a^2X \in Image(\det)$. In this case each of these cosets have size: $\frac{p^n - p^{n-1}}{3}$, therefore again $Image(\det) = (\mathbb{Z}/p^n\mathbb{Z})^\times$. So we use ([1],p.14) to conclude:

$$|S| = \frac{|S'|}{|Image(\det)|} = \frac{|S'|}{|(\mathbb{Z}/p^n\mathbb{Z})^\times|} = \frac{(p^3-1)p^{3n-3}}{p^n - p^{n-1}} = (p^2 + p + 1)p^{2n-2}.$$

$\square$

2.4 Character Theory

In this section we create a quick reference for the character theory used in this paper.

Definition 2.4.1. Let G be a group, and let V be a vector space. A *representation* of G in V is a group homomorphism $\rho\colon G \to \mathrm{GL}(V)$ from G to the general linear group $\mathrm{GL}(V)$ of invertible linear transformations of V. The representation ρ is *irreducible* if there is no proper nonzero invariant subspace of V under ρ.

Alternatively we have a corresponding definition.

Definition 2.4.2. A (*matrix*) representation of a group G is a group homomorphism between G and $GL_k(\mathbb{C})$, that is, a function

$$\rho : G \to GL_k(\mathbb{C})$$

such that $\rho(gh) = \rho(g)\rho(h)$.

Notice that this definition is equivalent to the above definition when the vector space V is finite dimensional over $\mathbb{C}$. The parameter k (or in the above case, the dimension of V) is called the *degree* of the representation denoted $dim(\rho)$.

Definition 2.4.3. Let G be a group. The Character χ of a representation

$$\rho : G \to GL_k(\mathbb{C})$$

is defined as:

$$\chi(g) = tr(\rho g) \ (g \in G).$$

We say χ is a character of G if χ is the character of some representation of G. Further, χ is an *irreducible* character of G if χ is the character of some irreducible representation of G. We define the set $Irr(G)$ to be the set of all irreducible characters of G. The *degree* of χ is given by degree of ρ.

Remark 2.4.4. By the definition, representations of degree 1 are also characters, these are called *linear* characters. In fact, these are the only characters which are homomorphisms: since given a character χ of a representation ρ, which is a homomorphism,

$$\chi(1) = \chi(1 \cdot 1) = \chi(1)^2 \Rightarrow \chi(1) = 1.$$

Also, $\chi(1) =$ "degree of χ" because:

$$\chi(1) = tr(\rho(1)) = tr(I_{dim(\rho)}) = dim(\rho) = \text{"degree of } \chi\text{"}.$$

In [5],p.82 all irreducible representations of finite abelian groups are determined. Since representations of abelian groups are always of degree 1 they are also characters. So all irreducible characters of finite abelian groups are determined. We now state the theorem.

Theorem 2.4.5. *Let G be the abelian group $C_{n_1} \times \ldots \times C_{n_r}$. Let g_i be a generator of C_{n_i} $(1 \leq r \leq 1)$. Let λ_i be n_ith roots of unity $(1 \leq r \leq 1)$. Define the map:*

$\rho_{\lambda_1,\ldots,\lambda_r} : G \longrightarrow \mathbb{C}$

$\rho_{\lambda_1,\ldots,\lambda_r}(g_1^{i_1} \ldots g_r^{i_r}) = \lambda_1^{i_1} \ldots \lambda_r^{i_r}.$

There are $|G|$ choices for $\rho_{\lambda_1,\ldots,\lambda_r}$ which give all the irreducible characters of G.

Definition 2.4.6. Let $H \leq G$ be a subgroup and suppose that θ is a character of H. We say θ is extendible to G if $\exists\chi$, a character of G, such that $\chi_H = \theta$. We call χ an *extension* of θ to G.

Given two subgroups with characters of degree 1 there is a very useful construction of an extension to the product of the two characters.

Definition 2.4.7. Let χ and ψ be characters of a group G. Then

$$[\chi, \psi] = \frac{1}{\mid G \mid} \sum_{g \in G} \chi(g)\overline{\psi(g)}$$

is the inner product of χ and ψ.

Proposition 2.4.8. *([6],p.21) Let χ and ψ be characters of G. Then $[\chi, \psi] = [\psi, \chi]$ is a nonnegative integer. Also χ is irreducible if and only if $[\chi, \chi] = 1$.*

Definition 2.4.9. Let $H \leq G$ be a subgroup and let θ be a character of H. Then θ^G, the induced character on G, is given by

$$\theta^G(g) = \frac{1}{\mid H \mid} \sum_{x \in G} \theta^\circ(xgx^{-1}),$$

where θ° is defined by $\theta^\circ(h) = \theta(h)$ if $h \in H$ and $\theta^\circ(y) = 0$ if $y \notin H$. Letting $g = 1$ in the above sum gives:

$$deg(\theta^G) = deg(\theta)\frac{\mid G \mid}{\mid H \mid}.$$

Proposition 2.4.10. *([6],p.73) Let $H < K < G$ and suppose that ϕ is a character of H. Then $(\phi^K)^G = \phi^G$.*

Lemma 2.4.11. *(Frobenius Reciprocity) Let $H \leq G$ and suppose that ϕ is a character on H and that χ is a character on G. Then*

$$[\phi, \chi_H] = [\phi^G, \chi].$$

Definition 2.4.12. ([6],p.78) Let $N \lhd G$. If ϕ is a character of N and $g \in G$, we define $\phi^g : N \to \mathbb{C}$ by $\phi^g(h) = \phi(ghg^{-1})$. We say that ϕ^g is *conjugate* to ϕ in G.

Lemma 2.4.13. *([6],p.78) Let $N \lhd G$ and let ϕ, θ be characters of N and $x, y \in G$. Then*

(a) ϕ^x is a character;

(b) $(\phi^x)^y = \phi^{xy}$;

(c) $[\phi^x, \theta^x] = [\phi, \theta]$;

(d) $[\chi_N, \phi^x] = [\chi_N, \phi]$ for characters χ of G.

Remark 2.4.14. Letting $N \lhd G$ we can now consider the following group action: let G act on the set $Irr(N)$ by defining $g \cdot \phi = \phi^g$, for $g \in G$ and $\phi \in Irr(N)$. This is an action since $\phi^1 = \phi$, and by part (b) above. Recall the stabilizer for this action:

$$G_\phi = \left\{ g \in G \;\middle|\; \phi^g = \phi \right\}.$$

When $G_\chi = G$ we say χ is *stable under* G.

We now state a result from [6],p.82 which is of fundamental importance in character theory of normal subgroups. This paper uses this theorem *extensively.*

Theorem 2.4.15. *Let $N \lhd G$, $\phi \in Irr(N)$, and $T = G_\phi$. Let*

$$\mathcal{A} = \{\psi \in Irr(T) \mid [\psi_N, \phi] \neq 0\}, \mathcal{B} = \{\chi \in Irr(G) \mid [\chi_N, \phi] \neq 0\}.$$

Then

(a) If $\psi \in \mathcal{A}$, then ψ^G is irreducible;

(b) The map $\psi \mapsto \psi^G$ is a bijection of $\mathcal{A}$ onto $\mathcal{B}$;

(c) If $\psi^G = \chi$, with $\psi \in \mathcal{A}$, then ψ is the unique irreducible constituent of χ_T which lies in $\mathcal{A}$;

(d) If $\psi^G = \chi$, with $\psi \in \mathcal{A}$, then $[\psi_N, \phi] = [\chi_N, \phi]$.

Corollary 2.4.16. *Let $N \lhd G$ and $\phi \in Irr(N)$. Then $\phi^G \in Irr(G) \Leftrightarrow G_\phi = N$.*

Proposition 2.4.17. *Let N be a subgroup affording the character ϕ of degree 1, and let H be a subgroup affording the character ψ of degree 1. If NH is a group with $N \trianglelefteq NH$, $\phi_{N\cap H} = \psi_{N\cap H}$ and ϕ stable under H then:*

$$\theta : NH \longrightarrow \mathbb{C}$$
$$\theta : nh \longmapsto \phi(n)\psi(h),$$

is a extension of ϕ and ψ to NH .

Proof. First we show θ is well defined. Consider two elements $n_1h_1, n_2h_2 \in NH$ where $n_1h_1 = n_2h_2$, we want to show $\theta(n_1h_1) = \theta(n_2h_2)$:

$$\begin{aligned}
&\theta(n_1h_1) \\
&= \phi(n_1)\psi(h_1) \\
&= \phi(n_2x)\psi(x^{-1}h_2) && \text{letting } x = n_2^{-1}n_1 = h_2h_1^{-1} \in N \cap H \\
&= \phi(n_2)\phi(x)\psi(x)^{-1}\psi(h_2) && \phi, \psi \text{ are homomorphisms} \\
&= \phi(n_2)\phi(x)\phi(x)^{-1}\psi(h_2) && \phi_{N\cap H} = \psi_{N\cap H} \\
&= \phi(n_2)\psi(h_2) \\
&= \theta(n_2h_2).
\end{aligned}$$

Also, θ is a homomorphism:

$$\begin{aligned}
&\theta(n_1h_1 \cdot n_2h_2) \\
&= \theta(n_1h_1n_2h_1^{-1}h_1h_2) \\
&= \phi(n_1h_1n_2h_1^{-1})\psi(h_1h_2) && \text{using } N \trianglelefteq NH \\
&= \phi(n_1)\phi(h_1n_2h_1^{-1})\psi(h_1)\psi(h_2) \\
&= \phi(n_1)\psi(h_1)\phi(n_2)\psi(h_2) && \text{since } \phi \text{ is stable under } H \\
&= \theta(n_1h_1) \cdot \theta(n_2h_2).
\end{aligned}$$

Therefore θ is a character with degree 1 of NH. $\square$

Lemma 2.4.18. *Let G be a group, $N \triangleleft G, S < G, S$ be abelian, and $G = NS$. If $\phi \in Irr(N)$ is such that $deg(\phi) = 1$ and ϕ is stable under G then ϕ is extendible to G.*

Note: whenever ϕ a character defined on a normal subgroup is extended to a group G, we also have ϕ **stable under** G.

Proposition 2.4.19. *Let $N \triangleleft G$ with G/N cyclic and let $\phi \in Irr(N)$ be stable under G. Then ϕ is extendible to G.*

Proposition 2.4.20. *Let G be a group, $H \leq G$. Let χ, ψ be characters of G such that $\chi \in Irr(G)$, $\chi_H \in Irr(H)$, and $[\chi, \psi] \neq 0$. Then $[\chi_H, \psi_H] \neq 0$.*

Proof. Let $\chi, \chi_1, \dots \chi_m$ be all the irreducible characters of G and $\chi_H, \phi_1, \dots \phi_l$ be all the irreducible characters of H and so [5], p.142 gives:

$$\begin{aligned}
&\psi = d\chi + d_1\chi_1 + \dots + d_m\chi_m && \text{where } d, d_i \text{ are non-negative integers and } d \neq 0 \\
&\Rightarrow \psi_H = d\chi_H + d_1\chi_{1_H} + \dots + d_m\chi_{m_H} && \text{by restricting to } H \\
&\Rightarrow \psi_H = d\chi_H + \sum_{i=1}^{m}\left(d_i\left(e_i\chi_H + \sum_{j=1}^{l}(e_{i_j}\phi_j)\right)\right) && \text{where } e_{i_j}, e_i \text{ are non-negative integers} \\
&\Rightarrow [\psi_H, \chi_H] = d + (d_1e_1 + \dots + d_me_m) \neq 0 && \text{since } d_1e_1 + \dots + d_me_m \text{ is a non-negative integer}
\end{aligned}$$

$\square$

Proposition 2.4.21. *Given* $N \trianglelefteq G$, *and* $\tilde{\chi} \in Irr(G/N)$, *then*

$$\chi : G \longrightarrow \mathbb{C}$$
$$\chi : g \longmapsto \tilde{\chi}(gN),$$

is an irreducible character of G, *called the lift of* $\tilde{\chi}$ *to* G. *Also,* χ *and* $\tilde{\chi}$ *have the same degree.*

Proposition 2.4.22. *Let* $N \triangleleft G$ *and let* $\chi \in Irr(G)$ *and* $\theta \in Irr(N)$ *with* $[\chi_N, \theta] \neq 0$. *Then the following are equivalent:*

(a) $\chi_N = e\theta$, *with* $e^2 = \mid G : N \mid$;

(b) χ *vanishes on* $G - N$ *and* θ *is invariant in* G;

(c) χ *is the unique irreducible constituent of* θ^G *and* θ *is invariant in* G.

Theorem 2.4.23. *(Gallagher) Let* $N \triangleleft G, \chi \in Irr(G)$ *be such that* $\chi_N = \theta \in Irr(N)$. *Then the characters* $\beta\chi$ *for* $\tilde{\beta} \in Irr(G/N)$ *are irreducible, distinct for distinct* $\tilde{\beta}$, *and are all of the irreducible constituents of* θ^G.

Theorem 2.4.24. *(Clifford) Let* $N \triangleleft G$ *and* $\chi \in Irr(G)$. *Let* ϕ *be an irreducible constituent of* χ_N *and suppose* $\phi = \phi_1, \phi_2, \ldots, \phi_t$ *are the distinct conjugates of* ϕ *in* G. *Then*

$$\chi_N = [\chi_N, \phi] \sum_{i=1}^{t} \phi_i.$$

Chapter 3

Irreducible Character Degrees of $SL_2(\mathbb{Z}/p^n\mathbb{Z})$

3.0 Introduction

In this chapter we let,

$$G = SL_2(\mathbb{Z}/p^n\mathbb{Z})$$

and find characters of G using 2.4.15. Our first step is to find a normal subgroup of G, so throughout this chapter for an integer m, we let:

$$L_m = \left\{ I + p^m A \;\middle|\; A \in M_2(\mathbb{Z}/p^n\mathbb{Z}),\ \det(I + p^m A) = 1 \right\}.$$

Proposition 3.0.1. *L_m is a normal subgroup of G, with $|L_m| = p^{3(n-m)}$. Furthermore when $\lceil \frac{n}{2} \rceil \leq m$, L_m is abelian.*

Proof. Start by considering the map

$$f : G \longrightarrow SL_2(\mathbb{Z}/p^m\mathbb{Z})$$
$$f : A \longmapsto A \bmod p^m.$$

The map f is a homomorphism since given $A, B \in G$

$$f(AB) = AB \bmod p^m = (A \bmod p^m) \cdot (B \bmod p^m) = f(A)f(B).$$

Now $\ker(f) = L_m$ and we have $L_m \trianglelefteq G$. To find $|L_m|$ we consider:

$$K_m = \left\{ I + p^m A \;\middle|\; A \in M_2(\mathbb{Z}/p^n\mathbb{Z}) \right\} \leq GL_2(\mathbb{Z}/p^n\mathbb{Z}).$$

The map $\det : K_m \longrightarrow (\mathbb{Z}/p^n\mathbb{Z})^\times$ has $\ker(\det) = L_m$ so by the first isomorphism theorem:

$$|L_m| = \frac{|K_m|}{|\det(K_m)|} = \frac{|K_m|}{|\{1 + p^m x |\, x \in \mathbb{Z}/p^n\mathbb{Z}\}|} = \frac{p^{4(n-m)}}{p^{n-m}} = p^{3(n-m)}.$$

Also, given that $\lceil \frac{n}{2} \rceil \leq m$, L_m is abelian because:

$$\begin{aligned}
&(I + p^m A)(I + p^m B) \\
&= I + p^m(A + B) + p^{2m} AB \\
&= I + p^m(A + B) && p^{2m} = 0 \text{ since } 2m \geq 2\left\lceil \frac{n}{2} \right\rceil \geq n \\
&= I + p^m(B + A) + p^{2m} BA \\
&= (I + p^m A)(I + p^m B).
\end{aligned}$$

□

Remark 3.0.2. Consider the map:

$$\pi : L_m \longrightarrow M_2(\mathbb{Z}/p^{n-m}\mathbb{Z})$$
$$\pi : I + p^m A \longmapsto A \bmod p^{n-m},$$

which is well defined since given $I + p^m A, I + p^m B \in L_m$ we have:

$$I + p^m A = I + p^m B \;\;\Rightarrow\;\; p^m A = p^m B \;\;\Rightarrow A \equiv B \bmod p^{n-m}.$$

Also π is injective because:

$$A \bmod p^{n-m} \equiv \pi(I + p^m A) \equiv \pi(I + p^m B) \equiv B \bmod p^{n-m} \;\;\Rightarrow\;\; p^m A = p^m B \;\;\Rightarrow I + p^m A = I + p^m B.$$

Therefore we know L_m is in a *one to one correspondence* with $\pi(L_m)$. So by picking an element in $\pi(L_m)$ we can uniquely determine an element in L_m. We now make a **convention throughout this paper** to use this correspondence when in context; so it makes sense to say:

$$L_m = \left\{ I + p^m A \;\middle|\; A \in M_2(\mathbb{Z}/p^{n-m}\mathbb{Z}),\; \det(I + p^m A) = 1 \right\}.$$

Note: the corresponding convention is also made on other subgroups of G.

Now for the case $\lceil \frac{n}{2} \rceil \leq m$ we classify L_m as an abelian group. This will provide us with irreducible characters of L_m as all irreducible characters of any abelian group are known.

