

$GL_2(\mathbf{F}_p)$

Amritanshu Prasad

THE INSTITUTE OF MATHEMATICAL SCIENCES, CHENNAI.

URL: <http://www.imsc.res.in/~amri>

Contents

Introduction	iii
Chapter I. Fourier theory for finite abelian groups	1
1. The Pontryagin dual	1
2. The Fourier transform	1
Chapter II. Some finite fields	5
1. Existence and uniqueness	5
2. The multiplicative group of \mathbf{F}_q	6
3. Galois theoretic properties	7
4. Fourier theory on finite fields	8
5. Matrix representation of \mathbf{F}_{p^2}	8
Chapter III. Representations of finite groups	11
1. Basic definitions	11
2. Induced representations	11
3. Mackey's theorem	12
Chapter IV. Some representations of $GL_2(\mathbf{F}_p)$	15
1. Conjugacy classes in $GL_2(\mathbf{F}_p)$	15
2. Subgroup of upper-triangular matrices	16
3. Induced representations	16
Chapter V. Cuspidal representations	21
1. The degrees of cuspidal representations	21
2. A presentation of $SL_2(\mathbf{F}_p)$	22
3. The Weil representation	24
Bibliography	27

Introduction

Let p denote a prime number. Denote by \mathbf{F}_p the finite field $\mathbf{Z}/p\mathbf{Z}$. These lectures concern general linear groups of order two over \mathbf{F}_p . This is the beginning of a much larger theory involving all the finite groups of Lie type. These groups play an important role in the classification of finite simple groups. Besides understanding the finite simple groups and their representation theory, these groups also play an important role in number theory. The Langlands correspondence envisages a subtle relationship between Galois groups of various fields that occur in number theory and the representation theory of matrix groups over these fields via certain analytic functions called L -functions. Among these are the p -adic field \mathbf{Q}_p . The representation theory of matrix groups over \mathbf{Q}_p is built up over the theory for matrix groups over \mathbf{F}_p . It is therefore no surprise that the study of these groups has proved to be extremely rewarding to mathematicians for over a century, as we will soon see.

In these lectures we will consider the groups

$$GL_2(\mathbf{F}_p) = \left\{ \begin{pmatrix} x & y \\ z & w \end{pmatrix} \middle| x, y, z, w \in \mathbf{F}_p, \quad xw - yz \neq 0 \right\}$$

of invertible 2×2 matrices with entries in \mathbf{F}_p . The representations of these groups were first classified independently by Herbert E. Jordan [Jor07] and Issai Schur [Sch07] in 1907. The method used here is not that of Jordan or Schur, but rather a special case of an idea due to the French mathematician André Weil, who introduced it in his famous article [Wei64]. Daniel Bump's beautiful exposition from [Bum97, Section 4.1] is used as the main source.

For $n \times n$ matrices, the representations were classified by James A. Green in 1955 [Gre55]. The general linear groups are special cases of a class of groups known as *reductive groups*, which occur as closed subgroups of general linear groups (in the sense of algebraic geometry). In 1970, T. A. Springer presented a set of conjectures describing the characters of irreducible representations of all reductive groups over finite fields, some of which he attributed to Ian G. MacDonald [Spr70]. The essence of these conjectures is that the irreducible representations of reductive groups over finite fields occur in families associated to

maximal tori in these groups (in this context, a torus is a subgroups that is isomorphic to a product of multiplicative groups of finite extensions of \mathbf{F}_p). The big breakthrough in this subject came in 1976, when Pierre Deligne and George Lusztig [DL76], were able to construct the characters of almost all the irreducible representations (in an asymptotic sense) of all reductive groups over finite fields, in particular, proving the conjectures of MacDonald. Much more information about the irreducible representations of reductive groups over finite fields has been obtained in later work, particularly by Lusztig (see e.g., [Lus84]). The above survey here is far from complete and fails to mention many important developments in the subject. It is included only to give the reader a rough sense of where the material to be presented in these lectures lies in the larger context of 20th century mathematics.

Thus one may treat these lectures as an introduction to the first results in what turned out to be one of the great mathematical achievements of the 20th century, and continues to influence mathematics today.

CHAPTER I

Fourier theory for finite abelian groups

1. The Pontryagin dual

Let G be an abelian group. A *character* of G is a homomorphism $\chi : G \rightarrow \mathbf{C}^\times$. The character χ is called *unitary* if $|\chi(g)| = 1$ for all $g \in G$.

EXERCISE 1.1. Show that every character of a finite abelian group is unitary.

If G is a finite abelian group, its *Pontryagin dual* is the set \widehat{G} of its characters. Under point-wise multiplication of characters, \widehat{G} forms a group. This is a special case of a general construction for *locally compact abelian groups*.

PROPOSITION 1.2. For any finite abelian group G , $G \cong \widehat{\widehat{G}}$.

PROOF.

EXERCISE 1.3. Show that the Proposition is true for a finite cyclic group $\mathbf{Z}/n\mathbf{Z}$.

EXERCISE 1.4. If G_1 and G_2 are abelian groups, show that

$$\widehat{G_1 \times G_2} \cong \widehat{G_1} \times \widehat{G_2}.$$

EXERCISE 1.5. Show that every finite abelian group is isomorphic to a product of finite cyclic groups.

□

It follows from the above proposition that $\widehat{\widehat{G}} \cong G$. However, in this case, there is a *canonical* isomorphism $G \rightarrow \widehat{\widehat{G}}$ given by $g \mapsto \check{g}$ where \check{g} is defined by

$$\check{g}(\chi) = \chi(g) \text{ for each } \chi \in \widehat{G}.$$

2. The Fourier transform

There are two \mathbf{C}^* -algebra structures on $\mathbf{C}[G]$, which we will think of as complex-valued functions on G . The first is that of the complex

group algebra. Here the product is *convolution*:

$$(f * h)(x) = \frac{1}{|G|} \sum_{y \in G} f(xy^{-1})h(y) \text{ for } f, h \in \mathbf{C}[G]$$

and the $*$ -involution is given by $f^*(g) = \overline{f(g^{-1})}$. Henceforth in these notes, by $f^*(g)$ we will always mean $\overline{f(g^{-1})}$.

EXERCISE 2.1. Compare the above with the definition given in the lectures on \mathbf{C}^* -algebras.

The second is where product is given by point-wise multiplication of functions and the $*$ -involution is point-wise complex conjugation $f(x) \mapsto \overline{f(x)}$.

Fourier theory on finite abelian groups provides a canonical isomorphism between $\mathbf{C}[G]$ and $\mathbf{C}[\widehat{G}]$, which, up to a scalar factor, takes the convolution-algebra structure to the point-wise multiplication structure and vice-versa. When this operation is repeated two times, we get a map $\mathbf{C}[G] \rightarrow \mathbf{C}[\widehat{G}] \rightarrow \mathbf{C}[G]$. There is a Fourier inversion formula which says that this composition map is *essentially* the identity on $\mathbf{C}[G]$.

Given a function $f \in \mathbf{C}[G]$, its *Fourier transform* is defined as the function $\widehat{f} \in \mathbf{C}[\widehat{G}]$ given by

$$\widehat{f}(\chi) = \frac{1}{|G|} \sum_{g \in G} f(g)\overline{\chi(g)} = (f * \chi)(1).$$

EXERCISE 2.2. Show that $\widehat{f * h} = \widehat{f}\widehat{h}$ for all $f, h \in \mathbf{C}[G]$.

The following lemma will be needed for Exercise 2.5.

