Niels Ketelaars

The irreducible mod p representations of $\mathbf{GL}_2(\mathbf{F}_p)$

Bachelor thesis

June 25, 2021

Thesis supervisor: dr. M.F.A. Steinmetz

Leiden University
Mathematical Institute

Contents

Introduction

Representation theory is the branch of mathematics that studies groups and related algebraic structures via their actions on vector spaces. A representation of a group is nothing more than a linear action of said group on a vector space. Since its inception in the late 19th century, representation theory has found numerous applications, ranging from particle physics to number theory.

In number theory in particular, the representation theory of Galois groups is at the center of the *Langlands program*, a vast collection of conjectures and ideas relating all kinds of different types of representations, originally formulated by Robert Langlands in a letter to André Weil [Lan67]. Central to the Langlands program is the apparent connection between representations of Galois groups and the groups GL_n over certain fields. Most of Langlands' original work dealt with representations where the underlying vector space was over the field of complex numbers. In recent years, there have been strides to formulate and prove analogous statements for representations over positive characteristic fields, known as the *mod p Langlands* correspondence. The starting point was a 1994 paper by Laure Barthel and Ron Livné [BL94], in which the authors gave a partial classification of certain *irreducible* representations of the group $\mathrm{GL}_2(F)$ over $\overline{\mathbf{F}}_p$, where F is a finite extension of $\mathbf{Q}_p$, the field of *p-adic numbers*. It turns out that these can be built out of irreducible representations of a different group, namely $\mathrm{GL}_2(\mathbf{F}_q)$, for q a power of p. In 2003, Christophe Breuil published a paper [Bre03] completing the classification in the case $F = \mathbf{Q}_p$, and used it to formulate and prove a version of the mod p Langlands correspondence for $\mathrm{GL}_2(\mathbf{Q}_p)$.

As mentioned, the irreducible representations of $\mathrm{GL}_2(\mathbf{F}_q)$ over fields of characteristic p were the starting point for creating representations of $\mathrm{GL}_2(F)$, and it is therefore no surprise that the first proposition appearing in Barthel and Livné's paper is a classification of these representations. Our goal in this thesis will be to prove this classification and hopefully along the way expose the reader to the different ideas and techniques that are still important to this day in representation theory. Barthel and Livné's proof is only a few lines long. This is because the classification can

be seen an easy consequence of a very general and powerful theorem from modular representation theory. Instead, we have opted for a more direct proof based on the outline given in [BR]. The author is grateful to Laurent Berger for his permission to use these notes.

In Chapter 1, we will start with a general analysis of some of the properties of the group $\mathrm{GL}_2(\mathbf{F}_q)$, including its characters and special subgroups. Chapter 2 is dedicated to introducing all the necessary representation theory. Section 2.1 deals with the basic definitions and results, including the Jordan-Hölder theorem and a few lemmas on positive characteristic representations, before moving on to the more specialized topics like contragredients and induced representations in Section 2.2 and tensor products in Section 2.3. In Chapter 3 we prove the main classification for the group $\mathrm{GL}_2(\mathbf{F}_p)$. We start off in Section 3.1 by defining the representations which will occur in the classification, the *symmetric tensor powers*, and prove they are irreducible and distinct. Then in Section 3.2, we will introduce a new type of representation, the *parabolic inductions*, which have the special property that their irreducible quotients are always a symmetric tensor power. The final steps are then taken in Section 3.3, combining the results from all the previous sections to finally prove the classification. Chapter 4 deals with generalizing the results from the previous chapter to the group $\mathrm{GL}_2(\mathbf{F}_q)$, and is structured similarly. Lastly, in Chapter 5 we define the p-adic numbers, integers and certain groups of matrices over these. We then briefly show how representations of these matrix groups are related to those of $\mathrm{GL}_n(\mathbf{F}_p)$.

1 The group GL_2

In this chapter we analyze some of the properties of the group GL_2 over a finite field that will be useful to us in the coming sections. We begin with a result from basic algebra.

LEMMA 1.0.1. Let E be a field. Then any finite subgroup of $E^\times$ is cyclic. Furthermore, if E is finite, then any homomorphism $E^\times \to E^\times$ is of the form $a \mapsto a^r$ for some integer r.