Proposition 3.0.3. *$L_m \simeq \mathbb{Z}/p^{n-m}\mathbb{Z} \times \mathbb{Z}/p^{n-m}\mathbb{Z} \times \mathbb{Z}/p^{n-m}\mathbb{Z}$ when $\lceil \frac{n}{2} \rceil \leq m$.*

Proof. We start by defining the following matrices:

$$B_1 = I + p^m \begin{pmatrix} 1 & 0 \\ 0 & -1 \end{pmatrix}, B_2 = I + p^m \begin{pmatrix} 0 & 1 \\ 0 & 0 \end{pmatrix}, B_3 = I + p^m \begin{pmatrix} 0 & 0 \\ 1 & 0 \end{pmatrix}.$$

Notice that when multiplying elements $I + p^m A, I + p^m B \in L_m$, as above we have the equality:

$$(I + p^m A)(I + p^m B) = I + p^m (A + B),$$

so multiplication in L_m is determined by the addition $A + B$. We use this fact to calculate the subgroups:

$$< B_1 >= \left\{ I + p^m \begin{pmatrix} i & 0 \\ 0 & -i \end{pmatrix} \;\middle|\; i \in \mathbb{Z}/p^{n-m}\mathbb{Z} \right\},$$

$$< B_2 >= \left\{ I + p^m \begin{pmatrix} 0 & j \\ 0 & 0 \end{pmatrix} \;\middle|\; j \in \mathbb{Z}/p^{n-m}\mathbb{Z} \right\},$$

$$< B_3 >= \left\{ I + p^m \begin{pmatrix} 0 & 0 \\ k & 0 \end{pmatrix} \;\middle|\; k \in \mathbb{Z}/p^{n-m}\mathbb{Z} \right\}.$$

Now,

• $< B_1 >< B_2 > \leq L_m$	since L_m is abelian
• $< B_1 >, < B_2 > \trianglelefteq < B_1 >< B_2 >$	since L_m is abelian
• $< B_1 > \bigcap < B_2 >= I$	by examining the above subgroups

$\Longrightarrow$

$< B_1 >< B_2 >=< B_1 > \times < B_2 >$	by ([4],p.248) (internal direct product).

Similarly,

•$(< B_1 > \times < B_2 >) < B_3 > \leq L_m$	since L_m is abelian
• $< B_1 > \times < B_2 >, < B_3 > \trianglelefteq (< B_1 > \times < B_2 >) < B_3 >$	since L_m is abelian
• $< B_1 > \times < B_2 > \bigcap < B_3 >= I$	$< B_1 > \times < B_2 >$ contains only upper triangular matrices while, $< B_3 >$ contains only lower triangular matrices

$\Longrightarrow$

$(< B_1 > \times < B_2 >) < B_3 >=< B_1 > \times < B_2 > \times < B_3 >$	by ([4],p.248) (internal direct product).

So now we have the direct product:

$$< B_1 > \times < B_2 > \times < B_3 > \subseteq L_m.$$

By the definition of the direct product we can calculate the size

$$|< B_1 > \times < B_2 > \times < B_3 >| = p^{n-m}p^{n-m}p^{n-m} = p^{3(n-m)}.$$

From 3.0.1 we also have $|L_m| = p^{3(n-m)}$. So the facts $|L_m| = |< B_1 > \times < B_2 > \times < B_3 >|$ and $< B_1 > \times < B_2 > \times < B_3 > \subseteq L_m$ imply:

$$< B_1 > \times < B_2 > \times < B_3 >= L_m.$$

Finally the map:

$$< B_1 > \times < B_2 > \times < B_3 > \longrightarrow \mathbb{Z}/p^{n-m}\mathbb{Z} \times \mathbb{Z}/p^{n-m}\mathbb{Z} \times \mathbb{Z}/p^{n-m}\mathbb{Z}$$
$$B_1^i B_2^j B_3^k \longmapsto (i, j, k) \text{ for } i, j, k \in \mathbb{Z}/p^{n-m}\mathbb{Z}$$

is an isomorphism.

$$\therefore L_m \simeq \mathbb{Z}/p^{n-m}\mathbb{Z} \times \mathbb{Z}/p^{n-m}\mathbb{Z} \times \mathbb{Z}/p^{n-m}\mathbb{Z}.$$

□

Remark 3.0.4. From this proof we can see that every element of L_m can be written uniquely in the form $B_1^i B_2^j B_3^k$ for $i, j, k \in \mathbb{Z}/p^{n-m}\mathbb{Z}$. We will continue to use B_1, B_2, B_3 in the next section.

Now that we know which abelian group L_m is we can use 2.4.5 to find it's characters.

3.1 An Irreducible Character of Degree $\frac{p^{n-2}(p^2-1)}{2}$.

3.1.1 When n is Even.

In this subsection we assume n is even and define m so that: $\boldsymbol{n=2m}$.

Our goal is to find all the ingredients to use 2.4.15 to find a character of G. We start by picking three p^m-th roots of unity: $(1, \omega, 1)$, where ω is some *primitive* p^m-th root of unity. Using these roots of unity with 2.4.5 we can define a character of L_m:

$$\phi \begin{bmatrix} 1+ip^m & jp^m \\ kp^m & 1-ip^m \end{bmatrix} = \rho_{1,\omega,1}(B_1^i B_2^j B_3^k) = 1^i \omega^j 1^k = \omega^j,$$

where $B_1^i B_2^j B_3^k \in L_m$ as in 3.0.3. Our first step is to calculate the stabilizer of ϕ with G acting on $Irr(L_m)$ (the group action used here is defined in 2.4.14).

Proposition 3.1.1.

$$G_\phi = T = \left\{ \begin{bmatrix} \delta + ap^m & bp^m \\ c & d \end{bmatrix} \middle| \begin{array}{ll} a, b \in \mathbb{Z}/p^m\mathbb{Z}, & c \in \mathbb{Z}/p^{2m}\mathbb{Z}, \\ d = (1+p^m bc)(\delta - ap^m), & \delta \in \{1, -1\} \end{array} \right\},$$

and

$$\mid G_\phi \mid = 2p^{4m}.$$

Proof. The proof is by double inclusion:

"$\subseteq$" Let $g = \begin{bmatrix} a & b \\ c & d \end{bmatrix} \in G_\phi$

$\Rightarrow \phi^g = \phi$

$$\Rightarrow \phi^g \begin{bmatrix} 1+xp^m & yp^m \\ wp^m & 1-xp^m \end{bmatrix} = \phi \begin{bmatrix} 1+xp^m & yp^m \\ wp^m & 1-xp^m \end{bmatrix} \qquad \text{equality holding } \forall x, y, w \in \mathbb{Z}/p^m\mathbb{Z}$$

$$\Rightarrow \phi \left(\begin{bmatrix} a & b \\ c & d \end{bmatrix} \begin{bmatrix} 1+xp^m & yp^m \\ wp^m & 1-xp^m \end{bmatrix} \begin{bmatrix} d & -b \\ -c & a \end{bmatrix} \right) = \omega^y$$

$$\Rightarrow \phi \begin{bmatrix} 1+p^m(2bcx+bdw-acy+x) & p^m(-2bax-b^2w+a^2y) \\ p^m(2dcx+d^2w-c^2y) & 1-p^m(2bcx+bdw-acy+x) \end{bmatrix} = \omega^y$$

$$\Rightarrow \omega^{-2\,bax-b^2w+a^2y} = \omega^y$$

$\Rightarrow -2bax - b^2w + a^2y \equiv y \bmod p^m$ — since ω is a primitive p^m-th root of unity

$\Rightarrow a^2 \equiv 1 \bmod p^m$ — letting: $x=0, y=1, w=0$

$\& \ -2ba \equiv 0 \bmod p^m$ — letting: $x=1, y=0, w=0$

$\Rightarrow a \equiv \pm 1 \bmod p^m$ — by [7],p.157

$\& \ b \equiv 0 \bmod p^m$ — since $-2a \in (\mathbb{Z}/p^m\mathbb{Z})^\times$

$$\Rightarrow g = \begin{bmatrix} \delta + n_1p^m & n_2p^m \\ c & (1+p^mn_2c)(\delta - n_1p^m) \end{bmatrix}$$

for $n_1, n_2 \in \mathbb{Z}/p^m\mathbb{Z}$, and using: $d = (1+bc)a^{-1}$, and $\delta \in \{1,-1\}$

$\Rightarrow g \in T$

$\Rightarrow G_\phi \subseteq T$

"$\supseteq$" Let $t = \begin{bmatrix} \delta + ap^m & bp^m \\ c & d \end{bmatrix} \in T$

$$\Rightarrow \ \phi^t \begin{bmatrix} 1+xp^m & yp^m \\ wp^m & 1-xp^m \end{bmatrix}$$

for $x, y, w \in \mathbb{Z}/p^m\mathbb{Z}$

$$= \phi\left(\begin{bmatrix}\delta + ap^m & bp^m \\ c & d\end{bmatrix}\begin{bmatrix}1+xp^m & yp^m \\ wp^m & x-ip^m\end{bmatrix}\begin{bmatrix}d & -bp^m \\ -c & \delta+ap^m\end{bmatrix}\right)$$

$$= \phi\begin{bmatrix}1+\delta(dx-cy)p^m & yp^m \\ p^m(2dcx+d^2w-c^2y) & 1-\delta(dx-cy)p^m\end{bmatrix}$$

$$= \phi\begin{bmatrix}1+xp^m & yp^m \\ wp^m & x-ip^m\end{bmatrix}$$

$$\Rightarrow \phi^t = \phi$$

$$\Rightarrow t \in G_\phi$$

$$\Rightarrow T \subseteq G_\phi$$

$\therefore\ T = G_\phi$. Also in the set T there are 2 choices for δ, p^m choices for each of $\{a, b\}$ and, p^{2m} choices for c. These choices determine d so we have:

$$\mid G_\phi \mid = \mid T \mid = 2 \cdot p^m \cdot p^m \cdot p^{2m} = 2p^{4m}.$$

□

Our next step is to find an extension of ϕ to G_ϕ

Proposition 3.1.2. *Define the map:*

$$\psi : G_\phi \longrightarrow \mathbb{C}$$

$$\psi : \begin{bmatrix}\delta + ap^m & bp^m \\ c & d\end{bmatrix} \longmapsto \omega^{\delta b}.$$

This map is an extension of ϕ to G_ϕ. In other words ψ is a character of G_ϕ with $\psi|_{L_m} = \phi$.

Proof. We shall show ψ is a homomorphism telling us ψ is both a representation and a character of G_ϕ with degree one (2.4.4).

Let:

$$A = \begin{bmatrix} \delta + ap^m & bp^m \\ c & d \end{bmatrix}, \ A' = \begin{bmatrix} \delta' + a'p^m & b'p^m \\ c' & d' \end{bmatrix} \in G_\phi$$

Now,

$\psi(AA')$

$= \psi \begin{bmatrix} \delta\delta' + xp^m & (\delta b' + bd')p^m \\ y & z \end{bmatrix}$ — for some $x, y, z \in \mathbb{Z}/p^{2m}\mathbb{Z}$

$= \omega^{\delta\delta'(\delta b' + bd')}$

$= \omega^{\delta\delta'(\delta b' + b(1+b'c'p^m)(\delta' - a'p^m))}$ — noting $A' \in G_\phi$ gives: $d' = (1 + b'c'p^m)(\delta' - a'p^m)$

$= \omega^{\delta' b' + \delta b + wp^m}$ — for some $w \in \mathbb{Z}/p^{2m}\mathbb{Z}$ and since $\delta^2 = \delta'^2 = 1$

$= \omega^{\delta' b' + \delta b}$ — since ω is a p^mth root of unity

$= \psi(A)\psi(A'),$

so ψ is a character of G_ϕ. We also note:

$$\psi|_{L_m}(I + p^m C) = \omega^{C_{12}} = \phi(I + p^m C),$$

for all $I + p^m C$ in L_m. Therefore:

$$\psi|_{L_m} = \phi.$$

$\square$

Finally we use 2.4.15:

- $L_m \lhd G$ — from 3.0.1
- $\phi \in Irr(L_m)$ — by our definition using 2.4.5
- $\psi \in Irr(G_\phi)$ — from 3.1.2
- $[\psi|_{L_m}, \phi] = 1 \neq 0$ — since $\psi|_{L_m} = \phi$

$\implies$

$\chi = \psi^G$ is irreducible.

In conclusion we have calculated the character:

$$\chi(g) = \psi^G(g) = \frac{1}{\mid G_\phi \mid} \sum_{x \in G} \psi^\circ(xgx^{-1}),$$

with,

$$deg(\chi) = \frac{\mid G \mid}{\mid G_\phi \mid} = \frac{(p^2-1)p^{6m-2}}{2p^{4m}} = \frac{(p^2-1)p^{2m-2}}{2} = \frac{(p^2-1)p^{n-2}}{2} \qquad (2.4.9).$$

3.1.2 When n is Odd.

In this subsection we assume n is odd and define m so that: $\boldsymbol{n=2m+1}$. In this case we start with L_{m+1} as our normal subgroup of G. As before, we start by picking three p^m-th (since: $n-(m+1) = m$) roots of unity: $(1, \omega, 1)$, where ω is some primitive p^m-th root of unity. Using these roots of unity with 2.4.5 we can define ϕ a character of L_{m+1}:

$$\phi \begin{bmatrix} 1+ip^{m+1} & jp^{m+1} \\ kp^{m+1} & 1-ip^{m+1} \end{bmatrix} = \rho_{1,\omega,1}(B_1^i B_2^j B_3^k) = 1^i \omega^j 1^k = \omega^j,$$

where $B_1^i B_2^j B_3^k \in L_m$ as in 3.0.3.

We can trace the proof of 3.1.1 (changing p^m to p^{m+1} appropriately) to get the stabilizer of ϕ:

$$G_\phi = T = \left\{ \begin{bmatrix} \delta + ap^m & bp^m \\ c & d \end{bmatrix} \middle| \begin{array}{cc} a, b \in \mathbb{Z}/p^{m+1}\mathbb{Z}, & c \in \mathbb{Z}/p^{2m+1}\mathbb{Z}, \\ d = (1+p^m bc)(\delta + ap^m)^{-1}, & \delta \in \{1, -1\} \end{array} \right\}$$

although, in this case the size is different: $|G_\phi| = 2p^{2n+1}$. As a result inducing up a linear character from G_ϕ to G (like in the even case) would not give our desired character because G_ϕ is too big.

To handle this problem we define:

$$N = \left\{ \begin{bmatrix} \delta + ap^m & bp^{m+1} \\ c & d \end{bmatrix} \middle| \begin{array}{cc} a \in \mathbb{Z}/p^{m+1}\mathbb{Z}, b \in \mathbb{Z}/p^m\mathbb{Z}, & c \in \mathbb{Z}/p^{2m+1}\mathbb{Z}, \\ d = (1 + p^{m+1}bc)(\delta + ap^m)^{-1}, & \delta \in \{1, -1\} \end{array} \right\}.$$

Proposition 3.1.3. $N \trianglelefteq T$

Proof. First, the facts: N is a subset of the *subgroup* G_ϕ and for $A, B \in N$ we have $(AB)_{12} = xp^{m+1}$ for some $x \in \mathbb{Z}/p^m\mathbb{Z}$ imply N is a subgroup. Now we show N is normal in G_ϕ . Let $n = \begin{bmatrix} \delta + ap^m & bp^{m+1} \\ c & d \end{bmatrix} \in N$, $t = \begin{bmatrix} \delta' + a'p^m & b'p^m \\ c' & d' \end{bmatrix} \in G_\phi$. Now,

- $p^{m+1} \big| (tnt^{-1})_{12}$
- N is a subset of the *subgroup* G_ϕ

implies $tnt^{-1} \in N$; therefore $N \trianglelefteq G_\phi$. □

Our next step is to find an extension of ϕ to N. Tracing the proof of 3.1.2 gives the character:

$$\psi : N \longrightarrow \mathbb{C}$$

$$\psi : \begin{bmatrix} \delta + ap^m & bp^{m+1} \\ c & d \end{bmatrix} \longmapsto \omega^{\delta b}.$$

this character is an extension of ϕ to N. Again we have interest in the stabilizer.

Proposition 3.1.4. $T_\psi = N$.

Proof. We start by showing T_ψ is a proper subset of T. Let: $t = \begin{bmatrix} 1 & p^m \\ 0 & 1 \end{bmatrix} \in T$, now:

$$\psi\left(t \begin{bmatrix} 1 + p^m & 0 \\ 0 & 1 - p^m + p^{2m} \end{bmatrix} t^{-1} \right) = \omega^0 \quad \Rightarrow \quad \omega^{-2p^{m-1}} = \omega^0 \quad \Rightarrow \quad p^{m-1} \equiv 0 \mod p^m$$

is a contradiction. Thus $t \notin T_\psi$ and we have: $T_\psi \subsetneq T$. Now note:

- $N \subseteq T_\psi$ — since $\psi\left(n'n(n')^{-1}\right) = \psi(n')\psi(n)\psi\left((n')^{-1}\right) = \psi(n)$ for $n, n' \in N$
- $[T : N] = p$ — since $\mid N \mid = 2p^{2n}$, $\mid T \mid = 2p^{2n+1}$
- $T_\psi \subsetneq T$ — above

implying $T = N$. □

We can now use 2.4.16 to get a character of T:

- $N \lhd T$ from 3.1.3
- $\psi \in Irr(N) = Irr(T_\psi)$ from 3.1.4

$\Longrightarrow$

ψ^T is irreducible.

By the Frobenius Reciprocity theorem $1 = \left[\psi^T, \psi^T\right] = \left[\psi, \psi^T_N\right] \neq 0$. Now, $\psi \in Irr(N)$, $\psi_{L_{m+1}} = \phi \in Irr(L_{m+1})$ so we use 2.4.20 implying $\left[\psi_{L_{m+1}}, (\psi^T_N)_{L_{m+1}}\right] = \left[\phi, \psi^T_{L_{m+1}}\right] \neq 0$. Finally we use 2.4.15:

- $L_{m+1} \lhd G$ from 3.0.1
- $\phi \in Irr(L_{m+1})$ since $deg(\phi) = 1$
- $\psi^T \in Irr(G_\phi)$ from above recalling $T = G_\phi$
- $\left[\phi, \psi^T_{L_{m+1}}\right] \neq 0$

$\Longrightarrow$

$\chi = (\psi^T)^G = \psi^G$ is irreducible.