LEMMA 2.3. For any $\chi \in \widehat{G}$

$$\frac{1}{|G|} \sum_{g \in G} \chi(g) = \begin{cases} 1 & \text{if } \chi \text{ is the trivial character,} \\ 0 & \text{otherwise.} \end{cases}$$

PROOF. For the trivial character the lemma is easy. If χ is a non-trivial character, then there exists an element $g \in G$ such that $\chi(g) \neq 1$. Let X be a set of representatives for $G/\langle g \rangle$. Then

$$\begin{aligned} \sum_{g \in G} \chi(g) &= \sum_{x \in X} \sum_{y \in \langle g \rangle} \chi(xy) \\ &= \sum_{x \in X} \chi(x) \left(\sum_{y \in \langle g \rangle} \chi(y) \right). \end{aligned}$$

The sum in parentheses is zero if and only if the lemma is true for a cyclic group.

EXERCISE 2.4. Prove Lemma 2.3 when G is a cyclic group. □

Before we proceed further, note the simple fact that an element of \widehat{G} can be thought of as a complex-valued function on G , and hence an element of $\mathbf{C}[G]$. We will use the notation 1_g to denote the function on G whose value is 1 at g and 0 everywhere else.

EXERCISE 2.5. Show that for each $\chi \in \widehat{G}$, thought of as an element of $\mathbf{C}[G]$, $\widehat{\chi} = 1_\chi$.

EXERCISE 2.6. Show that for any $g \in G$, $\widehat{1_g}(\chi) = \frac{1}{|G|}\chi(g^{-1})$.

EXERCISE 2.7. Use the previous two exercises to show that $\widehat{\widehat{\chi}}(x) = \frac{1}{|G|}\chi(x^{-1})$.

Giving $\mathbf{C}[G]$ a little additional structure (that of a Hilbert space), allows us to derive all the essential properties of Fourier transforms from the above exercises. For $f, h \in \mathbf{C}[G]$ define

$$\langle f, h \rangle = \frac{1}{|G|} \sum_{g \in G} f(g) \overline{h(g)}.$$

PROPOSITION 2.8. *With respect to the Hermitian inner product defined above, the set \widehat{G} is an orthonormal basis of $\mathbf{C}[G]$.*

PROOF. Note that for $\chi, \eta \in \widehat{G}$

$$\langle \chi, \eta \rangle = \frac{1}{|G|} \sum_{g \in G} \chi \eta^{-1}(g).$$

But $\chi \eta^{-1}$ is also in \widehat{G} . It is the trivial character if $\chi = \eta$ and a non-trivial character otherwise. Therefore orthonormality follows from Lemma 2.3. □

We are now in a position to prove the Fourier inversion formula:

THEOREM 2.9 (the Fourier inversion formula). *For all $f \in \mathbf{C}[G]$,*
 $\widehat{\widehat{f}}(x) = \frac{1}{|G|}f(x^{-1})$.

PROOF. Note that the Fourier transform is \mathbf{C} -linear. Moreover, by Exercise 2.7 and Proposition 2.8, the Fourier inversion formula holds for a basis of $\mathbf{C}[G]$. Therefore it must hold for all $f \in \mathbf{C}[G]$. □

EXERCISE 2.10. Use the Fourier inversion formula with Exercise 2.2 to show that for $f, h \in \mathbf{C}[G]$, $\widehat{f \widehat{h}} = \widehat{f} * \widehat{h}$.

CHAPTER II

Some finite fields

In this section, we study the finite fields. Such a field must have prime characteristic (the characteristic of a field is the smallest integer n such that $1 + 1 + \cdots + 1$ (n times) is 0). Therefore, it contains one of the finite fields \mathbf{F}_p . This makes it a finite dimensional vector space over \mathbf{F}_p , so that its order must be some power of p . We will see that, up to isomorphism, there is exactly one field of a given prime power order. We will also show that choosing a non-trivial character of the additive group of a finite field gives an identification of this group with its Pontryagin dual, and we will study the Fourier transform in this context.

1. Existence and uniqueness

We will show that for any power p^k of p , there is a unique finite field of order p^k , which is unique up to isomorphism¹. For convenience, write $q = p^k$. Fix an algebraic closure $\overline{\mathbf{F}_p}$ of \mathbf{F}_p . Look at the set

$$\mathbf{F}_q := \{x \in \overline{\mathbf{F}_p} \mid x^q = x\}.$$

EXERCISE 1.1. If $x, y \in \mathbf{F}_q$, then show that $x + y$ and xy are in \mathbf{F}_q .

It follows from the above exercise that \mathbf{F}_q is a field (why?).

EXERCISE 1.2. Let K be any field, and $f(X) \in K[X]$ be of degree d . Show that $f(X)$ can not have more than d roots in K .

Since the elements of S are roots of the polynomial $X^q - X$ which has degree q , there can be no more than q of them.

EXERCISE 1.3. Let K be any field. For a polynomial $f(X) \in K[X]$

$$f(X) = a_0X^n + a_1X^{n-1} + \cdots + a_{n-1}X + a_n$$

define its (formal) derivative to be the polynomial

$$f'(X) = na_0X^{n-1} + (n-1)a_1X^{n-2} + \cdots + a_{n-1}.$$

¹The method given here assumes the existence of an algebraic closure of \mathbf{F}_p . This is contingent upon the axiom of choice. However, there are other ways to prove the same results without using the axiom of choice, see [IR90, Chapter 7].

Show that if a is a multiple root of $f(X)$ (i.e., $(X - a)^2 | f(X)$) then $f'(a) = 0$.

The derivative of the polynomial $X^q - X$ is the constant polynomial -1 . Therefore, all its roots in $\overline{\mathbf{F}}_p$ are distinct. This means that S has exactly q elements. Therefore there exists a subfield of order q in $\overline{\mathbf{F}}_p$. In particular there exists a finite field of order q .

On the other hand, in any field of order q , the multiplicative group of non-zero elements in the field has order $q-1$. Therefore, each element of the field satisfies $x^{q-1} = 1$, or $x^q = x$. Thus any subfield of \mathbf{F}_q of order q must be equal to S .

Now any field of order q must have characteristic p , hence is an algebraic extension of \mathbf{F}_p . Therefore, it is isomorphic to some subfield of $\overline{\mathbf{F}}_p$. We have seen that only such field is \mathbf{F}_q . It follows that every field of order q is isomorphic to \mathbf{F}_q . We have proved the following theorem:

THEOREM 1.4. *For every power q of a prime number field, there exists a finite field of order q . Any two such fields are isomorphic.*

2. The multiplicative group of \mathbf{F}_q

We present the proof of the following theorem straight out of Serre's book [Ser73].

THEOREM 2.1. *The multiplicative group \mathbf{F}_q^\times is cyclic of order $q-1$.*

PROOF. If d is an integer ≥ 1 , then let $\phi(d)$ denote the number of integers x with $1 \leq x \leq d$ such that $(x, d) = 1$. In other words, the image of x in $\mathbf{Z}/d\mathbf{Z}$ is a generator of $\mathbf{Z}/d\mathbf{Z}$. The function $\phi(d)$ is called the *Euler totient function*.

LEMMA 2.2. *If $n \geq 1$ is an integer then*

$$n = \sum_{d|n} \phi(d).$$

PROOF. If $d|n$, let C_d denote the unique subgroup of order d in $\mathbf{Z}/n\mathbf{Z}$, and Φ_d denote the generators of C_d . Then $\mathbf{Z}/n\mathbf{Z}$ is the disjoint union of the Φ_d . Φ_d had $\phi(d)$ elements. Adding up cardinalities, $n = \sum_{d|n} \phi(d)$. \square

LEMMA 2.3. *Let H be a finite group of order n . Suppose that, for all divisors d of n the set*

$$\{x \in H | x^d = 1\}$$

has at most d elements. Then H is cyclic.