Proof. See [Lan02, Ch. IV, Theorem 1.9] for the first part. The second part follows from the first via the fact that the image of a generator g of $E^\times$ is of the form g^r, hence any element g^s gets mapped to $(g^r)^s = (g^s)^r$. □

Recall that for any prime p and prime power $q = p^n$ there is a unique field (up to isomorphism) with q elements, denoted by $\mathbf{F}_q$, which is the splitting field of $x^q - x$ over $\mathbf{F}_p = \mathbf{Z}/p\mathbf{Z}$ (see [Lan02, Ch. V, Theorem 5.1] for instance).

Next, we define some special subgroups of the group $\mathrm{GL}_2(\mathbf{F}_q)$ which will play an important role in what follows. Namely, we let $B = \left\{ \left(\begin{smallmatrix} a & b \\ 0 & d \end{smallmatrix}\right) \mid a, d \in \mathbf{F}_q^\times, b \in \mathbf{F}_q \right\}$ denote the subgroup of upper triangular matrices, $U = \left\{ \left(\begin{smallmatrix} 1 & b \\ 0 & 1 \end{smallmatrix}\right) \mid b \in \mathbf{F}_q \right\}$ the subgroup of upper triangular matrices with ones on the diagonal, and $T = \left\{ \left(\begin{smallmatrix} a & 0 \\ 0 & d \end{smallmatrix}\right) \mid a, d \in \mathbf{F}_q^\times \right\}$ the diagonal matrices. We also define the element $w = \left(\begin{smallmatrix} 0 & 1 \\ 1 & 0 \end{smallmatrix}\right)$. We have the following results regarding homomorphisms of these groups.

PROPOSITION 1.0.2. Every homomorphism $\chi \colon B \to \mathbf{F}_q^\times$ is of the form $\chi\left(\begin{smallmatrix} a & b \\ 0 & d \end{smallmatrix}\right) = a^r d^s$ for integers r, s. If we denote this homomorphism by $\chi_{r,s}$, then $\chi_{r,s} = \chi_{r',s'}$ if and only if $q-1$ divides both $r - r'$ and $s - s'$.

Proof. We have a homomorphism $\mathbf{F}_q^\times \to B$ given by $a \mapsto \left(\begin{smallmatrix} a & 0 \\ 0 & 1 \end{smallmatrix}\right)$. By Lemma 1.0.1, composing this map with χ must give a map of the form $a \mapsto a^r$, showing that $\chi\left(\begin{smallmatrix} a & 0 \\ 0 & 1 \end{smallmatrix}\right) = a^r$ for some integer r. A similar reasoning shows that $\chi\left(\begin{smallmatrix} 1 & 0 \\ 0 & d \end{smallmatrix}\right) = d^s$ for

some integer s. The subgroup U has order q, which is coprime to $\#\mathbf{F}_q^\times = q-1$, so we must have $\chi|_U = 1$. Hence for arbitrary $\left(\begin{smallmatrix} a & b \\ 0 & d \end{smallmatrix}\right) \in B$, we find that

$$\chi\begin{pmatrix} a & b \\ 0 & d \end{pmatrix} = \chi\left(\begin{pmatrix} a & 0 \\ 0 & 1 \end{pmatrix}\begin{pmatrix} 1 & 0 \\ 0 & d \end{pmatrix}\begin{pmatrix} 1 & a^{-1}b \\ 0 & 1 \end{pmatrix}\right) = a^r d^s.$$

For the second assertion, it is immediate that if $q-1|r-r', s-s'$ then $\chi_{r,s} = \chi_{r',s'}$. For the converse, assume that $\chi_{r,s} = \chi_{r',s'}$ and let a be a generator of $\mathbf{F}_q^\times$. Then $a^r = \chi_{r,s}\left(\begin{smallmatrix} a & 0 \\ 0 & 1 \end{smallmatrix}\right) = \chi_{r',s'}\left(\begin{smallmatrix} a & 0 \\ 0 & 1 \end{smallmatrix}\right) = a^{r'}$, hence $q-1|r-r'$. The same reasoning shows that $q-1|s-s'$. □

To analyze the homomorphisms of $\mathrm{GL}_2(\mathbf{F}_q)$, we need the following.