The degree of χ is:

$$deg(\psi^G) = \frac{\mid G \mid}{\mid N \mid} = \frac{(p^2-1)p^{3n-2}}{2p^{2n}} = \frac{(p^2-1)p^{n-2}}{2} \qquad (2.4.9).$$

3.2 An Irreducible Character of Degree $p^{n-1}(p+1)$

We will use the same strategy as we used in the previous section, but this time we will start with a different character of our normal subgroup (L_m and L_{m+1}) of G. To construct our character we use the fact $(\mathbb{Z}/p^{2m}\mathbb{Z})^\times$ is cyclic ([3], p.314) and define the injective homomorphism:

$$\lambda : (\mathbb{Z}/p^{2m}\mathbb{Z})^\times \longrightarrow \mathbb{C}^\times$$

$$\lambda : v^i \longmapsto \omega^i.$$

where ω is a $(p^{2m} - p^{2m-1})^{\text{th}}$ root of unity and v is a generator of $(\mathbb{Z}/p^{2m}\mathbb{Z})^\times$. Now define the map:

$$\phi : M_2(\mathbb{Z}/p^n\mathbb{Z}) \longrightarrow \mathbb{C}^\times$$

$$\phi : A_{11} \longmapsto \lambda(A_{11}).$$

We use the map ϕ **throughout** the next two subsections. ϕ will be restricted to different subgroups so it becomes a group homomorphism and therefore also a character of degree 1.

3.2.1 When n is Even.

In this subsection we assume n is even and define m so that: $\boldsymbol{n=2m}$. Now for $A, B \in L_m$ we have,

$$\phi_{L_m}(AB) = \lambda((AB)_{11}) = \lambda(A_{11}B_{11}) = \lambda(A_{11})\lambda(B_{11}) = \phi_{L_m}(A)\phi_{L_m}(B) \quad (*)$$

so ϕ_{L_m} is a homomorphism and therefore an irreducible character (also a representation) of L_m. As in the previous section we need to calculate the stabilizer of ϕ_{L_m} with G acting on $Irr(L_m)$ (2.4.14).

Proposition 3.2.1.

$$G_{\phi_{L_m}} = T = \left\{ \begin{bmatrix} a & bp^m \\ cp^m & a^{-1} \end{bmatrix} \middle| \begin{array}{c} a \in (\mathbb{Z}/p^{2m}\mathbb{Z})^\times, \\ b, c \in \mathbb{Z}/p^m\mathbb{Z} \end{array} \right\},$$

and

$$|G_{\phi_{L_m}}| = p^{4m-1}(p-1).$$

Proof. The proof is by double inclusion:

"$\subseteq$" Let $g = \begin{bmatrix} a & b \\ c & d \end{bmatrix} \in G_{\phi_{L_m}}$

$\Rightarrow \phi_{L_m}^g = \phi_{L_m}$

$\Rightarrow \lambda(1 + p^m(2bcx + bdw - acy + x)) = \lambda(1 + p^m x)$ — from tracing 3.1.1 with equality holding $\forall x, y, w \in \mathbb{Z}/p^m\mathbb{Z}$

$\Rightarrow 1 + p^m(2bcx + bdw - acy + x) = 1 + p^m x$ — since λ is injective

$\Rightarrow p^m(2bcx + bdw - acy) = 0$

$\Rightarrow$

(1) $p^m 2bc = 0$ — letting (x, w, y)=(1,0,0)

(2) $p^m bd = 0$ — letting (x, w, y)=(0,1,0)

(3) $-p^m ac = 0$ — letting (x, w, y)=(0,0,1)

$\Rightarrow b = n_1 p^m$ — since $2c$ is a unit in (1) or d is a unit in (2)

$\Rightarrow a$ is a unit — since one of a, b must be a unit

$\Rightarrow c = n_2 p^m$ — since $-a$ is a unit in (3)

$\Rightarrow d = a^{-1}$ — since $ad - bc = ad - n_1 n_2 p^{2m} = ad = 1$

$\Rightarrow g = \begin{bmatrix} a & n_1 p^m \\ n_2 p^m & a^{-1} \end{bmatrix}$

$\Rightarrow g \in T$

$\Rightarrow G_{\phi_{L_m}} \subseteq T$

"$\supseteq$" Let $t = \begin{bmatrix} a & bp^m \\ cp^m & a^{-1} \end{bmatrix} \in T$

$\Rightarrow \ \phi_{L_m}^t \begin{bmatrix} 1+xp^m & yp^m \\ wp^m & x-ip^m \end{bmatrix}$ for $x, y, w \in \mathbb{Z}/p^m\mathbb{Z}$

$= \ \phi_{L_m} \left(\begin{bmatrix} a & bp^m \\ cp^m & a^{-1} \end{bmatrix} \begin{bmatrix} 1+xp^m & yp^m \\ wp^m & x-ip^m \end{bmatrix} \begin{bmatrix} a^{-1} & -bp^m \\ -cp^m & a \end{bmatrix} \right)$

$= \ \phi_{L_m} \begin{bmatrix} 1+xp^m & a^2yp^m \\ a^{-2}wp^m & 1-xp^m \end{bmatrix}$

$= \ \phi_{L_m} \begin{bmatrix} 1+xp^m & yp^m \\ wp^m & x-ip^m \end{bmatrix}$ since these matrices have the same entry in position $1, 1$

$\Rightarrow \phi_{L_m}^t = \phi_{L_m}$

$\Rightarrow t \in G_{\phi_{L_m}}$

$\Rightarrow T \subseteq G_{\phi_{L_m}}$

Therefore $T = G_{\phi_{L_m}}$. Also, in the set T there are $p^{2m} - p^{2m-1}$ choices for a (the number of units in $\mathbb{Z}/p^{2m}\mathbb{Z}$) and p^m choices for each of $\{b, c\}$. So we have:

$$\mid G_{\phi_{L_m}} \mid = \mid T \mid = (p^{2m} - p^{2m-1}) \cdot p^m \cdot p^m = p^{4m-1}(p-1).$$

$\square$

Now the same argument in (*) shows ϕ_T is a homomorphism and therefore an extension of ϕ_{L_m}. Finally we use 2.4.15:

- $L_m \lhd G$ — from 3.0.1
- $\phi_{L_m} \in Irr(L_m)$ — ϕ_{L_m} a homomorphism with $\phi_{L_m}(1) = 1$
- $\phi_T \in Irr(G_{\phi_{L_m}})$ — ϕ_T a homomorphism with $\phi_T(1) = 1$
- $\left[\phi_T|_{L_m}, \phi_{L_m}\right] = [\phi_{L_m}, \phi_{L_m}] = 1 \neq 0$

$\Longrightarrow$

$\chi = \phi_T^G$ is irreducible.

In conclusion, we have calculated the character:

$$\chi(g) = \frac{1}{\mid G_\phi \mid} \sum_{x \in G} \psi^\circ(xgx^{-1}),$$

with

$$deg(\chi) = \frac{|G|}{|G_\phi|} = \frac{(p^2-1)p^{6m-2}}{p^{4m-1}(p-1)} = (p+1)p^{2m-1} \qquad (2.4.9).$$

3.2.2 When n is Odd.

In this subsection we assume n is odd and define m so that: $\boldsymbol{n=2m+1}$. Now the argument (*) from the previous subsection shows $\phi_{L_{m+1}}$ is an irreducible character of L_{m+1}. Again we turn our attention to the stabilizer of $\phi_{L_{m+1}}$.

We can trace the proof of 3.2.1 (changing p^m to p^{m+1} appropriately) to get the stabilizer of $\phi_{L_{m+1}}$:

$$G_{\phi_{L_{m+1}}} = T = \left\{ \begin{bmatrix} a & bp^m \\ cp^m & a^{-1}(1+cbp^{2m}) \end{bmatrix} \middle| \begin{array}{c} a \in (\mathbb{Z}/p^{2m+1}\mathbb{Z})^\times, \\ b, c \in \mathbb{Z}/p^{m+1}\mathbb{Z} \end{array} \right\},$$

although, in this case the size is different: $|T| = p^{2n-1}(p-1)$. As a result inducing up a linear character from T to G (like in the even case) would not give our desired character because T is too big. As a result we must use the following subgroup:

$$N = \left\{ \begin{bmatrix} 1+ap^{m+1} & bp^{m+1} \\ cp^m & 1-ap^{m+1} \end{bmatrix} \middle| \begin{array}{c} a,b \in \mathbb{Z}/p^m\mathbb{Z}, \\ c \in \mathbb{Z}/p^{m+1}\mathbb{Z} \end{array} \right\},$$

and the argument in (*) tells us N affords the irreducible character ϕ_N.

Proposition 3.2.2. *$N \trianglelefteq T$.*

Proof. We shall show: $tNt^{-1} \subseteq N$ for all $t \in T$. Let $t = \begin{bmatrix} a & bp^m \\ cp^m & a^{-1}(1+cbp^{2m}) \end{bmatrix} \in T$ and $n = \begin{bmatrix} 1+xp^{m+1} & yp^{m+1} \\ wp^m & 1-xp^{m+1} \end{bmatrix} \in N$.

$$\begin{aligned} &\Rightarrow tNt^{-1} \\ &= \begin{bmatrix} a & bp^m \\ cp^m & a^{-1}(1+cbp^{2m}) \end{bmatrix} \cdot \begin{bmatrix} 1+xp^{m+1} & yp^{m+1} \\ wp^m & 1-xp^{m+1} \end{bmatrix} \cdot \begin{bmatrix} a^{-1}(1+cbp^{2m}) & -bp^m \\ -cp^m & a \end{bmatrix} \\ &= \begin{bmatrix} 1+(x+a^{-1}bwp^{m-1})p^{m+1} & a^2yp^{m+1} \\ a^{-2}wp^m & 1-(x+a^{-1}bwp^{m-1})p^{m+1} \end{bmatrix} \in N. \end{aligned}$$

□

Now calculate the stabilizer T_{ϕ_N}.

Proposition 3.2.3.

$$T_{\phi_N} = H = \left\{ \begin{bmatrix} a & bp^{m+1} \\ cp^m & a^{-1} \end{bmatrix} \middle| \begin{array}{c} a \in (\mathbb{Z}/p^{2m+1}\mathbb{Z})^\times, \\ b \in \mathbb{Z}/p^m\mathbb{Z}, \\ c \in \mathbb{Z}/p^{m+1}\mathbb{Z} \end{array} \right\}.$$

Proof. We first show: $H \subseteq T_{\phi_N}$. Let

$$h = \begin{bmatrix} a & bp^{m+1} \\ cp^m & a^{-1} \end{bmatrix} \in H, \text{ and } n = \begin{bmatrix} 1+xp^{m+1} & yp^{m+1} \\ wp^m & 1-xp^{m+1} \end{bmatrix} \in N,$$

so we have:

$$\Rightarrow \phi_{_N}^h(n)$$

$$= \phi_{_N}(hnh^{-1})$$

$$= \phi_{_N} \begin{bmatrix} 1+xp^{m+1} & a^2yp^{m+1} \\ a^{-2}wp^m & 1-xp^{m+1} \end{bmatrix}$$

$$= \phi_{_N}(n) \qquad \text{since the matrices are equal in entry (1,1)}$$

$$\therefore H \subseteq T_{\phi_N}.$$

Next we show: $T_{\phi_N} \subsetneq T$. Let: $n = \begin{bmatrix} 1 & 0 \\ p^m & 1 \end{bmatrix} \in N$, and $t = \begin{bmatrix} 1 & p^m \\ 0 & 1 \end{bmatrix} \in T$. Now:

$$\phi_{_N}(tnt^{-1}) = \lambda(1+p^{2m}) \neq \lambda(1) = \phi_{_N}(n)$$

shows $t \notin T_{\phi_N}$ and we have: $T_{\phi_N} \subsetneq T$. Now note:

- $H \subseteq T_{\phi_N}$
- $[H : T] = p$ since $\mid H \mid = p^{2n-1}(p-1), \ \mid T \mid = p^{2n}(p-1)$
- $T_{\phi_N} \subsetneq T$

implies $H = T_{\phi_N}$. □

Again the argument in (*) tells us H affords the irreducible character $\phi_{_H}$. To summarize the results of this subsection we give the lattice of subgroups involved:

$$\begin{array}{rl}
G & \qquad \text{affording } \chi \text{ (below)} \\
\Big| {\scriptstyle p^{2m-1}(p+1)} & \\
G_{\phi_{L_{m+1}}} = T & \qquad \text{affording } \phi_H^T \text{ (below)} \\
\Big| {\scriptstyle p} & \\
T_{\phi_N} = H & \qquad \text{affording } \phi_H \\
\Big| {\scriptstyle p^m(p-1)} & \\
N & \qquad \text{affording } \phi_N \\
\Big| {\scriptstyle p} & \\
L_{m+1} & \qquad \text{affording } \phi_{L_{m+1}} \\
\Big| {\scriptstyle p^{3m}} & \\
< I > &
\end{array}$$

To get an irreducible character of T we use 2.4.15 on the middle of the lattice above:

- $N \lhd T$ — from 3.2.2
- $\phi_N \in Irr(N)$ — ϕ_N a homomorphism with $\phi_N(1) = 1$
- $\phi_H \in Irr(T_{\phi_N})$ — ϕ_H a homomorphism with $\phi_H(1) = 1$
- $\left[\phi_H|_N, \phi_N\right] = [\phi_N, \phi_N] = 1 \neq 0$

$\Longrightarrow$

ϕ_H^T is irreducible.

By Frobenius Reciprocity $1 = \left[\phi_H^T, \phi_H^T\right] = \left[\phi_H, \phi_H^T|_H\right] \neq 0$. Now, $\phi_H \in Irr(H)$, $\phi_H|_{L_{m+1}} = \phi_{L_{m+1}} \in Irr(L_{m+1})$ so we use 2.4.20 implying

$$\left[\phi_H|_{L_{m+1}}, (\phi_H^T|_H)|_{L_{m+1}}\right] = \left[\phi_{L_{m+1}}, \phi_H^T|_{L_{m+1}}\right] \neq 0.$$

Finally we use 2.4.15 to get our irreducible character of G:

- $L_{m+1} \lhd G$ from 3.0.1
- $\phi_{L_{m+1}} \in Irr(L_{m+1})$ from the argument in (*)
- $\phi_H^T \in Irr(T)$ from using 2.4.15 above
- $\left[\phi_{L_{m+1}}, \phi_H^T\big|_{L_{m+1}}\right] \neq 0$

$\Longrightarrow$

$\chi = (\phi_H^T)^G = \phi_H^G$ is irreducible.

In conclusion, we have calculated the character:

$$\chi(g) = \frac{1}{\mid T \mid} \sum_{x \in G} \phi_H^{T\,\circ}(xgx^{-1}),$$

with

$$deg(\chi) = deg(\phi_H^G) = \frac{|G|}{|H|} = \frac{p^{3n-2}(p^2-1)}{p^{2n-1}(p-1)} = (p+1)p^{n-1} \qquad (2.4.9).$$

3.3 An Irreducible Character of Degree $p^{n-1}(p-1)$

In this section we will use results from 2.2 where we defined the subgroup S of G. This subgroup plays a key roll in this chapter. We will use the matrix:

$$B := \begin{pmatrix} 0 & \varepsilon \\ 1 & 0 \end{pmatrix},$$

where ε is a quadratic nonresidue of p to define characters on both L_m and L_{m+1}.

3.3.1 When n is Even.

Again in this subsection we use our ongoing strategy of starting with a character of L_m. This time define the map:

$$\phi : L_m \longrightarrow \mathbb{C}^\times$$
$$\phi : I + p^m A \longmapsto \lambda tr(p^m AB),$$

where given ω a p^{2m}th root of unity and λ is the injective map:

$$\lambda : (\mathbb{Z}/p^{2m}\mathbb{Z})^+ \longrightarrow \mathbb{C}^\times$$
$$\lambda : x \longmapsto \omega^x.$$

We see that ϕ is a homomorphism:

$$\begin{aligned} \phi((I + p^m A)(I + p^m A')) &= \phi(I + p^m(A + A')) \\ &= \lambda tr(p^m(A + A')B) \\ &= \lambda(tr(p^m AB) + tr(p^m A'B)) \\ &= \lambda tr(p^m AB)\lambda tr(p^m A'B) \\ &= \phi(I + p^m A)\phi(I + p^m A'). \end{aligned}$$

Thus, ϕ is a character of degree one of L_m and we calculate its stabilizer (the action is defined in 2.4.14) recalling the subgroup S from 2.2.5.

Proposition 3.3.1.

$$G_\phi = L_m S$$

and

$$|G_\phi| = p^{4m-1}(p+1).$$

Proof. "$\subseteq$" Let $t = \begin{bmatrix} a & b \\ c & d \end{bmatrix} \in G_\phi$:

$$\begin{aligned}
&\Rightarrow \phi^t = \phi \\
&\Rightarrow \phi(t(I + p^m A)t^{-1}) = \phi(I + p^m tAt^{-1}) = \phi(I + p^m A) && \forall A \in M_2(\mathbb{Z}/p^m\mathbb{Z}) \text{ with } A_{11} = -A_{22} \\
&\Rightarrow tr(p^m tAt^{-1}B) = tr(p^m AB) \\
&\Rightarrow tr(p^m At^{-1}Bt) = tr(p^m AB) && \text{property of trace} \\
&\Rightarrow tr(p^m At^{-1}Bt - p^m AB) = 0 \\
&\Rightarrow p^m tr(A(t^{-1}Bt - B)) = 0 && (*)
\end{aligned}$$

Our next step is to show: $p^m t^{-1}Bt = p^m B$.