PROOF. Let $d|n$. If there exists $x \in H$ of order d , the subgroup

$$\langle x \rangle = \{1, x, \dots, x^{d-1}\}$$

is cyclic of order d . By hypothesis, every element y such that $y^d = 1$ is in $\langle x \rangle$. In particular, the elements of order d are the generators of $\langle x \rangle$, and these are $\phi(d)$ in number. Hence the number of elements of order d is either 0 or $\phi(d)$. If it were zero for some $d|n$, Lemma 2.2 would show that the number of elements in H is strictly less than n , contrary to hypothesis. In particular, there exists an element of order n in H , and H so H is cyclic of order n . \square

To complete the proof of Theorem 2.1, note that the equation $x^d = 1$ is a polynomial equation, and hence, by Exercise 1.2 has at most d solutions in \mathbf{F}_q . \square

3. Galois theoretic properties

Since \mathbf{F}_{p^2} is a quadratic extension of \mathbf{F}_p , its Galois group is cyclic of order 2. Clearly, the map $F : x \mapsto x^p$ is an automorphism of \mathbf{F}_{p^2} that fixes \mathbf{F}_p . Therefore, it must be the non-trivial element in the Galois group of \mathbf{F}_{p^2} over \mathbf{F}_p . F is called the *Frobenius automorphism*. In analogy with complex conjugation, we write $F(x) = \bar{x}$ for each $x \in \mathbf{F}_{p^2}$.

PROPOSITION 3.1. *Suppose $x \in \mathbf{F}_{p^2}$. Then $x = \bar{x}$ if and only if $x \in \mathbf{F}_p$.*

There are two natural maps from \mathbf{F}_{p^2} to \mathbf{F}_p :

(1) The *norm map* N :

$$N(x) = x\bar{x}.$$

(2) The *trace map* tr :

$$\text{tr}(x) = x + \bar{x}.$$

Note that for any $x \in \mathbf{F}_{p^2}$, $N(x) = 0$ if and only if $x = 0$.

EXERCISE 3.2. Show that the norm map $N : \mathbf{F}_{p^2}^\times \rightarrow \mathbf{F}_p^\times$ is surjective. Conclude that for any $x \in \mathbf{F}_p$, the number of elements $y \in \mathbf{F}_{p^2}$ such that $N(y) = x$ is

$$\begin{cases} p+1 & \text{if } x \neq 0 \\ 1 & \text{if } x = 0. \end{cases}$$

4. Fourier theory on finite fields

Assume that $p \neq 2$. In the case of the additive group of a finite field \mathbf{F}_{p^2} , it is possible to identify the Pontryagin dual with \mathbf{F}_{p^2} by using an *additive character* of \mathbf{F}_p and the trace map (an additive character of a field is a character of its additive group). Fix a non-trivial additive character $\psi : \mathbf{F}_p \rightarrow \mathbf{C}^\times$. Given $x \in \mathbf{F}_{p^2}$ define $\chi_x \in \widehat{\mathbf{F}_{p^2}}$ by

$$\chi_x(y) = \psi(\mathrm{tr}(xy)).$$

THEOREM 4.1. *The map $x \mapsto \chi_x$ is an isomorphism $\mathbf{F}_{p^2} \rightarrow \widehat{\mathbf{F}_{p^2}}$.*

PROOF. It suffices to show that for each $x \neq 0 \in \mathbf{F}_{p^2}$ there exists $y \in \mathbf{F}_{p^2}$ such that $\mathrm{tr}(xy) \neq 0$. However, the set $\{xy \mid y \in \mathbf{F}_{p^2}\}$ is all of \mathbf{F}_{p^2} . Therefore, it suffices to show that there is an element in \mathbf{F}_{p^2} whose trace is not 0. Since $p \neq 2$, $\mathrm{tr}(1) \neq 0$ in \mathbf{F}_p . \square

EXERCISE 4.2. What happens if $p = 2$?

Therefore, we may define the Fourier transform of a function $\Phi : \mathbf{F}_q \rightarrow \mathbf{C}$ as

$$\begin{aligned} \widehat{\Phi}(x) &= \widehat{\Phi}(\chi_x) \\ &= \frac{1}{p^2} \sum_{y \in \mathbf{F}_{p^2}} \Phi(y) \chi_x(y)^{-1} \\ &= \frac{1}{p^2} \sum_{y \in \mathbf{F}_{p^2}} \Phi(y) \psi(-\mathrm{tr}(xy)). \end{aligned}$$

We have the Fourier inversion formula:

$$\widehat{\widehat{\Phi}}(x) = \frac{1}{p^2} \Phi(-x).$$

5. Matrix representation of \mathbf{F}_{p^2}

\mathbf{F}_{p^2} is a two-dimensional vector space over \mathbf{F}_p . Moreover, for a fixed element $a \in \mathbf{F}_{p^2}$, the map $\theta_a : \mathbf{F}_{p^2} \rightarrow \mathbf{F}_{p^2}$ defined by

$$\theta_a(x) = ax \text{ for each } x \in \mathbf{F}_{p^2}$$

is \mathbf{F}_p linear. Therefore, if we fix a basis for the vector space \mathbf{F}_{p^2} over \mathbf{F}_p , each element of \mathbf{F}_{p^2} can be thought of as a 2×2 matrix with entries in \mathbf{F}_p . For example, if $D \in \mathbf{F}_p^\times$ is not a perfect square in \mathbf{F}_p (such an element always exists if $p \neq 2$), pick a square root of D and call it \sqrt{D} . Then $\{1, \sqrt{D}\}$ is a basis of \mathbf{F}_{p^2} over \mathbf{F}_p . We have

$$\mathbf{F}_{p^2} = \{x + y\sqrt{D} \mid x, y \in \mathbf{F}_p\}.$$

In terms of this basis, the matrix of $\theta_{x+y\sqrt{D}}$ is given by

$$\begin{pmatrix} x & Dy \\ y & x \end{pmatrix}.$$

PROPOSITION 5.1. *There exists an injective homomorphism of groups $\mathbf{F}_{p^2}^\times \rightarrow GL_2(\mathbf{F}_p)$ given by*

$$x + y\sqrt{D} \mapsto \begin{pmatrix} x & Dy \\ y & x \end{pmatrix}.$$

We will denote the image of the above map by T_a . We will sometimes refer to it as the *anisotropic torus* in $GL_2(\mathbf{F}_p)$.

EXERCISE 5.2. Show that $\det(\theta_a) = N(a)$ for all $a \in \mathbf{F}_{p^2}$.

It follows that the norm one elements of $\mathbf{F}_{p^2}^\times$ map into $SL_2(\mathbf{F}_p)$. Note that the map μ from the image of $\mathbf{F}_{p^2}^\times$ in $GL_2(\mathbf{F}_p)$ to $GL_2(\mathbf{F}_{p^2})$ defined by

$$\mu \begin{pmatrix} x & y \\ Dy & x \end{pmatrix} = \begin{pmatrix} x + y\sqrt{D} & 0 \\ 0 & x - y\sqrt{D} \end{pmatrix}$$

is an isomorphism of $\mathbf{F}_{p^2}^\times$ onto a diagonal subgroup of $GL_2(\mathbf{F}_{p^2})$ which preserves the determinant.