PROPOSITION 1.0.3 (Bruhat decomposition). We have that $[\mathrm{GL}_2(\mathbf{F}_q) : B] = q+1$, and $\mathrm{GL}_2(\mathbf{F}_q) = B \cup UwB$.

Proof. For the first part, note that all elements of $\mathrm{GL}_2(\mathbf{F}_q)$ are found by first picking any of the q^2-1 nonzero vectors in $\mathbf{F}_q^2$ for the first column, and then any of the q^2-q vectors not in the span of the first for the second column, giving $(q^2-1)(q^2-q)$ options. For an element of B, we can pick any nonzero values for the upper left and lower right entries, and any value for the upper right entry, giving $q(q-1)^2$ options. Hence $[G:B] = \#G/\#B = q+1$.

For the second assertion, let $g = \left(\begin{smallmatrix} a & b \\ c & d \end{smallmatrix}\right) \in \mathrm{GL}_2(\mathbf{F}_q)$. If $c = 0$ then $g \in B$, and otherwise

$$g = \begin{pmatrix} 1 & ac^{-1} \\ 0 & 1 \end{pmatrix} w \begin{pmatrix} c & d \\ 0 & b - adc^{-1} \end{pmatrix} \in UwB.$$ □

PROPOSITION 1.0.4. Every homomorphism $\chi\colon \mathrm{GL}_2(\mathbf{F}_q) \to \mathbf{F}_q^\times$ is of the form $\chi(g) = \det(g)^r$ for an integer r.

Proof. By Proposition 1.0.2 we know that $\chi|_B = \chi_{r,s}$ for some integers r, s. We first show $\chi(w) = \det(w)^r$. If $p = 2$, then since $w^2 = \left(\begin{smallmatrix} 1 & 0 \\ 0 & 1 \end{smallmatrix}\right)$, we have $\chi(w)^2 = 1$ and hence $\chi(w) = 1$. If $p \neq 2$, the matrix $S = \left(\begin{smallmatrix} -1 & 1 \\ 1 & 1 \end{smallmatrix}\right)$ is invertible and we have $w = S\left(\begin{smallmatrix} -1 & 0 \\ 0 & 1 \end{smallmatrix}\right)S^{-1}$. Thus $\chi(w) = \chi(S)\chi\left(\begin{smallmatrix} -1 & 0 \\ 0 & 1 \end{smallmatrix}\right)\chi(S)^{-1} = (-1)^r = \det(w)^r$. Now let $a \in \mathbf{F}_q^\times$ be a generator. Then we have that

$$a^r = \chi(w)\chi\begin{pmatrix} a & 0 \\ 0 & 1 \end{pmatrix}\chi(w) = \chi\left(w\begin{pmatrix} a & 0 \\ 0 & 1 \end{pmatrix}w\right) = \chi\begin{pmatrix} 1 & 0 \\ 0 & a \end{pmatrix} = a^s$$

and it follows that $q-1|r-s$. So $\chi|_B = \chi_{r,r}$, meaning that $\chi(h) = \det(h)^r$ for $h \in B$. If $g \in \mathrm{GL}_2(\mathbf{F}_q)$, but $g \notin B$, we know by Proposition 1.0.3 that we can

write $g = uwh$ for $u \in U$, $h \in B$. In this case we find $\chi(g) = \chi(u)\chi(w)\chi(h) = \det(u)^r \det(w)^r \det(h)^r = \det(g)^r$. $\square$

2 A crash course in representation theory

In this chapter we introduce the necessary results from representation theory for understanding and proving our main theorems. We start of with the basics, before moving on to the more complicated topics like induction and tensor products. Most of the material is standard and can be found in any book on representation theory, like [Ser77] and [FH04].

In the remainder of this chapter, E will denote an arbitrary field and G an arbitrary group.

§2.1 Basic definitions and results

We of course start of with the most important definition.