• Letting $A = \begin{bmatrix} 0 & 1 \\ 0 & 0 \end{bmatrix}$ in (*) gives:

$$p^m \cdot tr \begin{bmatrix} (t^{-1}Bt - B)_{21} & (t^{-1}Bt - B)_{22} \\ 0 & 0 \end{bmatrix} = 0 \Rightarrow p^m (t^{-1}Bt)_{21} = p^m B_{21}.$$

• Letting $A = \begin{bmatrix} 0 & 0 \\ 1 & 0 \end{bmatrix}$ in (*) gives:

$$p^m \cdot tr \begin{bmatrix} 0 & 0 \\ (t^{-1}Bt - B)_{11} & (t^{-1}Bt - B)_{12} \end{bmatrix} = 0 \Rightarrow p^m (t^{-1}Bt)_{12} = p^m B_{12}.$$

• Letting $A = \begin{bmatrix} 1 & 0 \\ 0 & -1 \end{bmatrix}$ in (*) gives:

$$p^m \cdot tr \begin{bmatrix} (t^{-1}Bt - B)_{11} & (t^{-1}Bt - B)_{12} \\ -(t^{-1}Bt - B)_{21} & -(t^{-1}Bt - B)_{22} \end{bmatrix} = 0 \Rightarrow p^m(t^{-1}Bt)_{11} = p^m(t^{-1}Bt)_{22},$$

noting: $B_{11} = B_{22} = 0$. Also,

$$t^{-1}Bt = \begin{bmatrix} d & -b \\ -c & a \end{bmatrix} \begin{bmatrix} 0 & \varepsilon \\ 1 & 0 \end{bmatrix} \begin{bmatrix} a & b \\ c & d \end{bmatrix} = \begin{bmatrix} -ba + dc\varepsilon & -b^2 + d^2\varepsilon \\ a^2 - c^2\varepsilon & ba - dc\varepsilon \end{bmatrix}.$$

So we have: $p^m(t^{-1}Bt)_{11} = -p^m(t^{-1}Bt)_{22}$. Adding this equality with the equality $p^m(t^{-1}Bt)_{11} = p^m(t^{-1}Bt)_{22}$ from above gives: $p^m(t^{-1}Bt)_{11} = p^m(t^{-1}Bt)_{22} = 0$. Therefore $p^m t^{-1}Bt = p^m B$.

Now;

$$p^m Bt = p^m \begin{bmatrix} c\varepsilon & d\varepsilon \\ a & b \end{bmatrix} = p^m \begin{bmatrix} b & a\varepsilon \\ d & c\varepsilon \end{bmatrix} = p^m tB$$

$$\Rightarrow d = a + n_1 p^m \text{ , } b = c\varepsilon + n_2 p^m, \text{ for some integers } n_1, n_2$$

$$\Rightarrow t = \begin{bmatrix} a & c\varepsilon + n_2 p^m \\ c & a + n_1 p^m \end{bmatrix}$$

Let $g = a + n_1 2^{-1} p^m$, $h = c + n_2 2^{-1} \varepsilon^{-1} p^m$ and assign:

$$s = \begin{bmatrix} g & h\varepsilon \\ h & g \end{bmatrix} \Rightarrow |s| = g^2 - h^2\varepsilon = a(a + n_1 p^m) - c(c\varepsilon + n_2 p^m) = ad - bc = 1,$$

so that $s \in S$. To complete the proof of our inclusion we use two cases.

CASE 1. c is a unit. We note that $a^2 - c^2\varepsilon \equiv 1 \mod p^m$ is a unit and assign:

$$x = wac^{-1} + n_2(2c\varepsilon)^{-1}, y = c^{-1}(-n_1 2^{-1} - ax), w = -c^{-1}(a^2 - c^2\varepsilon)^{-1}(n_1 2^{-1} + n_2 a(2\varepsilon c)^{-1}).$$

CASE 2. c is not a unit. This implies that b is also not a unit since $b = c\varepsilon + n_2 p^m$, and this implies a is a unit otherwise we would have $p \mid \det t$. Also, $p \mid c$ and $p \nmid a$ implies $a - c^2\varepsilon a^{-1}$ is a unit, thus we can assign:

$$x = -a^{-1}(n_1 2^{-1} + yc), y = (a - c^2\varepsilon a^{-1})^{-1}(n_2 2^{-1} + n_1 c\varepsilon 2^{-1} a^{-1}), w = a^{-1}(cx - n_2 2^{-1}\varepsilon^{-1}).$$

Now in **each case** we have,

$$\begin{bmatrix} 1+xp^m & yp^m \\ wp^m & 1-xp^m \end{bmatrix} \cdot s = \begin{bmatrix} a & c\varepsilon + n_2 p^m \\ c & a + n_1 p^m \end{bmatrix} = t$$

$$\therefore t \in L_m S$$

(*included in the appendix is some maple code to verify this matrix algebra*)

"$\supseteq$" Let $s \in S$ be arbitrary. The proof of 2.2.4 shows sB=Bs, so we have:

$$\phi^s(I + p^m A) = \lambda tr(p^m s A s^{-1} B) = \lambda tr(p^m A s^{-1} B s) = \lambda tr(p^m AB) = \phi(I + p^m A).$$

Therefore we have $S \subseteq G_\phi$ and $L_m \subseteq G_\phi$ (recalling L_m is abelian) so we have:

$$L_m S \subseteq G_\phi.$$

$$\therefore L_m S = G_\phi.$$

We are left to find $|L_m S|$. Since $L_m \bigcap S = \left\{ \begin{bmatrix} 1 & wp^m\varepsilon \\ wp^m & 1 \end{bmatrix} \middle| w \in \mathbb{Z}/p^m\mathbb{Z} \right\}$, we have:

$$\begin{aligned} |L_m S| &= \frac{|L_m| \cdot |S|}{|L_m \bigcap S|} \\ &= \frac{p^{3m} \cdot (p+1)p^{2m-1}}{p^m} && \text{since } |S| \text{ was given in 2.2.5} \\ &= p^{4m-1}(p+1) \end{aligned}$$

□

To show the existence of a character of G_ϕ we use 2.4.18:

$\bullet\, L_m \lhd G_\phi$	from 3.0.1
$\bullet\, S \leq G_\phi$ is abelian	from 2.2.4
$\bullet\, G_\phi = L_m S$	from 3.3.1
$\bullet\, \phi \in Irr(L_m),\ deg(\phi) = 1$	shown above

$$\Longrightarrow$$

$\exists \phi' \in Irr(G_\phi)$ with $\phi'|_{L_m} = \phi$.

Finally, we note the additional needed ingredient and use 2.4.15:

$\bullet\, \left[\phi'|_{L_m}, \phi\right] = 1 \neq 0$	since $\phi'|_{L_m} = \phi$

$$\Longrightarrow$$

$\chi = \phi'^G$ is irreducible.

In conclusion, this character has degree:

$$deg(\chi) = \frac{\mid G \mid}{\mid G_\phi \mid} = \frac{(p^2-1)p^{6m+1}}{(p+1)p^{4m-1}} = (p-1)p^{n-1} \qquad \text{(by 2.4.9)}.$$

3.3.2 When n is Odd.

Let $n = 2m+1$. In this section we construct a character of L_{m+1} and use 2.4.15. Although building the ingredients to use 2.4.15 is quite involved so we start by outlining the procedure with the following lattice:

$$\begin{array}{cc}
G & \text{affording } \chi = \gamma^G \text{ using 2.4.15} \\
\Big|\,{\scriptstyle p^{2m-1}(p-1)} & \\
G_\phi = L_m S & \text{affording } \delta \text{ an extension of } \gamma \\
\Big|\,{\scriptstyle p+1} & \\
L_m(L_1 \cap S) & \text{affording } \gamma = \beta^{L_m(L_1 \cap S)} \text{ using 2.4.16} \\
\Big|\,{\scriptstyle p} & \\
N(L_1 \cap S) & \text{affording } \beta \text{ an extension of } \alpha \\
\Big|\,{\scriptstyle p} & \\
L_{m+1}(L_1 \cap S) & \text{affording } \alpha \text{ an extension of } \phi \\
\Big|\,{\scriptstyle p^m} & \\
L_{m+1} & \text{affording } \phi \\
\Big|\,{\scriptstyle p^{3m}} & \\
< I > &
\end{array}$$

Where we recall that,

$$L_{m+1} = \left\{ I + p^{m+1}A \;\middle|\; A \in M_2(\mathbb{Z}/p^m\mathbb{Z}),\ A_{11} = -A_{22} \right\},$$

$$L_m = \left\{ I + p^m A \;\middle|\; A \in M_2(\mathbb{Z}/p^{m+1}\mathbb{Z}),\ \det(I + p^m A) = 1 \right\},$$

$$L_1 = \left\{ I + pA \;\middle|\; A \in M_2(\mathbb{Z}/p^{2m}\mathbb{Z}),\ \det(I + pA) = 1 \right\},$$

$$S = \left\{ A \in G \;\middle|\; A_{11} = A_{22}, A_{12} = \varepsilon A_{21} \right\},\ \varepsilon \text{ a quadratic nonresidue of } p,$$

and define:

$$N = \left\{ \begin{bmatrix} 1 + ap^{m+1} & bp^m \\ cp^{m+1} & 1 - ap^{m+1} \end{bmatrix} \;\middle|\; a, c \in \mathbb{Z}/p^m\mathbb{Z}, b \in \mathbb{Z}/p^{m+1}\mathbb{Z} \right\}.$$

Following our lattice above our first step is to construct ϕ a character of L_{m+1}. The method for this step is the same as the method for the even case so we get a homomorphism:

$$\phi : L_{m+1} \longrightarrow \mathbb{C}^{\times}$$
$$\phi : A \longmapsto \lambda tr(AB),$$

where given ω a p^{2m+1}th root of unity λ is the injective homomorphism:

$$\lambda : (\mathbb{Z}/p^{2m+1}\mathbb{Z})^{+} \longrightarrow \mathbb{C}^{\times}$$
$$\lambda : x \longmapsto \omega^{x}.$$

Now, ϕ is a character of L_{m+1} with degree 1. A similar calculation to the one used in 3.3.1 shows: $G_{\phi} = L_m S$.

Our next step is to find α a character of $L_{m+1}(L_1 \cap S)$.

Proposition 3.3.2. *ϕ is extendible to $L_{m+1}(L_1 \cap S)$.*

Proof.

• $L_{m+1} \trianglelefteq L_{m+1}(L_1 \cap S)$	from 3.0.1
• $L_1 \cap S$ is abelian	from 2.2.4
• $L_{m+1}(L_1 \cap S) \subseteq SL_m = G_{\phi}$	from above
$\Longrightarrow$	using 2.4.18
ϕ is extendible to $L_{m+1}(L_1 \cap S)$	

□

Let α **be an extension of** ϕ to $L_{m+1}(L_1 \cap S)$.

Taking a break from constructing characters we find the sizes of our subgroups in the above lattice. We need to find these sizes in order to find the character degree's. A key to the proof of 3.3.4 is the following version of Hensel's lemma.

Proposition 3.3.3. *Given $f(x) \in \mathbb{Z}[x]$ with $f(0) \equiv 0 \mod p$ and $f'(0) \not\equiv 0 \mod p$ then for each $k = 2, 3, \ldots$ there is a unique $x_k \mod p^k$ so $f(x_k) \equiv 0 \mod p^k$.*

Proposition 3.3.4. *$|L_{m+1}| = p^{3m}$, $|L_{m+1}(L_1 \cap S)| = p^{4m}$, $|N(L_1 \cap S)| = p^{4m+1}$, $|L_m(L_1 \cap S)| = p^{4m+2}$, $|L_m S| = p^{4m+2}(p+1)$.*

Proof. $|L_{m+1}| = p^{3m}$, and $|L_m| = p^{3m+3}$ from 3.0.1. Looking at the choices for each entry of a matrix in N we deduce $|N| = p^{3m+1}$. Furthermore:

$$N \cap S = \left\{ \begin{bmatrix} 1 & yp^{m+1}\varepsilon \\ yp^{m+1} & 1 \end{bmatrix} \middle| \, y \in \mathbb{Z}/p^m\mathbb{Z} \right\},$$

so $|N \cap S| = p^m$. To calculate $|L_1 \cap S|$ pick an arbitrary $A \in L_1 \cap S$ and count the solutions to $\det(A) = 1$:

$$|A| = \begin{vmatrix} 1+xp & yp\varepsilon \\ yp & 1+xp \end{vmatrix} = 1 \qquad \text{for some } x, y \in \mathbb{Z}/p^{2m}\mathbb{Z}$$

$$\Leftrightarrow 1 + 2xp + (xp)^2 - (yp)^2\varepsilon = 1$$

$$\Leftrightarrow f(x) = 2x + x^2p - y^2p\varepsilon \equiv 0 \mod p^{2m} \qquad (*)$$

Now, $f(0) \equiv 0 \mod p$ and $f'(0) \not\equiv 0 \mod p$ so by 3.3.3 there is a unique x_{2m} so $f(x_{2m}) \equiv 0 \mod p^{2m}$. This means that for each y in (*) there is exactly one x which gives a solution. Therefore there are p^{2m} choices for x, y in (*) and by the above chain of equivalences there are p^{2m} solutions to $\det(A) = 1$. As a result $|L_1 \cap S| = p^{2m}$. By using the same method we calculate:

$$|L_m \cap S| = p^{m+1}, \quad |L_{m+1} \cap S| = p^m.$$

Now,

$$|L_{m+1}(L_1 \cap S)| = \frac{|L_{m+1}| \cdot |L_1 \cap S|}{|L_{m+1} \cap S|} = \frac{p^{3m} \cdot p^{2m}}{p^m} = p^{4m},$$

$$|N(L_1 \cap S)| = \frac{|N| \cdot |L_1 \cap S|}{|N \cap S|} = \frac{p^{3m+1} \cdot p^{2m}}{p^m} = p^{4m+1},$$

$$|L_m(L_1 \cap S)| = \frac{|L_m| \cdot |L_1 \cap S|}{|L_m \cap S|} = \frac{p^{3m+3} \cdot p^{2m}}{p^{m+1}} = p^{4m+2},$$

and using 2.2.5

$$|L_m S| = \frac{|L_m| \cdot |S|}{|L_m \cap S|} = \frac{p^{3m+3} \cdot (p+1)p^{2m}}{p^{m+1}} = p^{4m+2}(p+1)$$

□

We are now ready to construct an extension to $N(L_1 \cap S)$. First notice since $L_{m+1} \subseteq N$ we have $N(L_1 \cap S) = NL_{m+1}(L_1 \cap S)$, so to construct our extension consider the subgroups N and $L_{m+1}(L_1 \cap S)$ separately and use 2.4.17. Define a character of degree 1 on N:

$$\phi' : N \longrightarrow \mathbb{C}^{\times}$$
$$\phi' : n \longmapsto \lambda tr(nB),$$

which allows us to define the map:

$$\beta : N \cdot L_{m+1}(L_1 \cap S) \longrightarrow \mathbb{C}^{\times}$$
$$\beta : n \cdot l \longmapsto \phi'(n)\alpha(l) \quad (n \in N, l \in L_{m+1}(L_1 \cap S)).$$

Proposition 3.3.5. *β is an extension of α.*

Proof. Since the proof of 3.3.7 shows ϕ' is stable under $L_{m+1}(L_1 \cap S)$ we have two items left to prove in order to use 2.4.17:

(1) $N \trianglelefteq NL_{m+1}(L_1 \cap S)$, and

(2) noting $N \cap L_{m+1}(L_1 \cap S) = L_{m+1}$ (since $L_{m+1} \subseteq N$ and given $x \in N \cap L_{m+1}(L_1 \cap S)$ forces $p^{m+1}|x_{12}$) we need $\phi'_{L_{m+1}} = \alpha_{L_{m+1}}$.

Since $NL_{m+1} = N$ to show (1) our only concern is to show: $(L_1 \cap S)$ is in the normalizer of N. Given $n = I + p^m A \in N$ with $A \in X = \left\{ \begin{bmatrix} pa & b \\ pc & -pa \end{bmatrix} \middle| a, c \in \mathbb{Z}/p^m\mathbb{Z}, b \in \mathbb{Z}/p^{m+1}\mathbb{Z} \right\}$ and $I + psI + ptB \in L_1 \cap S$, we consider the conjugate:

$$
\begin{aligned}
&(I + psI + ptB)n(I + psI + ptB)^{-1} \\
&= (I + psI + ptB)(I + p^m A)(I + ps'I + pt'B) && \text{for some } s', t' \in \mathbb{Z}/p^{2m}\mathbb{Z} \\
&= I + p^m(I + psI + ptB)A(I + ps'I + pt'B) \\
&= M = I + p^m(A + pM') && \text{for some matrix } M' \\
&\Rightarrow M_{11}, M_{12}, M_{21} \text{ have the desired form} && (1 + p^{m+1}*,\ p^m*,\ p^{m+1}*) \\
&\Rightarrow 1 = \det(M) = M_{11} \cdot M_{22} \\
&\Rightarrow M_{22} = M_{11}^{-1} \text{ has the desired form} && 1 - p^{m+1}* \\
&\Rightarrow M \in N \\
&\therefore N \trianglelefteq NL_{m+1}(L_1 \cap S).
\end{aligned}
$$

Finally, for (2): since the image of ϕ' is defined exactly as the image of ϕ it is clear that: $\phi'_{L_{m+1}} = \phi$. Also α is an extension of ϕ so by definition $\alpha_{L_{m+1}} = \phi$. Therefore $\alpha_{L_{m+1}} = \phi = \phi'_{L_{m+1}}$, and the conditions in 2.4.17 are satisfied so β is an extension of α. □

Our next goal is to use 2.4.16 to induce up β to obtain an irreducible character of $L_m(L_1 \cap S)$. The next two propositions give exactly the conditions needed.

Proposition 3.3.6. $N(L_1 \cap S) \trianglelefteq L_m(L_1 \cap S)$

Proof. First show conjugating elements in $L_1 \cap S$ by elements in L_m gives elements in $N(L_1 \cap S)$. Take $I + ps \in L_1 \cap S$, and $I + p^m A \in L_m$ so we have:

$$
\begin{aligned}
&(I + p^m A)(I + ps)(I + p^m A)^{-1} \\
&= I + p(I + p^m A)s(I - p^m A) && \text{since: } p(I + p^m A)^{-1} = p(I - p^m A) \\
&= I + ps + p^{m+1}(As - sA) \\
&= (I + ps)(I + p^{m+1}(I + ps)^{-1}(As - sA)) \\
&\in (L_1 \cap S)N = N(L_1 \cap S).
\end{aligned}
$$

Since $(L_1 \cap S)$ is in the normalizer of N from the previous proof, we are left only to show $N \trianglelefteq L_m$. By tracing the above proof we reduce this problem to proving: for every $A \in X$ and $I + p^m C \in L_m$ we have $(I + p^m C)A(I + p^m C)^{-1} \in X$ (X as above). This is clear since for some matrix M we have:

$$(I + p^m C)A(I + p^m C)^{-1} = (I + p^m C)A(I - p^m C + p^{2m}C^2) = A + pM \in X.$$

□

Proposition 3.3.7. $L_m(L_1 \cap S)_\beta = N(L_1 \cap S)$.