CHAPTER III

Representations of finite groups

1. Basic definitions

Let G be a finite group. A representation of G on a vector space V is a pair (π, V) where V is a complex vector space and π is a homomorphism $G \rightarrow GL(V)$. The dimension of V is called the degree of the representation (π, V) . From now on, we will assume all representations to be of finite degree. If (π, V) and (τ, U) are two representations of G , then a linear map $\phi : U \rightarrow V$ is called a homomorphism of G -modules if

$$\phi(\tau(g)u) = \pi(g)\phi(u) \text{ for all } u \in U.$$

EXERCISE 1.1. If (π, V) is a representation of G , define a $\mathbf{C}[G]$ -module structure on V . Show that the category of representations of G is equivalent to the category of $\mathbf{C}[G]$ -modules.

2. Induced representations

Let H be a subgroup of G . Given a representation (π, V) of H the induced representation of G is the representation (π^G, V^G) where

$$V^G = \{f : G \rightarrow V \mid f(hg) = \pi(h)f(g) \text{ for all } h \in H, g \in G\}.$$

The action of G on such functions is by *right translation*

$$(\pi^G(g)f)(x) = f(xg).$$

Now suppose that (τ, U) is a representation of G and (π, V) is a representation of H . Because $H \subset G$, we can regard U as a representation of H by restricting the homomorphism $G \rightarrow GL(U)$ to H . Denote this representation as U_H . Given $\phi \in \text{Hom}_G(U, V^G)$ set

$$\tilde{\phi}(u) = \phi(u)(1) \text{ for each } u \in U.$$

EXERCISE 2.1. The map $\tilde{\phi} : U \rightarrow V$ is a homomorphism of H -modules.

THEOREM 2.2 (Frobenius reciprocity). *The map $\phi \mapsto \tilde{\phi}$ induces an isomorphism*

$$\text{Hom}_G(U, V^G) \xrightarrow{\sim} \text{Hom}_H(U_H, V).$$

PROOF. For $\psi \in \text{Hom}_H(U_H, V)$ define $\tilde{\psi} : U \rightarrow V^G$ by

$$\tilde{\psi}(u)(x) = \psi(\tau(x)u) \text{ for each } u \in U \text{ and } x \in G.$$

EXERCISE 2.3. For all $h \in H$, $\tilde{\psi}(u)(hx) = \pi(h)\tilde{\psi}(u)(x)$. Therefore, $\tilde{\psi}(u) \in V^G$.

EXERCISE 2.4. The map $\tilde{\psi} : U \rightarrow V^G$ is a homomorphism of G -modules.

EXERCISE 2.5. For all $\phi \in \text{Hom}_G(U, V^G)$, $\tilde{\phi} = \phi$, and for all $\psi \in \text{Hom}_H(U_H, V)$, $\tilde{\tilde{\psi}} = \psi$.

Therefore the maps $\phi \mapsto \tilde{\phi}$ and $\psi \mapsto \tilde{\tilde{\psi}}$ are mutual inverses. \square

3. Mackey's theorem

We present a beautiful and intricate theorem on induced representations due to George W. Mackey. Let G be a finite group. Let H_1 and H_2 be subgroups. Let (π_1, V_1) and (π_2, V_2) be representations of H_1 and H_2 respectively. For $f : G \rightarrow V_1$, and $\Delta : G \rightarrow \text{Hom}_{\mathbb{C}}(V_1, V_2)$, define a convolution $\Delta * f : G \rightarrow V_2$ by

$$(\Delta * f)(x) = \frac{1}{|G|} \sum_{g \in G} \Delta(xg^{-1})(f(g)).$$

Let D be the set of all functions $\Delta : G \rightarrow \text{Hom}_{\mathbb{C}}(V_1, V_2)$ satisfying

$$\Delta(h_2gh_1) = \pi_2(h_2) \circ \Delta(g) \circ \pi_1(h_1)$$

for all $h_1 \in H_1$, $h_2 \in H_2$ and $g \in G$.

EXERCISE 3.1. Show that if $\Delta \in D$ and $f_1 \in V_1^G$ then $\Delta * f_1 \in V_2^G$.

EXERCISE 3.2. Show that the map $L_\Delta : V_1^G \rightarrow V_2^G$ defined by $f_1 \mapsto \Delta * f_1$ is a homomorphism of G -modules.

THEOREM 3.3 (Mackey). *The map $\Delta \mapsto L_\Delta$ is an isomorphism from $D \rightarrow \text{Hom}_G(V_1^G, V_2^G)$.*

PROOF. We construct an inverse mapping $\text{Hom}_G(V_1^G, V_2^G) \rightarrow D$. For this, let us define a collection $f_{g,v}$ of elements in V_1^G indexed by $g \in G$ and $v \in V_1$:

$$f_{g,v}(x) = \begin{cases} \pi_1(h)v & \text{if } x = hg, h \in H_1 \\ 0 & \text{if } x \notin H_1g. \end{cases}$$

EXERCISE 3.4. Show that for every $v \in V_1$, we have

$$\Delta(g)(v) = [G : H_1]L_\Delta(f_{g^{-1},v})(1).$$

The above equation can be turned around to define, for each $L : \text{Hom}_G(V_1^G, V_2^G)$ a function $\Delta \in D$.

EXERCISE 3.5. Show that if $L \in \text{Hom}_G(V_1, V_2)$ then $\Delta : G \rightarrow \text{Hom}_C(V_1, V_2)$ defined by

$$\Delta_L(g)(v) = [G : H_1]L(f_{g^{-1},v})(1)$$

is in D .

EXERCISE 3.6. Check that the maps $\Delta \mapsto \Delta_L$ and $L \mapsto L_\Delta$ are inverses of each other.

□

CHAPTER IV

Some representations of $GL_2(\mathbf{F}_p)$

1. Conjugacy classes in $GL_2(\mathbf{F}_p)$

Given a matrix $\begin{pmatrix} a & b \\ c & d \end{pmatrix}$ in $GL_2(\mathbf{F}_p)$ consider its characteristic polynomial

$$\lambda^2 - (a + d)\lambda + (ad - bc).$$

EXERCISE 1.1. If the roots (λ_1, λ_2) are distinct in \mathbf{F}_p then the matrix is conjugate to $\begin{pmatrix} \lambda_1 & 0 \\ 0 & \lambda_2 \end{pmatrix}$ and to $\begin{pmatrix} \lambda_2 & 0 \\ 0 & \lambda_1 \end{pmatrix}$.

EXERCISE 1.2. If the roots (λ_1, λ_2) are not in \mathbf{F}_p then they are in \mathbf{F}_{p^2} , they are distinct of the form $\lambda_1 = \alpha + \beta\sqrt{D}$ and $\lambda_2 = \alpha - \beta\sqrt{D}$, with $\alpha, \beta \in \mathbf{F}_p$, where D is as in Chapter II, Section 5.

EXERCISE 1.3. * In the case of Exercise 1.2, the matrix is conjugate to $\begin{pmatrix} \alpha & D\beta \\ \beta & \alpha \end{pmatrix}$ and $\begin{pmatrix} \alpha & -D\beta \\ \beta & \alpha \end{pmatrix}$ in $GL_2(\mathbf{F}_p)$.

EXERCISE 1.4. If $\lambda_1 = \lambda_2$ then, either the matrix is $\begin{pmatrix} \lambda_1 & 0 \\ 0 & \lambda_1 \end{pmatrix}$ or it is conjugate to $\begin{pmatrix} \lambda_1 & 1 \\ 0 & \lambda_1 \end{pmatrix}$ in $GL_2(\mathbf{F}_p)$.