Proof. First show: $N(L_1 \cap S) = L_m(L_1 \cap S)_{\phi'}$. We start by taking $s \in S$, $n \in N$ and considering the conjugate:

$$\begin{aligned}
&\phi'^s(n) \\
&= \lambda tr(sns^{-1}B) \\
&= \lambda tr(snBs^{-1}) && \text{since: } sB = Bs\ \forall s \in S \\
&= \lambda tr(nB) && \text{property of trace} \\
&= \phi'(n) \\
&\Rightarrow S \leq G_{\phi'} \\
&\Rightarrow L_1 \cap S \leq L_m(L_1 \cap S)_{\phi'} && \text{since } L_1 \cap S \leq S \\
&\Rightarrow N(L_1 \cap S) \leq L_m(L_1 \cap S)_{\phi'} && \text{since } \phi' \text{ is defined on } N.
\end{aligned}$$

Thus far we have:

$$N(L_1 \cap S) \leq L_m(L_1 \cap S)_{\phi'} \leq L_m(L_1 \cap S),$$

but $[L_m(L_1 \cap S) : N(L_1 \cap S] = p$. Therefore to force the equality at hand we are left to find one element in $L_m(L_1 \cap S)$ which is not in $L_m(L_1 \cap S)_{\phi'}$. Considering $x = \begin{bmatrix} 1 + p^m & 0 \\ 0 & (1 + p^m)^{-1} \end{bmatrix} \in L_m(L_1 \cap S)$, and $n_1 = \begin{bmatrix} 1 & p^m \\ 0 & 1 \end{bmatrix} \in N$, gives:

$$\phi'^x(n_1) = \lambda(p^m + 2p^{2m}) \neq \lambda(p^m).$$

Therefore: $N(L_1 \cap S) = L_m(L_1 \cap S)_{\phi'}$. Since β is an extension of ϕ' we have: $L_m(L_1 \cap S)_\beta \leq L_m(L_1 \cap S)_{\phi'}$. Also, since β is defined on $N(L_1 \cap S)$ we clearly get $N(L_1 \cap S) \leq L_m(L_1 \cap S)_\beta$. In conclusion:

$$L_m(L_1 \cap S)_\beta \leq L_m(L_1 \cap S)_{\phi'} = N(L_1 \cap S) \leq L_m(L_1 \cap S)_\beta$$

$$\therefore L_m(L_1 \cap S)_\beta = N(L_1 \cap S)$$

□

Now using 2.4.16 with the last two propositions gives: $\gamma = \beta^{L_m(L_1 \cap S)} \in Irr(L_m(L_1 \cap S))$. Next, we would like to get a description of γ, the following two propositions handle this problem.

Note that for each $l \in L_m$ we have $l(L_1 \cap S)l^{-1} \subseteq L_{m+1}(L_1 \cap S)$. This means $L_{m+1}(L_1 \cap S) \trianglelefteq L_m(L_1 \cap S)$, and the next proposition makes sense.

Proposition 3.3.8. *α is stable under $L_m S$.*

Proof. First show α is stable under S, let $s \in S$, $l \in L_{m+1}$ and $s_1 \in L_1 \cap S$ now:

$$\begin{aligned}
&\alpha^s(ls_1) && \\
&= \alpha(sl(s^{-1} \cdot s)s_1 s^{-1}) && \\
&= \alpha(sls^{-1} \cdot s_1) && \text{since } S \text{ is abelian} \\
&= \alpha(sls^{-1}) \cdot \alpha(s_1) && \alpha \text{ is a homomorphism and } sls^{-1} \in L_{m+1} \\
&= \phi(sls^{-1}) \cdot \alpha(s_1) && \alpha \text{ is an extension of } \phi \\
&= \phi(l) \cdot \alpha(s_1) && \text{by the same argument showing } \phi'^s = \phi' \text{ on page 47} \\
&= \alpha(ls_1). &&
\end{aligned}$$

We are left to show α is stable under L_m. Define the subgroups:

$$N_1 = \left\{ \begin{bmatrix} 1 + ap^{m+1} & bp^{m+1} \\ cp^m & 1 - ap^{m+1} \end{bmatrix} \middle| a, b \in \mathbb{Z}/p^m\mathbb{Z}, c \in \mathbb{Z}/p^{m+1}\mathbb{Z} \right\},$$

$$N_2 = \left\{ \begin{bmatrix} 1 + ap^m & bp^{m+1} \\ cp^{m+1} & 1 - ap^m + a^2p^{2m} \end{bmatrix} \middle| b, c \in \mathbb{Z}/p^m\mathbb{Z}, a \in \mathbb{Z}/p^{m+1}\mathbb{Z} \right\}.$$

Also these subgroups afford characters:

$$\phi_1 : N_1 \longrightarrow \mathbb{C}^\times \qquad\qquad \phi_2 : N_2 \longrightarrow \mathbb{C}^\times$$

$$\phi_1 : x \longmapsto \lambda tr(xB), \qquad\qquad \phi_2 : x \longmapsto \lambda tr(xB)$$

Now we can trace the proof of 3.3.5 replacing N with N_1, N_2 accordingly, this shows α can be extended to both $N_1(L_1 \cap S)$ and $N_2(L_1 \cap S)$. This means α is stable under each of N, N_1, and N_2. Noting: $N, N_1, N_2 \subseteq L_m$, $N_1 \nsubseteq N$, $N_2 \nsubseteq NN_1$, $|N| = p^{3m+1}$, $|NN_1| = p^{3m+2}$, and $|L_m| = p^{3m+3}$, gives: $N \cdot N_1 \cdot N_2 = L_m$. Therefore α is stable under L_m.

□

Proposition 3.3.9. $\gamma_{L_{m+1}(L_1 \cap S)} = p \cdot \alpha$.

Proof. Let $g \in L_{m+1}(L_1 \cap S)$:

$$\begin{aligned}
\gamma(g) &= \frac{1}{|N(L_1 \cap S)|} \sum_{x \in L_m(L_1 \cap S)} \beta^\circ(xgx^{-1}) && 2.4.9 \\
&= \frac{1}{p^{4m+1}} \sum_{x \in L_m(L_1 \cap S)} \beta(xgx^{-1}) && \text{since } xgx^{-1} \in L_{m+1}(L_1 \cap S) \\
&= \frac{1}{p^{4m+1}} \sum_{x \in L_m(L_1 \cap S)} \alpha(xgx^{-1}) && \beta \text{ an extension of } \alpha \\
&= \frac{1}{p^{4m+1}} \sum_{x \in L_m(L_1 \cap S)} \alpha(g) && 3.3.8 \text{ above} \\
&= \frac{|L_m(L_1 \cap S)|}{p^{4m+1}} \alpha(g) \\
&= \frac{p^{4m+2}}{p^{4m+1}} \alpha(g) \\
&= p \cdot \alpha(g)
\end{aligned}$$

□

Lemma 3.3.10. $L_m(L_1 \cap S) \trianglelefteq L_m S$

Proof. Noting $L_1 \cap S \trianglelefteq S$ since S is abelian, $L_m \trianglelefteq G$ and $l(L_1 \cap S)l^{-1} \subseteq L_m(L_1 \cap S)$ for $l \in L_m$ gives: $L_m(L_1 \cap S) \trianglelefteq L_m S$. □

Proposition 3.3.11. *$L_m \cdot S \diagup L_m(L_1 \cap S)$ is cyclic*

Proof.

$L_m \cdot S \diagup L_m(L_1 \cap S)$

$= L_m(L_1 \cap S) \cdot S \diagup L_m(L_1 \cap S)$ $\quad$ $L_1 \cap S \subseteq S$

$\simeq S \diagup L_m(L_1 \cap S) \cap S$ $\quad$ by the diamond isomorphism theorem

$= S \diagup L_1 \cap S$ $\quad$ $L_m \subseteq L_1$

$\simeq S' = \left\{ \begin{bmatrix} x & y\varepsilon \\ y & x \end{bmatrix} \middle| x, y \in \mathbb{Z}/p\mathbb{Z} \right\}$ $\quad$ by 1st iso. theorem with: $A \mapsto (A_{i,j} \mod p)_{1 \le i,j \le 2}$

$\simeq \tau(S')$ $\quad$ where $\tau : S' \to \left(\mathbb{Z}/p\mathbb{Z}[\sqrt{\varepsilon}]\right)^{\times}$ is the natural map

$\le \left(\mathbb{Z}/p\mathbb{Z}[\sqrt{\varepsilon}]\right)^{\times}$ is cyclic

□

We are now ready to construct δ using 2.4.19:

- $L_m(L_1 \cap S) \trianglelefteq L_m S$ $\quad$ 3.3.10
- $L_m \cdot S \diagup L_m(L_1 \cap S)$ is cyclic $\quad$ 3.3.11
- $\gamma \in Irr(L_m(L_1 \cap S))$ stable under $L_m S$ $\quad$ 3.3.9, 3.3.8, and 2.4.22

$\Longrightarrow$

γ can be extended to a character δ of $L_m S$.

So we have ϕ a character of the normal subgroup L_{m+1}, with $G_\phi = L_m S$ affording δ. There is one more needed ingredient to prove in order to use 2.4.15:

- $\left[\delta|_{L_{m+1}}, \phi\right]$

$= \left[\gamma|_{L_{m+1}}, \phi\right]$ since δ is an extension of γ

$= \left[p\alpha|_{L_{m+1}}, \phi\right]$ 3.3.9

$= [p\phi, \phi] \neq 0$ since α is an extension of ϕ

$\Longrightarrow$

$\chi = \delta^G$ is irreducible.

In conclusion this character has degree:

$$deg(\chi) = deg(\delta)\frac{\mid G \mid}{\mid G_\phi \mid} = p\frac{(p^2-1)p^{6m+1}}{(p+1)p^{4m+2}} = (p-1)p^{n-1} \qquad (\text{ by } 2.4.9).$$

3.4 Conclusion about Character Degrees

Theorem 3.4.1. *G affords irreducible characters of the following degrees:*

$$1,\ p-1,\ p,\ p+1,\ \frac{p-1}{2},\ \frac{p+1}{2},\ p^{m-1}(p+1),\ \frac{p^{m-2}(p^2-1)}{2},\ p^{m-1}(p-1),\ \text{for } 2 \leq m \leq n.$$

Proof. Consider the group homomorphism:

$$f : SL_2(\mathbb{Z}/p^n\mathbb{Z}) \longrightarrow SL_2(\mathbb{Z}/p^{n-1}\mathbb{Z})$$
$$f : A \longmapsto (A_{ij} \mod p^{n-1})_{1\leq i,j\leq 2}.$$

By the first isomorphism theorem we have $SL_2(\mathbb{Z}/p^n\mathbb{Z})\big/Ker(f) \simeq SL_2(\mathbb{Z}/p^{n-1}\mathbb{Z})$, so we can use 2.4.21 to lift every irreducible character of $SL_2(\mathbb{Z}/p^m\mathbb{Z})$ for $1 \leq m \leq n-1$ to G. Noting: for $n = 1$ there are characters of G with degrees $1,\ p-1,\ p,\ p+1,\ \frac{p-1}{2},\ \frac{p+1}{2}$ ([9],p.71-73) and in this chapter we found for $n = 2, 3, 4, \ldots$ there are characters of G with degrees $p^{n-1}(p+1),\ \frac{p^{n-2}(p^2-1)}{2},\ p^{n-1}(p-1)$ our result is shown. □

Over the next two sections we find all the irreducible characters of G which gives the following theorem.

Theorem 3.4.2. *The character degrees stated in 3.4.1 are all the character degrees appearing in the character table of G.*

3.5 Counting Characters

3.5.1 Conjugacy Classes

Letting ε be a quadratic nonresidue of p the conjugacy classes of G are summarized in this table:

Table 1: Conjugacy Classes of $SL_2(\mathbb{Z}/p^n\mathbb{Z})$

Name	Parameters	Representative	Number of Classes		Size of Class
I_α	$\alpha \in \{\pm 1\}$	$\begin{pmatrix} \alpha & 0 \\ 0 & \alpha \end{pmatrix}$	2		1
$B_{i\alpha\beta}$	$0 \leq i < n$ $\beta \in \mathbb{Z}/p^{n-i-1}\mathbb{Z}$ $\alpha^2 = 1 + p^{2i+1}\beta$	$\begin{pmatrix} \alpha & p^{i+1}\beta \\ p^i & \alpha \end{pmatrix}$	$\sum_{i=0}^{n-1} 2p^{n-i-1}$		$\frac{p^{2n-2i-2}(p^2-1)}{2}$
$B'_{i\alpha\beta}$	$0 \leq i < n$ $\beta \in \mathbb{Z}/p^{n-i-1}\mathbb{Z}$ $\alpha^2 = 1 + p^{2i+1}\beta$	$\begin{pmatrix} \alpha & p^{i+1}\beta\varepsilon^{-1} \\ p^i\varepsilon & \alpha \end{pmatrix}$	$\sum_{i=0}^{n-1} 2p^{n-i-1}$		$\frac{p^{2n-2i-2}(p^2-1)}{2}$
-	-	-	$i = 0$	$0 < i < n$	-
$C_{i\alpha\beta}$	$0 \leq i < n$ $\beta \in (\mathbb{Z}/p^{n-i}\mathbb{Z})^\times / \{\pm 1\}$ $\alpha^2 = 1 + p^{2i}\varepsilon\beta^2$	$\begin{pmatrix} \alpha & p^i\varepsilon\beta \\ p^i\beta & \alpha \end{pmatrix}$	$\frac{p^{n-1}(p-1)}{2}$	$p^{n-i-1}(p-1)$	$p^{2n-2i-1}(p-1)$
$D_{i\alpha}$	$0 \leq i < n$ $\alpha \in (\mathbb{Z}/p^n\mathbb{Z})^\times$ $\alpha \equiv \pm 1 \mod p^i$ $\alpha \not\equiv \pm 1 \mod p^{i+1}$	$\begin{pmatrix} \alpha & 0 \\ 0 & \alpha^{-1} \end{pmatrix}$	$\frac{p^{n-1}(p-3)}{2}$	$p^{n-i-1}(p-1)$	$p^{2n-2i-1}(p+1)$

Note: The element $\beta \in (\mathbb{Z}/p^{n-i}\mathbb{Z})^\times / \{\pm 1\}$ is regarded as an element in $(\mathbb{Z}/p^{n-i}\mathbb{Z})^\times$ by considering a one to one correspondence from a unique choice of the coset representatives of $(\mathbb{Z}/p^{n-i}\mathbb{Z})^\times / \{\pm 1\}$ to a subset of $(\mathbb{Z}/p^{n-i}\mathbb{Z})^\times$.

Proof. We start by referencing ([2],p.3) where all the conjugacy class types of $G' = GL_2(\mathbb{Z}/p^n\mathbb{Z})$ are given: I_α, $B_{i\alpha\beta}$, $C_{i\alpha\beta}$, and $D_{i\alpha\delta}$. Then restrict the parameters on these four class types to give only classes in G. These (restricted) classes form a disjoint union of G since G is a normal subgroup of G'. By calculating the centralizers in G of each representative of each class we discover the classes given by I_α, $C_{i\alpha\beta}$, and $D_{i\alpha\delta}$ remain the same size in G but the classes given by $B_{i\alpha\beta}$ split up in G. We now show for each choice of i, α, β each class $\begin{bmatrix} \alpha & p^{i+1}\beta \\ p^i & \alpha \end{bmatrix}^{G'}$ splits up into 2 classes in G: one class in G is represented by $B_{i\alpha\beta} = \begin{bmatrix} \alpha & p^{i+1}\beta \\ p^i & \alpha \end{bmatrix}$ and the other class is represented by $B^{'}_{i\alpha\beta} = \begin{bmatrix} \alpha & p^{i+1}\beta\varepsilon^{-1} \\ p^i\varepsilon & \alpha \end{bmatrix}$. Since we can pick $A = \begin{bmatrix} 1 & 0 \\ 0 & \varepsilon \end{bmatrix} \in G'$, so that:

$$AB_{i\alpha\beta}A^{-1} = B^{'}_{i\alpha\beta},$$

we know $B^{'}_{i\alpha\beta} \in B^{G'}_{i\alpha\beta}$. Our next step is to show: $B^{'}_{i\alpha\beta} \notin B^{G}_{i\alpha\beta}$. Let $X = \begin{bmatrix} x & y \\ w & z \end{bmatrix} \in G$ and look for a contradiction from the equality:

$$\begin{aligned}
& B^{'}_{i\alpha\beta} \cdot X = X \cdot B_{i\alpha\beta} && \\
& \Rightarrow p^i\varepsilon y = p^{i+1}w\beta \quad (1) && \\
& \quad\ \& \ \ p^i\varepsilon x = p^i z \quad (2) && \\
& \overset{(1)}{\Rightarrow} p|y && \\
& \Rightarrow p \nmid x, z && \text{since } p \nmid 1 = xz - yw \\
& \overset{(2)}{\Rightarrow} x\varepsilon + rp^{n-i} = z && \text{for some integer } r \\
& \Rightarrow -\left(\frac{x}{p}\right) = \left(\frac{x\varepsilon}{p}\right) = \left(\frac{x\varepsilon + rp^{n-i}}{p}\right) = \left(\frac{z}{p}\right) && \text{using 2.2.3} \\
& \Rightarrow -1 = \left(\frac{x}{p}\right) \cdot \left(\frac{z}{p}\right) = \left(\frac{xz}{p}\right) = \left(\frac{1+yw}{p}\right) \overset{p|y}{=} \left(\frac{1}{p}\right) = 1 && \text{a contradiction.}
\end{aligned}$$

Finally we calculate the size of the centralizers of $B_{i\alpha\beta}$ and $B^{'}_{i\alpha\beta}$ in G as $2 \cdot p^{n+2i}$ showing $|{B_{i\alpha\beta}}^G| = |B^{'G}_{i\alpha\beta}| = \frac{p^{2n-2i-2}(p^2-1)}{2}$. Therefore the class $B^{G'}_{i\alpha\beta}$ splits into exactly two classes in G and we have found all the conjugacy classes in G. □

By adding up the number of conjugacy classes of G we obtain:

Corollary 3.5.1. *G affords exactly:*

$$\frac{(p^{n+1}-1) + 3(p^n - 1)}{p-1}$$

irreducible characters.

3.5.2 The Number of Irreducible Characters For Each Degree

In this section we count the number of distinct irreducible characters for each degree. Our method to construct irreducible characters of G is the same as in the first three sections of the chapter, but in this section we generalize to find more characters. When $n = 2m$ we define a character on L_m, for an injective homomorphism $\lambda : (\mathbb{Z}/p^n\mathbb{Z})^+ \to \mathbb{C}^\times$, and for **any** 2 by 2 matrix B:

$$\phi_B : L_m \longrightarrow \mathbb{C}^\times$$
$$\phi_B : I + p^m A \longmapsto \lambda \circ tr(p^m BA).$$

When $n = 2m + 1$ we use the same notation and define:

$$\phi_B : L_{m+1} \longrightarrow \mathbb{C}^\times$$
$$\phi_B : I + p^{m+1} A \longmapsto \lambda \circ tr(p^{m+1} BA).$$

Regardless of the choice of B, ϕ_B is a group homomorphism and therefore a character of L_m and L_{m+1}. We now list some lemmas which will be used to find *distinct* characters of G.

Lemma 3.5.2. *Letting $N \trianglelefteq G$, $\phi_1, \phi_2 \in Irr(N)$ be non-conjugate, and $\psi_1 \in Irr(G_{\phi_1})$, $\psi_2 \in Irr(G_{\phi_2})$ with $[\psi_{1N}, \phi_1] \neq 0 \neq [\psi_{2N}, \phi_2]$, gives $\chi_1 = \psi_1^G$, $\chi_2 = \psi_2^G \in Irr(G)$ (by 2.4.15 part a) furthermore χ_1 and χ_2 are **distinct**.*

Proof. We show that χ_{1_N} is not equal to χ_{2_N}. By Frobenius Reciprocity $1 = [\chi_1, \chi_1] = [\psi_1, \chi_{1_{G_{\phi_1}}}]$ so $[\phi_1, \chi_{1_N}] \neq 0$ and ϕ_1 is a constituent of χ_{1_N}. Therefore by Clifford's theorem χ_{1_N} is a *direct* sum of conjugates of ϕ_1. By the same reasoning χ_{2_N} is a *direct* sum of conjugates of ϕ_2. Therefore, since ϕ_1 and ϕ_2 are non-conjugate χ_1 and χ_2 are distinct. □

Lemma 3.5.3. *Letting $N \trianglelefteq G$, $\phi \in Irr(N)$ with distinct $\psi_1, \psi_2 \in Irr(T)$ with $[\psi_{1N}, \phi] \neq 0 \neq [\psi_{2N}, \phi]$ gives $\chi_1 = \psi_1^G, \chi_2 = \psi_2^G \in Irr(G)$ (by 2.4.15 part a) furthermore χ_1 and χ_2 are **distinct**.*

Proof. We use 2.4.15 part c). □

Now given non-conjugate choices for ϕ_B or distinct characters of G_{ϕ_B} we have tools when using 2.4.15 to count distinct characters of G. We make use of these tools in the proof below.

Letting $R_i = \mathbb{Z}/p^i\mathbb{Z}$, $S \leq G$ so that $T = G_{\phi_B} = L_m S$ ($n = 2m$ or $n = 2m+1$) we summarize the non-conjugate choices for ϕ_B and the number of resulting irreducible characters χ for each case in the following table:

Table 2: Number of Irreducible Characters of Each Type

B	Parameters	S	Degree(χ)	# of χ
$\begin{pmatrix} 0 & p\beta \\ \delta & 0 \end{pmatrix}$	$\beta \in R_{m-1}$ $\delta \in \{1, \varepsilon\}$ ε is a fixed non-square unit	$\left\{\begin{bmatrix} x & p\frac{\beta}{\delta}y \\ y & x \end{bmatrix} \in G\right\}$	$\frac{p^{n-2}(p^2-1)}{2}$	$4p^{n-1}$
$\begin{pmatrix} \alpha & 0 \\ 0 & 0 \end{pmatrix}$	$\alpha \in R_m^{\times}/\{\pm 1\}$	$\left\{\begin{bmatrix} x & 0 \\ 0 & x^{-1} \end{bmatrix}\right\}$	$p^{n-1}(p+1)$	$\frac{p^{n-2}(p-1)^2}{2}$
$\begin{pmatrix} 0 & \varepsilon \\ 1 & 0 \end{pmatrix}$	ε is any non-square unit in R_m	$\left\{\begin{bmatrix} x & y\varepsilon \\ y & x \end{bmatrix} \in G\right\}$	$p^{n-1}(p-1)$	$\frac{p^{n-2}(p^2-1)}{2}$

Note: The element $\alpha \in R_m^{\times}/\{\pm 1\}$ is regarded as an element in $R_m^{\times}$ by considering a one to one correspondence from a unique choice of the coset representatives of $R_m^{\times}/\{\pm 1\}$ to a subset of $R_m^{\times}$.

Proof. We start by noting: S is abelian and $G_{\phi_B} = L_m S$ in each case. So when n is even 2.4.18 guarantees the existence of an extension of ϕ_B to G_{ϕ_B}. Therefore we can always use 2.4.15 (directly) to find χ in the even case.

<u>**Case 1:**</u> **Irreducible characters of degree** $\frac{p^{n-2}(p^2-1)}{2}$. When ***n=2m*** our table notes $2p^{m-1}$ choices of B giving ϕ_B non conjugate so 3.5.2 gives $2p^{m-1}$ distinct irreducible characters of G. Using Gallagher's theorem with the fact T/L_m is abelian we count distinct extensions of ϕ_B to T as $|T/L_m| = \frac{2 \cdot p^{4m}}{p^{3m}} = 2p^m$. Now for each choice of B, by 3.5.3, there are $2p^m$ distinct irreducible characters of G. Therefore there are at least

$$2p^{m-1} \cdot 2p^m = 4 \cdot p^{n-1}$$

distinct irreducible characters of degree $\frac{p^{n-2}(p^2-1)}{2}$ when n is even.

When ***n=2m+1*** we follow a similar process to the one used in 3.2.2 on page 35:

$$\begin{tikzcd}
G \arrow[d, dash, "\frac{p^{2m-2}(p^2-1)}{2}"] & \text{affording } \chi = \alpha^G \text{ using 2.4.15} \\
T = G_{\phi_B} = L_m S \arrow[d, dash, "p"] & \text{affording } \alpha^T \text{ using 2.4.15} \\
T_{\phi'_B} = NS \arrow[d, dash, "2 \cdot p^m"] & \text{affording } \alpha \text{ an extension of } \phi'_B \text{ which } \exists \text{ by 2.4.18} \\
N \arrow[d, dash, "p^2"] & \text{affording } \phi'_B \text{ an extension of } \phi_B \text{ defined below} \\
L_{m+1} \arrow[d, dash, "p^{3m}"] & \text{affording } \phi_B \\
< I > &
\end{tikzcd}$$

Where,

$$N = \left\{ \begin{bmatrix} 1+ap^m & bp^{m+1} \\ cp^m & (1+ap^m)^{-1} \end{bmatrix} \right\}, \text{ and}$$

$$\phi'_B : N \longrightarrow \mathbb{C}^\times$$

$$\phi'_B : n \longmapsto \lambda \circ tr(B(n-I))$$

which has $T_{\phi'_B} = NS$.

To count the distinct irreducible characters of G we start by only looking at the middle of the above lattice:

$$\begin{tikzcd}
T \arrow[d, dash, "p"] & \text{affording } \alpha^T \\
T_{\phi'_B} \arrow[d, dash, "2 \cdot p^m"] & \text{affording } \alpha \\
N & \text{affording } \phi'_B
\end{tikzcd}$$

Now we consider $\beta \in \mathbb{Z}/p^m\mathbb{Z}$ and $\delta \in \{1, \varepsilon\}$ which gives $2p^m$ choices of B giving non-conjugate choices for ϕ'_B in T. Therefore 3.5.2 gives $2p^m$ distinct irreducible characters each afforded by some choice of T (note T depends on B) using the construction outlined in the above lattice. Now, for each choice of B we want to find distinct constructions of α^T in the above lattice. Using Gallagher's theorem with the fact NS/N is abelian we count distinct extensions of ϕ'_B to $T_{\phi'_B} = NS$ as $|NS/N| = \frac{|NS|}{|N|} = \frac{2 \cdot p^{4m+2}}{p^{3m+2}} = 2p^m$. So, 3.5.3 gives $2p^m$ distinct choices for α^T. Therefore there are at least

$$2p^m \cdot 2p^m = 4 \cdot p^{n-1}$$

distinct irreducible characters each afforded by some choice of T and can be induced up to give an irreducible character of G. We want to show that each of the $4 \cdot p^{n-1}$ characters induced up to G are indeed distinct, suppose χ_1 and χ_2 are two choices from this list. Further suppose χ_1 was constructed using $\phi_{B_1} \in Irr(L_{m+1})$ and χ_1 was constructed using $\phi_{B_2} \in Irr(L_{m+1})$. Then either ϕ_{B_1} is non-conjugate to ϕ_{B_2} or $\phi_{B_1} = \phi_{B_2}$. In the former case χ_1 and χ_2 are distinct by 3.5.2 and in the latter case χ_1 and χ_2 were both induced from the same choice of T and as a result are distinct by 3.5.3. Therefore G affords at least

$$4 \cdot p^{n-1}$$

distinct irreducible of degree $\frac{p^{n-2}(p^2-1)}{2}$ when n is odd.

<u>**Case 2:**</u> **Irreducible characters of degree** $p^{n-1}(p+1)$. When ***n=2m*** our table notes $\frac{p^{m-1}(p-1)}{2}$ choices of B giving ϕ_B non conjugate. Using Gallagher's theorem with the fact T/L_m is abelian, we count distinct extensions of ϕ_B to T as $|T/L_m| = \frac{p^{4m-1}(p-1)}{p^{3m}} = p^{m-1}(p-1)$. Therefore, using 3.5.2 and 3.5.3, G affords at least

$$\frac{p^{m-1}(p-1)}{2} \cdot p^{m-1}(p-1) = \frac{p^{n-2}(p-1)^2}{2}$$

distinct irreducible characters of degree $p^{n-1}(p+1)$ when n is even.

When ***n=2m+1*** we follow a similar process to the one used in 3.2.2 on page 35:

$$
\begin{array}{cl}
G & \text{affording } \chi = \alpha^G \text{ using 2.4.15} \\
\Big| \, p^{2m-1}(p+1) & \\
T = G_{\phi_B} = L_m S & \text{affording } \alpha^T \text{ using 2.4.15} \\
\Big| \, p & \\
T_{\phi'_B} = NS & \text{affording } \alpha \text{ an extension of } \phi'_B \text{ which } \exists \text{ by 2.4.18} \\
\Big| \, p^m(p-1) & \\
N & \text{affording } \phi'_B \text{ an extension of } \phi_B \text{ defined below} \\
\Big| \, p & \\
L_{m+1} & \text{affording } \phi_B \\
\Big| \, p^{3m} & \\
< I > &
\end{array}
$$

Where,

$$N = \left\{ \begin{bmatrix} 1 + ap^{m+1} & bp^{m+1} \\ cp^m & (1 + ap^{m+1})^{-1} \end{bmatrix} \right\}, \text{ and}$$

$$\phi'_B : N \longrightarrow \mathbb{C}^\times$$

$$\phi'_B : n \longmapsto \lambda \circ tr(B(n - I))$$

which has $T_{\phi'_B} = NS$. Our table notes $\frac{p^{m-1}(p-1)}{2}$ choices of B giving ϕ_B non conjugate so 3.5.2 gives $\frac{p^{m-1}(p-1)}{2}$ distinct irreducible characters of G using the construction outlined by the above lattice. Now, for each choice of B we want to find distinct constructions of χ in the above lattice. Using Gallagher's theorem with the fact NS/N is abelian we count distinct extensions of ϕ'_B to NS as $|NS/N| = \frac{|NS|}{|N|} = \frac{p^{4m+1}(p-1)}{p^{3m+1}} = p^m(p-1)$. So 3.5.3 gives $p^m(p-1)$ distinct choices for α^T and using 3.5.3 again gives $p^m(p-1)$ distinct choices for α^G. Therefore G affords at least

$$\frac{p^{m-1}(p-1)}{2} \cdot p^m(p-1) = \frac{p^{n-2}(p-1)^2}{2}$$

distinct irreducible characters of degree $p^{n-1}(p+1)$ when n is odd.

Case 3: Irreducible characters of degree $p^{n-1}(p-1)$. This case is similar to the previous cases when n is even, but different from the previous cases when n is odd.

When ***n=2m*** our table notes $\frac{p^{m-1}(p-1)}{2}$ choices of B giving ϕ_B non conjugate. Using Gallagher's theorem we count distinct extensions of ϕ_B to $T = G_{\phi_B}$ as $|T/L_m| = \frac{p^{4m-1}(p+1)}{p^{3m}} = p^{m-1}(p+1)$. Therefore using 3.5.2 and 3.5.3 there are at least

$$\frac{p^{m-1}(p-1)}{2} \cdot p^{m-1}(p+1) = \frac{p^{n-2}(p^2-1)}{2}$$

distinct irreducible characters of degree $p^{n-1}(p+1)$ when n is even.

When ***n=2m+1*** we repeat the method from 3.3.2, for quick reference we recall the lattice outlining the construction:

$$\begin{array}{ccl}
G & & \text{affording } \chi = \gamma^G \text{ using 2.4.15} \\
\Big| & p^{2m-1}(p-1) & \\
G_\phi = L_m S & & \text{affording } \delta \text{ an extension of } \gamma \\
\Big| & p+1 & \\
L_m(L_1 \cap S) & & \text{affording } \gamma = \beta^{L_m(L_1 \cap S)} \text{ using 2.4.16} \\
\Big| & p & \\
N(L_1 \cap S) & & \text{affording } \beta \text{ an extension of } \alpha \\
\Big| & p & \\
L_{m+1}(L_1 \cap S) & & \text{affording } \alpha \text{ an extension of } \phi \\
\Big| & p^m & \\
L_{m+1} & & \text{affording } \phi = \phi_B \\
\Big| & p^{3m} & \\
< I > & &
\end{array}$$

Our table notes $\frac{p^{m-1}(p-1)}{2}$ choices of B giving ϕ_B non conjugate, so 3.5.2 gives $\frac{p^{m-1}(p-1)}{2}$ distinct irreducible characters of G using the construction in the above lattice. Now for each choice of B we want to find distinct constructions of χ in the above lattice. We start by counting distinct extensions of ϕ_B to $L_{m+1}(L_1 \cap S)$. Using Gallagher's theorem with the fact $L_{m+1}(L_1 \cap S)/L_{m+1}$ is abelian we count distinct extensions of ϕ_B to $L_{m+1}(L_1 \cap S)$ as $\frac{|L_{m+1}(L_1 \cap S)|}{|L_{m+1}|} = \frac{p^{4m}}{p^{3m}} = p^m$. So we have p^m distinct choices for α, each of which can be extended to $N(L_1 \cap S)$ giving p^m distinct choices for β. The p^m choices for β give p^m choices for γ which are distinct by 3.3.9 which says $\gamma_{L_{m+1}(L_1 \cap S)} = p \cdot \alpha$.