To summarise, the conjugacy classes in $GL_2(\mathbf{F}_p)$ are as follows:

- (1) $(p - 1)$ classes of the form $\begin{pmatrix} \lambda & 0 \\ 0 & \lambda \end{pmatrix}$, with $\lambda \in \mathbf{F}_p^\times$.
- (2) $(p - 1)$ classes of the form $\begin{pmatrix} \lambda & 1 \\ 0 & \lambda \end{pmatrix}$, with $\lambda \in \mathbf{F}_p^\times$.
- (3) $\frac{1}{2}(p - 1)(p - 2)$ classes of the form $\begin{pmatrix} \lambda_1 & 0 \\ 0 & \lambda_2 \end{pmatrix}$ with $\lambda_1 \neq \lambda_2$.
- (4) $\frac{1}{2}(p^2 - p)$ classes of the form $\begin{pmatrix} \alpha & D\beta \\ \beta & \alpha \end{pmatrix}$, with $\alpha, \beta \in \mathbf{F}_p$, and $\beta \neq 0$.

In all, there are

$$(1.5) \quad (p-1) + (p-1) + \frac{p^2-p}{2} + \frac{(p-1)(p-2)}{2}$$

conjugacy classes.

2. Subgroup of upper-triangular matrices

Let B be the subgroup of $GL_2(\mathbf{F}_p)$ consisting of invertible upper triangular matrices. Let N be the subgroup of upper triangular matrices with 1's along the diagonal. Let T be the subgroup of invertible diagonal matrices.

EXERCISE 2.1. Show that

- (1) Every element $b \in B$ can be written in a unique way as $b = tn$, with $t \in T$ and $n \in N$.
- (2) N is a normal subgroup of B .
- (3) $B/N \cong T$.

$$\text{Let } s = \begin{pmatrix} 0 & -1 \\ 1 & 0 \end{pmatrix}.$$

PROPOSITION 2.2 (Bruhat decomposition).

$$GL_2(\mathbf{F}_p) = B \cup BsB, \text{ a disjoint union.}$$

Note that B is really a double coset $B1B$. So Proposition 2.2 really tells us that the double coset space $B \backslash GL_2(\mathbf{F}_p) / B$ has two elements and that $\{1, s\}$ is a complete set of representatives for these double cosets.

PROOF. A matrix $\begin{pmatrix} a & b \\ c & d \end{pmatrix}$ lies in B if and only if $c = 0$. If $c \neq 0$, then

$$\begin{pmatrix} a & b \\ c & d \end{pmatrix} = \begin{pmatrix} 1 & a/c \\ 0 & 1 \end{pmatrix} s \begin{pmatrix} c & d \\ 0 & ad/c - b \end{pmatrix} \in BsB.$$

□

3. Induced representations

Given characters χ_1 and χ_2 of \mathbf{F}_p^\times , we get a character χ of T by

$$\chi \begin{pmatrix} y_1 & 0 \\ 0 & y_2 \end{pmatrix} = \chi_1(y_1)\chi_2(y_2).$$

We extend χ to a character of B by letting N lie in the kernel. Thus

$$(3.1) \quad \chi \begin{pmatrix} y_1 & x \\ 0 & y_2 \end{pmatrix} = \chi_1(y_1)\chi_2(y_2).$$

Let $I(\chi_1, \chi_2)$ be the representation of $GL_2(\mathbf{F}_p)$ induced from this character of B .

PROPOSITION 3.2. *Let χ_1, χ_2, μ_1 and μ_2 be characters of \mathbf{F}_p^\times . Then*

$$\dim \text{Hom}_{GL_2(\mathbf{F}_p)}(I(\chi_1, \chi_2), I(\mu_1, \mu_2)) = e_1 + e_s,$$

where,

$$e_1 = \begin{cases} 1 & \text{if } \chi_1 = \mu_1 \text{ and } \chi_2 = \mu_2, \\ 0 & \text{otherwise,} \end{cases}$$

and

$$e_s = \begin{cases} 1 & \text{if } \chi_1 = \mu_2 \text{ and } \chi_2 = \mu_1, \\ 0 & \text{otherwise.} \end{cases}$$

PROOF. Let χ and μ be the characters of B obtained from the pairs χ_1, χ_2 and μ_1, μ_2 respectively as in (3.1). We regard χ and μ as one-dimensional representations of B acting on the space \mathbf{C} . We may identify $\text{Hom}_{\mathbf{C}}(\mathbf{C}, \mathbf{C})$ with \mathbf{C} as well. Then, using Mackey's theorem, we see that we must compute the dimension of the space of functions $\Delta : GL_2(\mathbf{F}_p) \rightarrow \mathbf{C}$ such that

$$(3.3) \quad \Delta(b_2gb_1) = \mu(b_2)\Delta(g)\chi(b_1), \quad b_i \in B.$$

It follows from the Bruhat decomposition that Δ is completely determined by its values at 1 and s .

Taking $g = 1$ in (3.3), we see that for any $t \in T$,

$$\mu(t)\Delta(1) = \Delta(t) = \Delta(1)\chi(t)$$

Therefore, if $\mu \neq \chi$ then $\Delta(1) = 0$. On the other hand, if $\mu = \chi$, let Δ_1 be the function such that

$$\Delta_1(b) = \chi(b) \text{ for all } b \in B,$$

and whose restriction to BsB is zero. If $e_1 = 0$, we take $\Delta_1 \equiv 0$.

Taking $g = s$ in (3.3), we see that for any $t \in T$,

$$\mu(t)\Delta(s) = \Delta(ts) = \Delta(s(s^{-1}ts)) = \Delta(s)\chi(s^{-1}ts).$$

EXERCISE 3.4. $s^{-1} \begin{pmatrix} t_1 & 0 \\ 0 & t_2 \end{pmatrix} s = \begin{pmatrix} t_2 & 0 \\ 0 & t_1 \end{pmatrix}.$

Therefore, if $\mu_1 \neq \chi_2$ or $\mu_2 \neq \chi_1$ then $\Delta(s) = 0$. On the other hand, if $\mu_1 = \chi_2$ and $\mu_2 = \chi_1$, let Δ_s be the function such that

$$\Delta_s(b_2sb_1) = \chi(b_1)\mu(b_2) \text{ for all } b_1, b_2 \in B,$$

and whose restriction to B is 0. If $e_s = 0$, we take $\Delta_s \equiv 0$.

An arbitrary functions satisfying (3.3) can be expressed as a linear combination of Δ_1 and Δ_s , so we see that the dimension of the space of such functions must be $e_1 + e_s$. \square

THEOREM 3.5. *Let χ_1, χ_2, μ_1 and μ_2 be characters of \mathbf{F}_p^\times . Then $I(\chi_1, \chi_2)$ is an irreducible representation of degree $p + 1$ of $GL_2(\mathbf{F}_p)$ unless $\chi_1 = \chi_2$, in which case it is a direct sum of two irreducible representations having degrees 1 and p . We have*

$$I(\chi_1, \chi_2) \cong I(\mu_1, \mu_2)$$

if and only if either

$$(3.6) \quad \chi_1 = \mu_1 \text{ and } \chi_2 = \mu_2$$

or else

$$(3.7) \quad \chi_1 = \mu_2 \text{ and } \chi_2 = \mu_1.$$

PROOF. Apply Proposition 3.2 with $\chi_1 = \mu_1$ and $\chi_2 = \mu_2$. We see that

$$\dim \text{End}_{GL_n(\mathbf{F}_p)}(I(\chi_1, \chi_2)) = \begin{cases} 1 & \text{if } \chi_1 \neq \chi_2, \\ 2 & \text{if } \chi_1 = \chi_2. \end{cases}$$

Recall that if (π, V) is a representation of a finite group G and V is a direct sum of distinct irreducible representations π_1, \dots, π_h with multiplicities m_1, \dots, m_h and with degrees d_1, \dots, d_h respectively, then the dimension of $\text{End}_G(V)$ is $\sum m_i d_i^2$. Hence $I(\chi_1, \chi_2)$ is irreducible if $\chi_1 \neq \chi_2$, otherwise it is a direct sum of two irreducible representations because $2 = 1^2 + 1^2$ is the only way of writing 2 as a sum of non-zero multiples of more than one non-zero squares.