Now for each choice of γ we use Gallagher's theorem with the fact that $L_mS/L_m(L_1 \cap S)$ is abelian to count distinct extensions of γ to L_mS as $\frac{|L_mS|}{|L_m(L_1 \cap S)|} = p+1$. So for each distinct choice of γ there are $p+1$ distinct choices for δ. Finally we use 3.5.3 to get $p^m \cdot (p+1)$ distinct choices for χ. Therefore there are at least

$$\frac{p^{m-1}(p-1)}{2} \cdot p^m \cdot (p+1) = \frac{p^{n-2}(p^2-1)}{2}$$

distinct irreducible characters of degree $\frac{p^{n-2}(p^2-1)}{2}$ when n is odd. $\square$

Theorem 3.5.4. *The above table represents all the irreducible characters of G.*

Proof. To show this we count the number of distinct irreducible characters of G we have found and ensure that this equals the number given in 3.5.1. When $n = 1$ there are $p+4$ irreducible characters of $SL_2(\mathbb{Z}/p^n\mathbb{Z})$ having degrees less than or equal to $p+1$ ([9],p.71-73). For each $2 \leq m \leq n$ there are irreducible characters of $SL_2(\mathbb{Z}/p^m\mathbb{Z})$ as described in the above table. All of these irreducible characters just listed can be lifted to G using the technique from the proof of 3.4.1. For $p > 3$ we only need to look at the degrees to see that all of these lifted characters are distinct:

$$p^{(\mathbf{m\text{-}1})-1}(p+1) < \frac{p^{\mathbf{m}-2}(p^2-1)}{2} < p^{\mathbf{m}-1}(p-1) < p^{\mathbf{m}-1}(p+1).$$

When $p = 3$ there is an issue since the first strict inequality above fails. Though in this case the lifted characters remain distinct, to see this we look at the kernels of the lifted characters. The characters given in row 2 of the above table lifted to $SL_2(\mathbb{Z}/p^m\mathbb{Z})$ (of degree $3^{(\mathbf{m\text{-}1})-1}(3+1)) = 4 \cdot 3^{m-2}$) have L_{m-1} in their kernels *but* the characters of $SL_2(\mathbb{Z}/p^m\mathbb{Z})$ given in row 1 of the above table (of degree $\frac{p^{\mathbf{m}-2}(p^2-1)}{2} = 4 \cdot 3^{m-2}$) **do not** have L_{m-1} in their kernels. We now add up the distinct irreducible characters:

$$
\begin{aligned}
&p+4+\sum_{i=2}^{n}\frac{p^{i-2}(p-1)^2}{2}+\frac{p^{i-2}(p^2-1)}{2}+4p^{i-1}\\
&=p+4+\frac{p^{n-1}-1}{p-1}\cdot\frac{(p-1)^2}{2}+\frac{p^{n-1}-1}{p-1}\cdot\frac{(p^2-1)}{2}+4p\frac{p^{n-1}-1}{p-1}\\
&=\frac{(p-1)(p+4)}{p-1}+\frac{p^{n-1}-1}{p-1}\left(\frac{(p-1)^2+(p^2-1)}{2}+4p\right)\\
&=\frac{p^2+3p-4}{p-1}+\frac{p^{n-1}-1}{p-1}\left(p^2+3p\right)\\
&=\frac{1}{p-1}\left(p^2+3p-4+p^{n+1}-p^2+3p^n-3p\right)\\
&=\frac{p^{n+1}-4+3p^n}{p-1}\\
&=\frac{(p^{n+1}-1)+3(p^n-1)}{p-1}
\end{aligned}
$$

which is exactly the total number of irreducible characters of G. Therefore we have indeed accounted for every irreducible character of G. $\square$

Chapter 4

Irreducible Character Degrees of $SL_3(\mathbb{Z}/p^n\mathbb{Z})$

4.0 Introduction

In this chapter we let,

$$G = SL_3(\mathbb{Z}/p^n\mathbb{Z})$$
$$G' = GL_3(\mathbb{Z}/p^n\mathbb{Z})$$

and find characters of G using 2.4.15. Our first step is to find a normal subgroup of G, so throughout this chapter for an integer m, we let:

$$L_m = \left\{ I + p^m A \;\middle|\; A \in M_3(\mathbb{Z}/p^{n-m}\mathbb{Z}),\ \det(I + p^m A) = 1 \right\}$$
$$K_m = \left\{ I + p^m A \;\middle|\; A \in M_3(\mathbb{Z}/p^{n-m}\mathbb{Z}) \right\}.$$

K_m was explored in ([1]) and we make use of its similarity to L_m in this chapter (here we are using the corresponding convention described in 3.0.2). The same method used in chapter 3 gives the following proposition.

Proposition 4.0.1. *L_m is a normal subgroup of G with $|L_m| = p^{8(n-m)}$. When $\lceil \frac{n}{2} \rceil \leq m$ we have L_m abelian and*

$$L_m = \left\{ I + p^m A \;\middle|\; A \in M_3(\mathbb{Z}/p^{n-m}\mathbb{Z}),\ Tr(A) = 0 \right\}.$$

4.1 An Irreducible Character of Degree $p^{2n-4}(p^3-1)(p+1)$.

We start by defining the map:

$$\phi : M_3(\mathbb{Z}/p^n\mathbb{Z}) \longrightarrow \mathbb{C}^\times$$
$$\phi : A \longmapsto \lambda(A_{11}^{-1} \cdot A_{31}),$$

where given ω a p^nth root of unity λ is the injective map:

$$\lambda : (\mathbb{Z}/p^n\mathbb{Z})^+ \longrightarrow \mathbb{C}^\times$$
$$\lambda : x \longmapsto \omega^x.$$

ϕ will be restricted to subgroups giving us a homomorphism in each case.

4.1.1 When n is Even.

In this subsection we assume n is even and define m so that: $\boldsymbol{n=2m}$. Now ϕ_{L_m} is a homomorphism and therefore an irreducible character of L_m. We want to find the stabilizer of ϕ_{L_m}.

Proposition 4.1.1.

$$G_{\phi_{L_m}} = \left\{ \begin{bmatrix} a & x & y \\ p^m b & z & w \\ p^m c & p^m d & a + p^m e \end{bmatrix} \in G \right\} = T,$$

and

$$\left| G_{\phi_{L_m}} \right| = p^{12m-1}(p-1).$$

Proof. "$\subseteq$" We start by letting $B \in G_{\phi_{L_m}}$ and trace the exact steps taken in ([1], p.32-33) until the point $p^m(BAB^{-1})_{31} = p^m A_{31}$ for any A such that $I + p^m A \in L_m$. In our case we can choose any $A \in M_3(\mathbb{Z}/p^m\mathbb{Z})$ with $Tr(A) = 0$ in contrast to ([1], p.32-33) where A can any choice in

$M_3(\mathbb{Z}/p^m\mathbb{Z})$. As a result we get the system of equations:

(1) $p^m(B_{11}^{-1}B_{31} - B_{31}^{-1}B_{33}) = 0$ letting $A_{11} = 1, A_{33} = -1$, otherwise $A_{ij} = 0$

(2) $p^m B_{11}^{-1}B_{32} = 0$ letting $A_{21} = 1$, otherwise $A_{ij} = 0$

(3) $p^m(B_{21}^{-1}B_{32} - B_{31}^{-1}B_{33}) = 0$ letting $A_{22} = 1, A_{33} = -1$, otherwise $A_{ij} = 0$

(4) $p^m B_{11}^{-1}B_{33} = p^m$ letting $A_{31} = 1$, otherwise $A_{ij} = 0$

(5) $p^m B_{21}^{-1}B_{33} = 0$ letting $A_{32} = 1$, otherwise $A_{ij} = 0$.

Considering equation (4) we see that B_{11}^{-1} is a unit, so in (2) we have $p^m|B_{32}$. This means (3) reduces to $p^m B_{31}^{-1}B_{33} = 0$ but equation (4) also gives B_{33} as a unit so we have $p^m|B_{31}^{-1}$. This reduces (1) to $p^m B_{11}^{-1}B_{31} = 0$, and our system of equations has been reduced to the same system of 4 equations given in ([1], p.33) and we can finish tracing the rest of the proof given there. "$\supseteq$" is true since $T = G'_{\phi_{K_m}} \bigcap G \subseteq G_{\phi_{L_m}}$.

Lastly, consider the homomorphism $\det : G'_{\phi_{K_m}} \to (\mathbb{Z}/p^n\mathbb{Z})^\times$. Notice that $Image(\det) = (\mathbb{Z}/p^n\mathbb{Z})^\times$ so we have:

$$\left|G_{\phi_{L_m}}\right| = |\ker(\det)| = \frac{\left|G'_{\phi_{K_m}}\right|}{|(\mathbb{Z}/p^n\mathbb{Z})^\times|} = \frac{p^{14m-2}(p-1)^2}{p^{2m-1}(p-1)} = p^{12m-1}(p-1).$$

□

Next note ([1], p.33) where it is shown why ϕ_T is a homomorphism ($\phi_T \in Irr(T)$). This also shows $\phi_{L_m} \in Irr(L_m)$ since $L_m \leq T$. We can now repeat the steps taken in 3.1.1 on page 26 to get a character χ with:

$$deg(\chi) = \frac{|G|}{\left|G_{\phi_{L_m}}\right|} = \frac{p^{16m-5}(p^3-1)(p^2-1)}{p^{12m-1}(p-1)} = p^{4m-4}(p^2+p+1)(p^2-1) = p^{2n-4}(p^3-1)(p+1).$$

4.1.2 When n is Odd.

In this subsection we assume n is odd and define m so that: ***n=2m+1***. Now $\phi_{L_{m+1}}$ is an irreducible character of L_{m+1}. By a similar method used in the previous section we calculate the stabilizer:

$$G_{\phi_{L_m}} = \left\{ \begin{bmatrix} a & x & y \\ p^m b & z & w \\ p^m c & p^m d & a + p^m e \end{bmatrix} \in G \right\} = T,$$

with

$$\left|G_{\phi_{L_m}}\right| = p^{12m+7}(p-1).$$

In contrast to the even case we can not extend $\phi_{L_{m+1}}$ directly to T, so we outline the plan with the following lattice:

$$\begin{tikzcd}
G \arrow[d, dash, "p^{4m-4}(p^2-1)(p^2+p+1)"] & \text{affording } \chi = \phi_H^G \text{ using 2.4.15} \\
G_{\phi_{L_{m+1}}} = T \arrow[d, dash, "p^2"] & \text{affording } \phi_H^T \text{ using 2.4.15} \\
T_{\phi_N} = H \arrow[d, dash, "p^{4m-1}(p-1)"] & \text{affording } \phi_H \\
N \arrow[d, dash, "p^6"] & \text{affording } \phi_N \\
L_{m+1} \arrow[d, dash, "p^{8m}"] & \text{affording } \phi_{L_{m+1}} \\
< I > &
\end{tikzcd}$$

Where,

$$H = \left\{ \begin{bmatrix} a & x & y \\ p^m b & z & w \\ p^{m+1}c & p^{m+1}d & a+p^m e \end{bmatrix} \in G \right\}, \text{ and}$$

$$N = \left\{ \begin{bmatrix} 1+p^m a & p^m x & p^m y \\ p^m b & 1+p^m z & p^m w \\ p^{m+1}c & p^{m+1}d & 1+p^m e \end{bmatrix} \in G \right\}.$$

Proposition 4.1.2.

$$N \trianglelefteq T, \text{ with } T_{\phi_N} = H, \text{ also } |H| = p^{12m+5}(p-1), \text{ and } |N| = p^{8m+6}.$$

Proof. First $N \trianglelefteq T$ since given $I + np^m \in N$ (so $p|n_{31}, n_{32}$) and, $t \in T$ we have: $t(I+np^m)t^{-1} = I + p^m tnt^{-1} \in N$ because $p|(tnt^{-1})_{31}, (tnt^{-1})_{31}$.

Now let T', H', N' be defined exactly as T, H, N were defined respectively but with G' instead of G. Notice $|\det(N')| = p^{m+1}$, and $|\det(H')| = p^{2m}(p-1)$ giving:

$$|N| = \frac{N'}{\det(N')} = \frac{p^{9m+7}}{p^{m+1}} = p^{8m+6}, \quad |H| = \frac{H'}{\det(H')} = \frac{p^{14m+5}(p-1)^2}{p^{2m}(p-1)} = p^{12m+5}(p-1).$$

Finally we want $T_{\phi_N} = H$.

"$\subseteq$" Let

$$t = \begin{bmatrix} a & x & y \\ p^m b & z & w \\ p^m c & p^m d & a+p^m e \end{bmatrix} \in T_{\phi_N}, t^{-1} = \begin{bmatrix} a' & x' & y' \\ p^m b' & z' & w' \\ p^m c' & p^m d' & a'+p^m e' \end{bmatrix}, n = I+p^m \begin{bmatrix} x_1 & x_2 & x_3 \\ x_4 & x_5 & x_6 \\ px_7 & px_8 & x_9 \end{bmatrix} \in N.$$

So we have: $\phi_N^t(n) = \lambda(p^{m+1}a'ax_7 + p^{2m}(a'cx_1 + a'dx_4 + c'ax_9)) = \lambda(p^{m+1}x_7)$, for all choices of x_i where $n \in N$. Letting $x_4 = 1$ and $x_i = 0$ otherwise we have $a'dp^{2m} = 0 \overset{a' \text{ unit}}{\Rightarrow} p|d$. Next we let $x_1 = x_2 = x_4 = 1$, $x_5 = -1$, and $x_i = 0$ otherwise: which gives $a'cp^{2m} = 0 \overset{a' \text{ unit}}{\Rightarrow} p|c$. Therefore $t \in H$ and $T_{\phi_N} \subseteq H$.

"$\supseteq$" noting that the same argument from the previous section shows $\phi_H \in Irr(H)$ implying $\phi_N \in Irr(N)$ since $N \leq H$, gives ϕ_H as an extension of ϕ_N implying $H \subseteq T_{\phi_N}$. $\square$

We can now repeat the steps taken in 3.2.2 on page 35 (using 2.4.15 twice) to get a character χ with:

$$deg(\chi) = \frac{|G|}{|H|} = \frac{p^{16m+3}(p^3-1)(p^2-1)}{p^{12m+5}(p-1)} = p^{4m-2}(p^3-1)(p+1) = p^{2n-4}(p^3-1)(p+1).$$

4.2 An Irreducible Character of Degree $p^{2n-2}(p^2+p+1)$.

We start by recalling the map λ in 3.2 on page 29 and define the map:

$$\phi : M_3(\mathbb{Z}/p^n\mathbb{Z}) \longrightarrow \mathbb{C}^{\times}$$

$$\phi : A \longmapsto \lambda(A_{11}).$$

ϕ will be restricted to subgroups giving us a homomorphism in each case.

4.2.1 When n is Even.

In this subsection we assume n is even and define m so that: $\boldsymbol{n{=}2m}$. Now ϕ_{L_m} is a homomorphism and therefore an irreducible character of L_m. Again our next step is to calculate the stabilizer of ϕ_{L_m}.

Proposition 4.2.1.

$$G_{\phi_{L_m}} = \left\{ \begin{bmatrix} a & bp^m & cp^m \\ dp^m & x & y \\ ep^m & z & w \end{bmatrix} \in G \right\} = T,$$

and

$$|G_{\phi_{L_m}}| = p^{12m-3}(p-1)^2(p+1).$$

Proof. "$\subseteq$" We start by letting $B \in G_{\phi_{L_m}}$ and trace the exact steps taken in ([1], p.29-30) until the point $p^m(BAB^{-1})_{11} = p^m A_{11}$ for any A such that $I + p^m A \in L_m$. In our case we can choose any $A \in M_3(\mathbb{Z}/p^m\mathbb{Z})$ with $Tr(A) = 0$ in contrast to ([1], p.29-30) where A was any choice in $M_3(\mathbb{Z}/p^m\mathbb{Z})$. As a result we get the system of equations:

(1) $p^m(B_{11}^{-1}B_{11} - B_{21}^{-1}B_{12}) = p^m$ letting $A_{22} = 1, A_{33} = -1$, otherwise $A_{ij} = 0$

(2) $p^m(B_{21}^{-1}B_{12} - B_{31}^{-1}B_{13}) = 0$ letting $A_{11} = 1, A_{22} = -1$, otherwise $A_{ij} = 0$

(3) $p^m B_{11}^{-1}B_{12} = 0$ letting $A_{21} = 1$, otherwise $A_{ij} = 0$

(4) $p^m B_{11}^{-1}B_{13} = 0$ letting $A_{31} = 1$, otherwise $A_{ij} = 0$

(5) $p^m B_{21}^{-1}B_{11} = 0$ letting $A_{12} = 1$, otherwise $A_{ij} = 0$

(6) $p^m B_{31}^{-1}B_{11} = 0$ letting $A_{13} = 1$, otherwise $A_{ij} = 0$

(7) $p^m B_{31}^{-1}B_{12} = 0$ letting $A_{23} = 1$, otherwise $A_{ij} = 0$.

Multiply (3) by B_{11} implying: $p^m(B_{11}^{-1}B_{11})B_{12} = 0 \overset{(1)}{\Rightarrow} p^m(1 + B_{21}^{-1}B_{12})B_{12} = 0$, using this we consider two cases. Considering the case when B_{12} is a unit for some x we have: $1 + B_{21}^{-1}B_{12} = p^m x \Rightarrow B_{21}^{-1} = \frac{p^m x - 1}{B_{12}}$, so B_{21}^{-1} is also a unit. Otherwise if B_{12} is not a unit, then $1 + B_{21}^{-1}B_{12}$ is a unit, so for some x we have: $B_{12} = p^m x$. Next multiply (7) by B_{13} implying: $p^m(B_{31}^{-1}B_{13})B_{12} \overset{(2)}{=} p^m B_{21}^{-1}B_{12}^2 = 0$. This means that both B_{12} and B_{21}^{-1} can not be units so the first case stated above results in a contradiction and we must have the result of the second case: $B_{12} = p^m x$ for some x. But this reduces (1) to $p^m B_{11}^{-1}B_{11} = p^m$ so our system of equations has been reduced to the same system of 5 equations given in ([1], p.30) and we can finish tracing the rest of the proof given there.

"$\supseteq$" is true since $T = G'_{\phi_{K_m}} \bigcap G \subseteq G_{\phi_{L_m}}$.