Because the index of B in $GL_2(\mathbf{F}_p)$ is $p + 1$, the dimension of $I(\chi_1, \chi_2)$ is always $p + 1$. If $\chi_1 = \chi_2$, the representation of $GL_2(\mathbf{F}_p)$ generated by the function $f(g) = \chi_1(\det(g))$ clearly satisfies $f(bg) = \chi(b)f(g)$ for all $b \in B$ and $g \in G$. Therefore $f \in I(\chi_1, \chi_2)$. Moreover, $(g \cdot f)(x) = \chi_1(\det(g))f$. Therefore the one-dimensional subspace spanned by f is invariant under the action of G , hence forms a one-dimensional representation of G . The other component is therefore p -dimensional.

If $\chi_1 \neq \chi_2$ then, $I(\chi_1, \chi_2)$ is irreducible. By Proposition 3.2 there exists a non-zero element in $\text{Hom}(I(\chi_1, \chi_2), I(\mu_1, \mu_2))$ if and only if $\chi_1 = \mu_1$ and $\chi_2 = \mu_2$ or $\chi_1 = \mu_2$ and $\chi_2 = \mu_1$. By irreducibility, these homomorphisms must be isomorphisms. This proves the second part of the theorem. \square

EXERCISE 3.8. * Find the isomorphism $I(\chi_1, \chi_2) \rightarrow I(\chi_2, \chi_1)$ explicitly, when $\chi_1 \neq \chi_2$.

To summarise, in this section, we have constructed irreducible representations of $GL_2(\mathbf{F}_p)$ corresponding to characters $\chi = (\chi_1, \chi_2)$ of T :

- (1) When $\chi_1 \neq \chi_2$, there is a unique irreducible representation of $GL_2(\mathbf{F}_p)$ of degree $p + 1$ corresponding to χ ; the irreducible representation corresponding to (χ_1, χ_2) is isomorphic to the one corresponding to (χ_2, χ_1) . We have $\frac{1}{2}(p-1)(p-2)$ irreducible representations of degree $p + 1$.
- (2) When $\chi_1 = \chi_2$, there are two irreducible representations of $GL_2(\mathbf{F}_p)$ corresponding to χ , one of degree 1 and the other of degree p . All these representations are pairwise non-isomorphic. Therefore we have $p - 1$ representations of degree 1 and $p - 1$ representations of degree p .

Recall from Schur theory, that the number of irreducible representations is the same as the number of conjugacy classes in a group. We have constructed

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

irreducible representations so far. Comparing with (1.5), we see that there remain $\frac{1}{2}(p^2 - p)$ representations left to construct.

Recall that for a group of order n whose irreducible representations are π_1, \dots, π_r of degrees d_1, \dots, d_r respectively,

$$n = d_1^2 + \dots + d_r^2.$$

EXERCISE 3.9. Show that the order of $GL_2(\mathbf{F}_p)$ is $(p^2 - 1)(p^2 - p)$.

The sum of squares of degrees of the representations that we have constructed so far is

$$\frac{1}{2}(p-1)(p-2)(p+1)^2 + (p-1)(p^2 + 1).$$

The difference between the above numbers is

$$\frac{1}{2}(p^2 - p)(p-1)^2.$$

We will see in Chapter V, Section 1 that there are $\frac{1}{2}(p^2 - p)$ irreducible representations of degree $p - 1$ which still need to be constructed.

CHAPTER V

Cuspidal representations

1. The degrees of cuspidal representations

In Chapter IV we constructed all the representations (π, V) of $GL_2(\mathbf{F}_p)$ for which

$$\mathrm{Hom}_G(V, I(\chi_1, \chi_2)) \neq 0 \text{ for some characters } \chi_1, \chi_2 \in \widehat{\mathbf{F}_p^\times}.$$

Thus for the representations that remain,

$$(1.1) \quad \mathrm{Hom}_G(V, I(\chi_1, \chi_2)) = 0 \text{ for all characters } \chi_1, \chi_2 \in \widehat{\mathbf{F}_p^\times}.$$

Representations (π, V) satisfying (1.1) are known as the *cuspidal* representations of $GL_2(\mathbf{F}_p)$. By Frobenius reciprocity (Section 2), we have

$$\mathrm{Hom}_B(V, \chi) = 0 \text{ for all characters } \chi : B \rightarrow \mathbf{C}^\times \text{ such that } \chi|_N \equiv 1.$$

Given a representation (π, V) of any group G , let V^* be the dual space $\mathrm{Hom}_{\mathbf{C}}(V, \mathbf{C})$ of V . Let π^* be the representation of G on V^* given by

$$(\pi^*(g)\xi)(\mathbf{v}) = \xi(\pi(g^{-1})\mathbf{v}).$$

The representation (π^*, V^*) is called the *contragredient* of (π, V) .

PROPOSITION 1.2. *A representation (π, V) of $GL_2(\mathbf{F}_p)$ is cuspidal if and only if there exists no non-zero vector $\xi \in V^*$ such that*

$$(1.3) \quad \pi^*(n)\xi = \xi \text{ for all } n \in N.$$

PROOF. Suppose (π, V) is not cuspidal. Then there exists a non-zero element $\xi \in \mathrm{Hom}_B(V, \chi)$ for some $\chi : B \rightarrow \mathbf{C}^\times$ such that $\chi|_N \equiv 1$. Such a ξ can be regarded as an element of V^* . We have, for any $n \in N$ and $\mathbf{v} \in V$,

$$\begin{aligned} (\pi^*(n)\xi)(\mathbf{v}) &= \xi(\pi(n^{-1})\mathbf{v}) \\ &= \xi(\chi(n)\mathbf{v}) \\ &= \xi(\mathbf{v}), \end{aligned}$$

so that ξ satisfies (1.3).

Conversely, look at the space $V^*(N)$ of all vectors in V^* satisfying (1.3). This space is preserved under the action of T (since $tNt^{-1} = N$ for all $t \in T$). Therefore, one can write

$$V^*(N) = \bigoplus_{\chi \in \widehat{T}} V^*(N)_\chi,$$

where $V^*(N)_\chi$ is the space of vectors $\mathbf{v} \in V^*(N)$ which transform under T by χ . If $V^*(N) \neq 0$, then there exists χ such that $V^*(N)_\chi \neq 0$. For this χ it $\text{Hom}_B(V, \chi) \neq 0$, from which it follows that (π, V) is not cuspidal. \square

COROLLARY 1.4. *The degree of a cuspidal representation is always a multiple of $(p - 1)$.*

PROOF. Suppose that (π, V) is a cuspidal representation. For each $a \in \mathbf{F}_p$, let V_a^* be the space of all $\xi \in V^*$ such that

$$\pi^* \begin{pmatrix} 1 & x \\ 0 & 1 \end{pmatrix} \xi = \psi(ax)\xi.$$

Then the map

$$\xi \mapsto \pi^* \begin{pmatrix} t & 0 \\ 0 & 1 \end{pmatrix} \xi$$

is an isomorphism of $V^*(a)$ with $V^*(ta)$ for all $t \in \mathbf{F}_p^\times$. Hence for $a \neq 0$, the $p - 1$ spaces $V^*(a)$ have the same dimension. The space $V^*(a)$ is just $V^*(N)$, hence is trivial. Therefore the dimension of V^* , hence the degree of V must be a multiple of $p - 1$. \square

From Corollary 1.4 and the discussion at the end of Section 3 it follows that besides the representations constructed in that section, there are exactly $\frac{1}{2}(p^2 - p)$ irreducible cuspidal representations, each of degree $p - 1$. These representations are constructed in Section 3.