Lastly consider the homomorphism $\det : G'_{\phi_{K_m}} \to (\mathbb{Z}/p^n\mathbb{Z})^\times$. Notice that $Image(\det) = (\mathbb{Z}/p^n\mathbb{Z})^\times$ so we have:

$$\left|G_{\phi_{L_m}}\right| = |\ker(\det)| = \frac{\left|G'_{\phi_{K_m}}\right|}{|(\mathbb{Z}/p^n\mathbb{Z})^\times|} = \frac{p^{14m-4}(p-1)^3(p+1)}{p^{2m-1}(p-1)} = p^{12m-3}(p-1)^2(p+1)$$

□

Noting that ϕ_T is a homomorphism we can repeat the steps taken in 3.2.1 on page 32 to get a character χ with:

$$deg(\chi) = \frac{|G|}{\left|G_{\phi_{L_m}}\right|} = \frac{p^{16m-5}(p^3-1)(p^2-1)}{p^{12m-3}(p-1)^2(p+1)} = p^{4m-2}(p^2+p+1) = p^{2n-2}(p^2+p+1).$$

4.2.2 When n is Odd.

In this subsection we assume n is odd and define m so that: ***n=2m+1***. Now $\phi_{L_{m+1}}$ is an irreducible character of L_{m+1}. By a similar method used in the previous section we calculate the stabilizer:

$$G_{\phi_{L_{m+1}}} = \left\{ \begin{bmatrix} a & p^m b & p^m c \\ p^m d & x & y \\ p^m e & z & w \end{bmatrix} \in G \right\} = T,$$

and

$$|T| = p^{12m+5}(p-1)^2(p+1).$$

In contrast to the even case we can not extend $\phi_{L_{m+1}}$ directly to T, so we out line the plan with the following lattice:

$$\begin{tikzcd}[row sep=large]
G \arrow[d, dash, "p^{4m-2}(p^2+p+1)"] & \text{affording } \chi = \phi_H^G \text{ using 2.4.15} \\
G_{\phi_{L_{m+1}}} = T \arrow[d, dash, "p^2"] & \text{affording } \phi_H^T \text{ using 2.4.15} \\
T_{\phi_N} = H \arrow[d, dash, "p^{4m-3}(p-1)^2(p+1)"] & \text{affording } \phi_H \\
N \arrow[d, dash, "p^6"] & \text{affording } \phi_N \\
L_{m+1} \arrow[d, dash, "p^{8m}"] & \text{affording } \phi_{L_{m+1}} \\
< I >
\end{tikzcd}$$

Where,

$$H = \left\{ \begin{bmatrix} a & p^{m+1} b & p^{m+1} c \\ p^m d & x & y \\ p^m e & z & w \end{bmatrix} \in G \right\}, \text{ and}$$

$$N = \left\{ \begin{bmatrix} 1+p^m a & p^{m+1} b & p^{m+1} c \\ p^m d & 1+p^m x & p^m y \\ p^m e & p^m z & 1+p^m w \end{bmatrix} \in G \right\}.$$

Proposition 4.2.2.

$$N \trianglelefteq T, \text{ with } T_{\phi_N} = H, \text{ also } |H| = p^{12m+3}(p-1)^2(p+1), \text{ and } |N| = p^{8m+6}.$$

Proof. Let T', H', N' be defined exactly as T, H, N were defined respectively but with G' instead of G. We have from ([1], p.39) that $N' \trianglelefteq T' \Rightarrow N' \bigcap G \trianglelefteq T' \bigcap G \Rightarrow N \trianglelefteq T$. Also $|\det(N')| = p^{m+1}$, and $|\det(H')| = p^{2m}(p-1)$ giving:

$$|N| = \frac{N'}{\det(N')} = \frac{p^{9m+7}}{p^{m+1}} = p^{8m+6}, \quad |H| = \frac{H'}{\det(H')} = \frac{p^{14m+3}(p-1)^3(p+1)}{p^{2m}(p-1)} = p^{12m+3}(p-1)^2(p+1).$$

Finally considering $n \in N$ we notice the determinate does not depend on n_{12} and n_{13} so we can repeat the chain of equivalences given in ([1], p.40) to get $T_{\phi_N} = H$. □

We can now repeat the steps taken in 3.2.2 on page 35 (using 2.4.15 twice) to get a character χ with:

$$deg(\chi) = \frac{|G|}{|H|} = \frac{p^{16m+3}(p^3-1)(p^2-1)}{p^{12m+3}(p-1)^2(p+1)} = p^{4m}(p^2+p+1) = p^{2n-2}(p^2+p+1).$$

4.3 An Irreducible Character of Degree $p^{3n-3}(p-1)^2(p+1)$.

In this section we restrict $p > 3$ and use results from 2.3 where we defined the subgroup S of G: this subgroup plays a key roll in this chapter. We will use the matrix:

$$B = \begin{bmatrix} 0 & 0 & a \\ 1 & 0 & b \\ 0 & 1 & 0 \end{bmatrix}.$$

where where a, b are defined on page 9.

4.3.1 When n is Even.

In this subsection we assume n is even and define m so that: $\boldsymbol{n=2m}$. Now recall λ as defined in 3.3.1 and define:

$$\phi : L_m \longrightarrow \mathbb{C}^\times$$

$$\phi : I + p^m A \longmapsto \lambda tr(p^m AB),$$

which is a homomorphism and therefore an irreducible character of L_m. Again our next step is to calculate the stabilizer of ϕ.

Proposition 4.3.1.

$$G_\phi = L_m S$$

and

$$|G_\phi| = p^{10m-2}(p^2 + p + 1).$$

Proof. "$\subseteq$" We start by letting $C \in G_\phi$ and trace the exact steps taken in ([1], p.36-37) until the point where $tr(Ap^m(B - C^{-1}BC)) = 0$ for any A such that $I + p^m A \in L_m$. In our case we can choose any $A \in M_3(\mathbb{Z}/p^m\mathbb{Z})$ with $Tr(A) = 0$ in contrast to ([1], p.36-37) where A was any choice in $M_3(\mathbb{Z}/p^m\mathbb{Z})$. By considering different choices of A we get:

$$p^m(B - C^{-1}BC) = \begin{bmatrix} x & 0 & 0 \\ 0 & x & 0 \\ 0 & 0 & x \end{bmatrix}$$

for some $x \in \mathbb{Z}/p^{2m}\mathbb{Z}$. But since $tr(p^m(B - C^{-1}BC)) = 0$ we have: $3x = 0 \overset{3 \text{ a unit}}{\Longrightarrow} x = 0$. Now our equation has been reduced to $p^m(B - C^{-1}BC) = 0$ which is the same equation given in ([1], p.37) and we can continue tracing the proof given there until we get $C \in K_m S'$ (where S' is defined exactly as S was defined but with G' instead of G). Since $C \in G$ we now have $C \in K_m S \cap G$, so to conclude the proof of this inclusion we are left to show: $K_m S' \cap G = L_m S$. "$\subseteq$" Let $(I + p^m A)s \in K_m S' \cap G$ where, $(I + p^m A) \in K_m$, $s \in S'$ and $\det((I + p^m A)s) = 1$. Now pick

$$X = \left(1 + p^m \left(\frac{-(A_{11} + A_{22} + A_{33}) - 2zb}{3}\right)\right) I + p^m yB + p^m zB^2 \ \in K_m \cap S'.$$

We have:

$$\begin{aligned}
&(I + p^m A)s \\
&= (I + p^m A)(X \cdot X^{-1})s \\
&= ((I + p^m A)X) \cdot (X^{-1}s) \\
&\in L_m S && \text{since } \det(X) = \frac{1}{\det(I + p^m A)} \text{ and } \det(X^{-1}) = \frac{1}{\det(S)}.
\end{aligned}$$

Therefore $K_m S' \cap G \subseteq L_m S$. "$\supseteq$" Is clear since $L_m = K_m \cap G$ and $S' = S \cap G$. Finally we have $K_m S' \cap G = L_m S$ so that $C \in L_m S$ and $G_\phi \subseteq L_m S$.

"$\supseteq$" is true since we can follow the same argument in ([1], p.36).

Lastly consider the homomorphism $\det : K_m \cap S' \to (\mathbb{Z}/p^n\mathbb{Z})^\times$. Notice that: $Image(\det) = \{1 + p^m x \mid x \in \mathbb{Z}/p^m\mathbb{Z}\}$ so we have: $|L_m \cap S| = |Ker(\det)| = \frac{|K_m \cap S'|}{p^m} = \frac{p^{3m}}{p^m} = p^{2m}$. Implying $|L_m S| = \frac{|L_m| \cdot |S|}{|L_m \cap S|} = \frac{p^{8m} \cdot p^{4m-2}(p^2+p+1)}{p^{2m}} = p^{10m-2}(p^2 + p + 1)$. □

We can repeat the steps taken in 3.3.1 on page 41 to get a irreducible character χ with:

$$deg(\chi) = \frac{|G|}{|G_\phi|} = \frac{p^{16m-5}(p^3 - 1)(p^2 - 1)}{p^{10m-2}(p^2 + p + 1)} = p^{6m-3}(p-1)^2(p+1) = p^{3n-3}(p-1)^2(p+1).$$

4.3.2 When n is Odd.

In this subsection we assume n is odd and define m so that: ***n=2m+1***. We use the same method used in 3.3.2 constructing a character of L_{m+1} and using 2.4.15.

$$\begin{tikzcd}[row sep=large]
G \arrow[d, dash, "p^{6m-3}(p-1)^2(p+1)"] & \text{affording } \chi = \gamma^G \text{ using 2.4.15} \\
G_\phi = L_m S \arrow[d, dash, "p^2+p+1"] & \text{affording } \delta \text{ an extension of } \gamma \\
L_m(L_1 \cap S) \arrow[d, dash, "p^3"] & \text{affording } \gamma = \beta^{L_m(L_1 \cap S)} \text{ using 2.4.16} \\
N(L_1 \cap S) \arrow[d, dash, "p^3"] & \text{affording } \beta \text{ an extension of } \alpha \\
L_{m+1}(L_1 \cap S) \arrow[d, dash, "p^{2m}"] & \text{affording } \alpha \text{ an extension of } \phi \\
L_{m+1} \arrow[d, dash, "p^{8m}"] & \text{affording } \phi \\
< I >
\end{tikzcd}$$

Where,

$$N = \left\{ \begin{bmatrix} 1+p^{m+1}a & p^m x & p^m y \\ p^{m+1}b & 1+p^{m+1}z & p^m w \\ p^{m+1}c & p^{m+1}d & 1+p^{m+1}e \end{bmatrix} \in G \right\}.$$

Define the injective homomorphism: λ as in 3.3.2 a define:

$$\phi : L_{m+1} \longrightarrow \mathbb{C}^\times$$

$$\phi : A \longmapsto \lambda tr(AB),$$

Now, ϕ is a character of L_{m+1} with degree 1. A similar calculation to the one used in 4.3.1 shows: $G_\phi = L_m S$. Repeating the method used in 3.3.2 we find α **an extension of** ϕ to $L_{m+1}(L_1 \cap S)$.

Next we find the sizes of our subgroups in the above lattice. To do so we use Hensel's lemma (as stated in 3.3.3) in the following proposition.

Proposition 4.3.2. $|L_{m+1}(L_1 \cap S)| = p^{10m}$, $|N(L_1 \cap S)| = p^{10m+3}$, $|L_m(L_1 \cap S)| = p^{10m+6}$, $|L_m S| = p^{10m+6}(p^2+p+1)$.

Proof. Start by defining N' exactly as N was defined but with G' instead of G, so:

$$|N| = \frac{|N'|}{|\det(N')|} = \frac{p^{9m+3}}{p^m} = p^{8m+3}.$$

From 4.0.1 we have $|L_m| = p^{8m+8}$. Now we find $|L_1 \bigcap S|$, let $X = (1+px)I + pyB + pzB^2 \in L_1 \bigcap S$. To calculate $|L_1 \cap S|$ pick an arbitrary $X \in L_1 \cap S$ and count the solutions to $\det(X) = 1$. For $x, y, z \in \mathbb{Z}/p^n\mathbb{Z}$ X has the form $X = (1+px)I + pyB + pzB^2$ so we want to count solutions of:

$$\begin{aligned} &\det(X) = 1 + p(3x + 2bz) + p^2 g(x,y,z) = 1 && \text{for some polynomial } g \\ &\Leftrightarrow f(x^*) \equiv x^* + p \cdot g(x,y,z) \mod p^{2m} \quad (*) && \text{letting } x^* \equiv 3x + 2bz \mod p^{2m}. \end{aligned}$$

Now, $f(0) \equiv 0 \mod p$ and $f'(0) \not\equiv 0 \mod p$ so by 3.3.3 there is a unique $x_{2m} \mod p^{2m}$ so $f(x_{2m}) \equiv 0 \mod p^{2m}$. This means that for each y in (*) there is exactly one x^* which gives a solution. Therefore there are p^{2m} choices for y in (*) and for each choice of y there are p^{2m} solutions for x and z in $x^* \equiv 3x + 2bz \mod p^{2m}$. As a result $|L_1 \cap S| = p^{2m} \cdot p^{2m} = p^{4m}$. By using the same method we calculate:

$$|L_m \cap S| = p^{2m+2}, \quad |L_{m+1} \cap S| = p^{2m}.$$

Now,

$$\begin{aligned} |L_{m+1}(L_1 \cap S)| &= \frac{|L_{m+1}| \cdot |L_1 \cap S|}{|L_{m+1} \cap S|} = \frac{p^{8m} \cdot p^{4m}}{p^{2m}} = p^{10m}, \\ |N(L_1 \cap S)| &= \frac{|N| \cdot |L_1 \cap S|}{|N \cap S|} = \frac{p^{8m+3} \cdot p^{4m}}{p^{2m}} = p^{10m+3}, \\ |L_m(L_1 \cap S)| &= \frac{|L_m| \cdot |L_1 \cap S|}{|L_m \cap S|} = \frac{p^{8m+8} \cdot p^{4m}}{p^{2m+2}} = p^{10m+6}, \end{aligned}$$

and using 2.3.3

$$|L_m S| = \frac{|L_m| \cdot |S|}{|L_m \cap S|} = \frac{p^{8m+8} \cdot p^{4m}(p^2+p+1)}{p^{2m+2}} = p^{10m+6}(p^2+p+1)$$

□

Now we can repeat the method used in 3.3.2 to obtain a character δ of degree p^3 of G_ϕ; giving an irreducible character χ of G with:

$$deg(\chi) = deg(\delta)\frac{|G|}{|G_\phi|} = p^3 \cdot \left(\frac{p^{16m+3}(p^3-1)(p^2-1)}{p^{10m+6}(p^2+p+1)}\right) = p^{6m}(p-1)^2(p+1) = p^{3n-3}(p-1)^2(p+1).$$

Bibliography

[1] Qianglong Wen, *Irreducible Characters of* $GL_k(\mathbb{Z}/p^n\mathbb{Z})$, M.Sc. Thesis, University of Alberta, 2006.

[2] Robert Barrington Leigh, Gerald Cliff, and Qianglong Wen, *Characters Values for* $GL_2(\mathbb{Z}/p^n\mathbb{Z})$, Preprint, University of Alberta, 2009.

[3] David S. Dummit and Richard M. Foote, *Abstract Algebra 3rd Edition,* John Wiley and Sons, New Jersey, 2003.

[4] Thomas W. Hungerford, *Abstract Algebra 2nd Edition,* Thomson Brooks/Cole, Pacific Grove, California, 1997.

[5] Gordon James and Martin Liebeck, *Representations and Character of Groups,* University Press, Cambridge, 2001.

[6] I. Martin Isaacs, *Character Theory of Finite Groups,* Dover Publications, New York, 1976.

[7] Kenneth H. Rosen, *Elementary Number Theory 5th Edition,* Addison Wesley, Boston, 2005.

[8] Thomas P. Dence, *Elements of the Theory of Numbers,* Academic Press, San Diego, 1999.

[9] William Fulton, Joe Harris, *Representation Theory: A First Course,* Springer, New York, 1999.

Appendix: Maple Commands

- Case: c is not a unit.

```
> y := ((1/2)*n[2]+c*n[1]*epsilon/(2*a))/(a-c^2*epsilon/a);
> x := -n[1]/(2*a)-y*c/a;
> w := c*x/a-n[2]/(2*a*epsilon);
> g := a+(1/2)*n[1]*p; h := c+n[2]*p/(2*epsilon);
```

$$y := \left(1/2\,n_2 + 1/2\,\frac{cn_1\epsilon}{a}\right)\left(a - \frac{c^2\epsilon}{a}\right)^{-1}$$

$$x := -1/2\,\frac{n_1}{a} - \left(1/2\,n_2 + 1/2\,\frac{cn_1\epsilon}{a}\right)c\left(a - \frac{c^2\epsilon}{a}\right)^{-1}a^{-1}$$

$$w := c\left(-1/2\,\frac{n_1}{a} - \left(1/2\,n_2 + 1/2\,\frac{cn_1\epsilon}{a}\right)c\left(a - \frac{c^2\epsilon}{a}\right)^{-1}a^{-1}\right)a^{-1} - 1/2\,\frac{n_2}{a\epsilon}$$

$$g := a + 1/2\,n_1 p$$

$$h := c + 1/2\,\frac{n_2 p}{\epsilon}$$

```
> t := `.`(
Matrix(2, 2, {(1, 1) = 1+x*p, (1, 2) = y*p,(2, 1) = w*p, (2, 2) = 1-x*p}) ,
Matrix(2, 2, {(1, 1) = g, (1, 2) = h*epsilon,(2, 1) = h, (2, 2) = g})):
map(simplify, simplify(t, {p^2 = 0}));
```

$$\begin{bmatrix} a & c\epsilon + n_2 p \\ c & a + n_1 p \end{bmatrix}$$

- Case: c is a unit.

```
> w := ((1/2)*n[1]+a*n[2]/(2*c*epsilon))/(-a^2/c+c^2*epsilon*1/c);
> x := w*a/c+n[2]/(2*c*epsilon);
> y := -n[1]/(2*c)-a*x/c;
> g := a+(1/2)*n[1]*p; h := c+n[2]*p/(2*epsilon);
```

$$w := \left(1/2\,n_1 + 1/2\,\frac{an_2}{c\epsilon}\right)\left(-\frac{a^2}{c} + c\epsilon\right)^{-1}$$

$$x := \left(1/2\,n_1 + 1/2\,\frac{an_2}{c\epsilon}\right)a\left(-\frac{a^2}{c} + c\epsilon\right)^{-1}c^{-1} + 1/2\,\frac{n_2}{c\epsilon}$$

$$y := -1/2\,\frac{n_1}{c} - a\left(\left(1/2\,n_1 + 1/2\,\frac{an_2}{c\epsilon}\right)a\left(-\frac{a^2}{c} + c\epsilon\right)^{-1}c^{-1} + 1/2\,\frac{n_2}{c\epsilon}\right)c^{-1}$$

$$g := a + 1/2\,n_1 p$$

$$h := c + 1/2\,\frac{n_2 p}{\epsilon}$$

```
> t := `.`(
Matrix(2, 2, {(1, 1) = 1+x*p, (1, 2) = y*p, (2, 1) = w*p, (2, 2) = 1-x*p}),
Matrix(2, 2, {(1, 1) = g, (1, 2) = h*epsilon, (2, 1) = h, (2, 2) = g})):
map(simplify, simplify(t, {p^2 = 0}));
```

$$\begin{bmatrix} a & c\epsilon + n_2 p \\ c & a + n_1 p \end{bmatrix}$$

(*Note the simplification*: $p^m = p$ *so that* $p^2 = 0$)