2. A presentation of $SL_2(\mathbf{F}_p)$

THEOREM 2.1. *Let F be a field and S be the group generated by elements $t(y)$, $n(z)$ and s with $y \in F^\times$ and $z \in F$, subject to the following relations*

$$(2.2) \quad t(y_1)t(y_2) = t(y_1y_2), \quad n(z_1)n(z_2) = n(z_1 + z_2),$$

$$(2.3) \quad t(y)n(z)t(y^{-1}) = n(z^2y), \quad st(y)s = t(-y^{-1}) \text{ and}$$

$$(2.4) \quad \text{for } z \neq 0, \quad sn(z)s = t(-z^{-1})n(-z)sn(-z^{-1}).$$

Then S is isomorphic to $SL_2(F)$. In this isomorphism,

$$t(y) \mapsto \begin{pmatrix} y & 0 \\ 0 & y^{-1} \end{pmatrix}, \quad n(z) \mapsto \begin{pmatrix} 1 & z \\ 0 & 1 \end{pmatrix}, \quad s \mapsto \begin{pmatrix} 0 & 1 \\ -1 & 0 \end{pmatrix}.$$

What this means is that S contains the elements $t(y)$, $n(z)$ and s as described above and if S' is another group containing the elements $t'(y)$, $n'(z)$ and s' satisfying the same equations (2.2-2.4), then there exists a unique homomorphism $\phi : S \rightarrow S'$ such that $t'(y) = \phi(t(y))$, $n'(z) = \phi(n(z))$ and $s' = \phi(s)$.

PROOF. Let

$$t'(y) = \begin{pmatrix} y & 0 \\ 0 & y^{-1} \end{pmatrix}, \quad n'(z) = \begin{pmatrix} 1 & z \\ 0 & 1 \end{pmatrix}, \quad s' = \begin{pmatrix} 0 & 1 \\ -1 & 0 \end{pmatrix} \in SL_2(F).$$

These elements satisfy the relations (2.2-2.4), so by the universal property of S , there is a homomorphism $\phi : S \rightarrow SL_2(F)$ such that $\phi(t(y)) = t'(y)$, etc., and what we must show is that ϕ is an isomorphism. We will accomplish this by constructing an inverse map $\psi : SL_2(F) \rightarrow S$. Define

$$\psi \begin{pmatrix} a & b \\ c & d \end{pmatrix} = \begin{cases} n(a/c)t(-c^{-1})sn(d/c) & \text{if } c \neq 0 \\ t(a)n(b/a) & \text{if } c = 0. \end{cases}$$

We check that ψ is a homomorphism; that is if

$$\begin{pmatrix} a & b \\ c & d \end{pmatrix} \begin{pmatrix} A & B \\ C & D \end{pmatrix} = \begin{pmatrix} \alpha & \beta \\ \gamma & \delta \end{pmatrix}$$

then we must check that

$$(2.5) \quad \psi \begin{pmatrix} a & b \\ c & d \end{pmatrix} \psi \begin{pmatrix} A & B \\ C & D \end{pmatrix} = \psi \begin{pmatrix} \alpha & \beta \\ \gamma & \delta \end{pmatrix}.$$

We leave out these checks. The reader may do so himself, or look at [Bum97] (from which most of these notes are taken anyway). Since ϕ and ψ are homomorphisms and $\psi \circ \phi$ is the identity map on generators, it must be the identity map. It follows that ϕ is injective.

EXERCISE 2.6. Check that ϕ is surjective.

Therefore ϕ is an isomorphism. \square

3. The Weil representation

PROPOSITION 3.1. *There exists a representation $\omega : SL_2(\mathbf{F}_p) \rightarrow GL(\mathbf{C}[\mathbf{F}_{p^2}])$ such that for all $\Phi \in \mathbf{C}[\mathbf{F}_{p^2}]$,*

$$\begin{aligned} \left(\omega \begin{pmatrix} a & 0 \\ 0 & a^{-1} \end{pmatrix} \Phi \right) (x) &= \Phi(ax), \\ \left(\omega \begin{pmatrix} 1 & z \\ 0 & 1 \end{pmatrix} \Phi \right) (x) &= \psi(zN(x))\Phi(x), \text{ and} \\ \left(\omega \begin{pmatrix} 0 & 1 \\ -1 & 0 \end{pmatrix} \Phi \right) (x) &= -p\widehat{\Phi}(-\bar{x}). \end{aligned}$$

By Theorem 2.1, it suffices to check that the images of the generators of $SL_2(\mathbf{F}_p)$ under ω satisfy relations (2.2-2.4). We leave out the details of this proof. The second formula in (2.3) corresponds to the Fourier inversion formula for \mathbf{F}_{p^2} . The relation corresponding to (2.4) is relatively difficult, while all the others are straightforward. The details of the former may be found in Section 4.1 of [Bum97].

Let χ be a character of $\mathbf{F}_{p^2}^\times$ such that $\chi \neq \chi' \circ N$ for some character χ' of \mathbf{F}_p^\times (here N denotes the norm map $\mathbf{F}_{p^2} \rightarrow \mathbf{F}_p$).

EXERCISE 3.2. Show that there are $p^2 - p$ such characters.

Define

$$W_\chi = \{\Phi \in \mathbf{C}[\mathbf{F}_{p^2}] \mid \Phi(yx) = \chi(y)^{-1}\Phi(x) \text{ for all } y \in (\mathbf{F}_{p^2}^\times)_1\}.$$

Here

$$(\mathbf{F}_{p^2}^\times)_1 = \{y \in \mathbf{F}_{p^2}^\times \mid N(y) = 1\}.$$

EXERCISE 3.3. W_χ is preserved by the action of ω of $SL_2(\mathbf{F}_p)$ on W_χ (for this one must check that for each element g of a generating set of $SL_2(\mathbf{F}_p)$, $\omega(g)$ maps a function $\Phi \in W_\chi$ to another function in W_χ).

Therefore, ω gives a representation (π_χ, W_χ) for each such χ . This is called the Weil representation of corresponding to χ .

EXERCISE 3.4. Show that the dimension of W_χ is $p - 1$. Note that the hypothesis that χ can not be written in the form $\chi' \circ N$ is needed here.

Each matrix x in $GL_2(\mathbf{F}_p)$ can be written in a unique way as a product of $\begin{pmatrix} \det(x) & 0 \\ 0 & 1 \end{pmatrix}$ and a matrix in $SL_2(\mathbf{F}_p)$. Extend π_χ to $GL_2(\mathbf{F}_p)$ by extending ω to $GL_2(\mathbf{F}_p)$, requiring that for each $a \in \mathbf{F}_p^\times$,

$$(3.5) \quad \left(\omega \begin{pmatrix} a & 0 \\ 0 & 1 \end{pmatrix} \Phi \right) (x) = \chi(a)\Phi(x),$$

where $b \in \mathbf{F}_{p^2}^\times$ is chosen so that $N(b) = a$.

EXERCISE 3.6. Check that the right hand side of (3.5) does not depend on the choice of b .

For this extended function to be a homomorphism of groups, it is necessary that, for all $a, a' \in \mathbf{F}_p^\times$ and all $g, g' \in SL_2(\mathbf{F}_p)$,

$$(3.7) \quad \omega \left(\begin{pmatrix} a & 0 \\ 0 & 1 \end{pmatrix} g \begin{pmatrix} a' & 0 \\ 0 & 1 \end{pmatrix} g' \right) = \omega \left(\begin{pmatrix} a & 0 \\ 0 & 1 \end{pmatrix} g \right) \omega \left(\begin{pmatrix} a' & 0 \\ 0 & 1 \end{pmatrix} g' \right).$$

But

$$\begin{pmatrix} a & 0 \\ 0 & 1 \end{pmatrix} g \begin{pmatrix} a' & 0 \\ 0 & 1 \end{pmatrix} g' = \begin{pmatrix} aa' & 0 \\ 0 & 1 \end{pmatrix} \left[\begin{pmatrix} a'^{-1} & 0 \\ 0 & 1 \end{pmatrix} g \begin{pmatrix} a' & 0 \\ 0 & 1 \end{pmatrix} g' \right],$$

and $\begin{pmatrix} a'^{-1} & 0 \\ 0 & 1 \end{pmatrix} g \begin{pmatrix} a' & 0 \\ 0 & 1 \end{pmatrix} g' \in SL_2(\mathbf{F}_p)$.

EXERCISE 3.8. Using this to expand both sides of (3.7) in terms of (3.5), show that it is sufficient to check that for each $a \in \mathbf{F}_p^\times$, $\Phi \in \mathbf{C}[\mathbf{F}_{p^2}]$ and each generator g of $SL_2(\mathbf{F}_p)$,

$$\omega \left(\begin{pmatrix} a & 0 \\ 0 & 1 \end{pmatrix} \right) \omega(g) \left(\begin{pmatrix} a & 0 \\ 0 & 1 \end{pmatrix} \right)^{-1} = \omega \left(\begin{pmatrix} a & 0 \\ 0 & 1 \end{pmatrix} g \begin{pmatrix} a & 0 \\ 0 & 1 \end{pmatrix}^{-1} \right).$$

The latter check is straightforward.

PROPOSITION 3.9. *The Weil representation (π_χ, W_χ) is cuspidal.*

PROOF. We will show that W_χ contains no non-zero vectors fixed by N . For this, suppose that Φ_0 is a vector fixed by N . $\Phi_0(0) = 0$ (this is true for any element of W_χ , a fact which appears in the solution to Exercise 3.4—so here again the hypothesis $\chi \neq \chi' \circ N$ is used). On the other hand, if $x \in \mathbf{F}_{p^2}^\times$, then choose $z \in \mathbf{F}_p$ so that $\psi(zN(x)) \neq 1$. Then, because

$$\Phi_0(x) = \left(\omega \left(\begin{pmatrix} 1 & z \\ 0 & 1 \end{pmatrix} \right) \Phi_0 \right) (x) = \psi(zN(x)) \Phi_0(x),$$

we have $\Phi_0(x) = 0$. □

Clearly, any sub-representation of a cuspidal representation is also cuspidal. Therefore, by Corollary 1.4 (π_χ, W_χ) is simple for each χ of the type considered above.

LEMMA 3.10. *Let χ and η be two characters of $\mathbf{F}_{p^2}^\times$ as above. If the representations (π_χ, W_χ) and (π_η, W_η) are isomorphic, then either*

$\chi = \eta$ or $\chi = \eta \circ F$, where F is the Frobenius automorphism $\mathbf{F}_{p^2}^\times \rightarrow \mathbf{F}_{p^2}^\times$ (see Section 3).

PROOF. Note that for any $a \in \mathbf{F}_{p^2}^\times$,

$$\begin{pmatrix} a & 1 \\ 0 & a \end{pmatrix} = \begin{pmatrix} a^2 & 0 \\ 0 & 1 \end{pmatrix} \begin{pmatrix} a^{-1} & 0 \\ 0 & a \end{pmatrix} \begin{pmatrix} 1 & a^{-1} \\ 0 & 1 \end{pmatrix}.$$

For each $y \in \mathbf{F}_p^\times$, pick an element \tilde{y} such that $N(\tilde{y}) = y$.

EXERCISE 3.11. Show that

$$\left(\pi_\chi \begin{pmatrix} a & 1 \\ 0 & a \end{pmatrix} \Phi \right) (x) = \chi(a) \psi(a^{-1}N(x)) \Phi(x).$$

Let Φ_y be the unique function in W_χ for which $\Phi(\tilde{y}) = 1$ and $\Phi(\tilde{z}) = 0$ for all $z \neq y$ in \mathbf{F}_p^\times . The functions Φ_y , as y ranges over \mathbf{F}_p^\times form a basis of W_χ . Therefore

$$\mathrm{tr} \left(\pi_\chi \begin{pmatrix} a & 1 \\ 0 & a \end{pmatrix} \right) = \sum_{y \in \mathbf{F}_p^\times} \left(\pi_\chi \begin{pmatrix} a & 1 \\ 0 & a \end{pmatrix} \Phi_y \right) (\tilde{y}).$$

EXERCISE 3.12. Show that the sum of the right hand side of the above equation is $-\chi(a)$.

EXERCISE 3.13. Show that if χ and η are two characters of $\mathbf{F}_{p^2}^\times$, then their restrictions to \mathbf{F}_p^\times are equal if and only if either $\chi = \eta$ or $\chi = \eta \circ F$.

If (π_χ, W_χ) and (π_η, W_η) were isomorphic, then we would have

$$\mathrm{tr} \left(\pi_\chi \begin{pmatrix} a & 1 \\ 0 & a \end{pmatrix} \right) = \mathrm{tr} \left(\pi_\eta \begin{pmatrix} a & 1 \\ 0 & a \end{pmatrix} \right),$$

which by Exercise 3.13 would mean that either $\chi = \eta$ or $\chi = \eta \circ F$. \square

Bibliography

- [Bum97] Daniel Bump. *Automorphic forms and representations*, volume 55 of *Cambridge Studies in Advanced Mathematics*. Cambridge University Press, Cambridge, 1997.
- [DL76] P. Deligne and G. Lusztig. Representations of reductive groups over finite fields. *Ann. of Math. (2)*, 103(1):103–161, 1976.
- [Gre55] J. A. Green. The characters of the finite general linear groups. *Trans. Amer. Math. Soc.*, 80:402–447, 1955.
- [IR90] Kenneth Ireland and Michael Rosen. *A classical introduction to modern number theory*, volume 84 of *Graduate Texts in Mathematics*. Springer-Verlag, New York, second edition, 1990.
- [Jor07] Herbert E. Jordan. Group-characters of various types of linear groups. *Amer. J. Math.*, 29:387–405, 1907.
- [Lus84] George Lusztig. Characters of reductive groups over finite fields. In *Proceedings of the International Congress of Mathematicians, Vol. 1, 2 (Warsaw, 1983)*, pages 877–880, Warsaw, 1984. PWN.
- [Sch07] Issai Schur. Untersuchungen über die Darstellung der endlichen Gruppen durch gebrochene lineare Substitutionen. *J. Reine Angew. Math.*, 132, 1906-07.
- [Ser73] J.-P. Serre. *A course in arithmetic*. Springer-Verlag, New York, 1973. Translated from the French, Graduate Texts in Mathematics, No. 7.
- [Spr70] T. A. Springer. Cusp forms for finite groups. In *Seminar on Algebraic Groups and Related Finite Groups (The Institute for Advanced Study, Princeton, N.J., 1968/69)*, Lecture Notes in Mathematics, Vol. 131, pages 97–120. Springer, Berlin, 1970.
- [Wei64] André Weil. Sur certains groupes d'opérateurs unitaires. *Acta Math.*, 111:143–211, 1964.