Definition 2.1.1. A *representation of G over E* is a pair (ρ, V), where V is a vector space over E and $\rho\colon G \to \mathrm{Aut}_E(V)$ is a group homomorphism.

In other words, it is a linear action of G on V. The dimension of the underlying vector space V will be referred to as the dimension of the representation.

Remark 2.1.2. There are a few remarks to be made about the definition above. Firstly, if the field E is clear from context or not important for the discussion, we will often speak simply of a representation of G. Secondly, while a representation is now formally a pair (ρ, V), we will often talk about 'the representation ρ' or 'the representation V' when the underlying space or the homomorphism, respectively, is clear from context.

Example 2.1.3. Suppose G acts on a set X, and denote the action by $(g, x) \mapsto g \cdot x$. Take $V = E^{(X)}$ to be the free vector space on X, consisting of finite formal

E-linear combinations of elements of X. Define a map $\rho\colon G \to \mathrm{Aut}_E(V)$ by $\rho(g)\left(\sum_{x\in X} a_x x\right) = \sum_{x\in X} a_x(g\cdot x)$. Then (ρ, V) is a representation of G. The special case when G acts on itself by left multiplication is known as the *regular representation* of G (see [Ser77, Section 2.4] for why it is so special, at least when G is finite and $E = \mathbf{C}$).

Now that we have defined a representation, the next thing is to define what subrepresentations and homomorphisms of representations should be.

Definition 2.1.4. Let (ρ, V) be a representation of G. A subspace $W \subset V$ is called *(G-)stable* if $\rho(g)W = W$ for all $g \in G$. In this case ρ gives rise to a homomorphism $\rho\colon G \to \mathrm{Aut}_E(W)$, and the pair (ρ, W) is then called a *subrepresentation* of V.

Just as with representations themselves, we will often refer to W itself as the subrepresentation. The whole space V and the trivial subspace 0 are always subrepresentations. An interesting case is when these are the only ones.

Definition 2.1.5. A representation is called *irreducible* if it has exactly 2 subrepresentations.

Note that the 0 representation is not irreducible. Irreducible representations are special because they are in some sense the 'building blocks' of all representations.

Example 2.1.6. Let G be a nontrivial finite group and let (ρ, V) be the regular representation from Example 2.1.3. Then the span of $\sum_{g\in G} g$ is a nontrivial subrepresentation, so the regular representation is not irreducible.

Lastly, we give the notion of a homomorphism between representations.

Definition 2.1.7. Let (ρ, V) and (τ, W) be representations of G. A *(G-)homomorphism* from V to W is a linear map $S\colon V \to W$ such that $S \circ \rho(g) = \tau(g) \circ S$ for all $g \in G$. An *isomorphism* is a bijective homomorphism. The space of homomorphisms is denoted by either $\mathrm{Hom}_G(V, W)$ or $\mathrm{Hom}_G(\rho, \tau)$.

We also call a linear map satisfying this condition *(G)-equivariant*. As usual, if there exists an isomorphism $V \to W$, these representations are called isomorphic, denoted as $V \cong W$. Typical problems in representation theory are to classify the irreducible representations of a finite group up to isomorphism. Our goal is of this form as well.

From now on, we will assume that all our representations are finite dimensional. The reason is that we are interested in the irreducible representations of finite groups, and an infinite dimensional representation of a finite group can never be irreducible: given a representation (ρ, V), one can pick any nonzero $v \in V$, and look at the

span of $\{\rho(g)v \mid g \in G\}$. This is a nonzero subrepresentation of V, and it is finite dimensional if G is finite.

We now briefly mention a few important consequences of the above definitions.

PROPOSITION 2.1.8. The following properties hold:

- The image and kernel of a homomorphism are subrepresentations. Furthermore, if the domain and codomain are the same representation, then the eigenspace of any eigenvalue is also a subrepresentation.
- Given a subrepresentation W of (ρ, V), the map $\bar{\rho}(g)\colon V/W \to V/W$ defined by $\bar{\rho}(g)(v \bmod W) = \rho(g)v \bmod W$ is a well-defined automorphism, giving rise to the quotient representation $(\bar{\rho}, V/W)$.
- If $S\colon V \to W$ is a G-homomorphism, then S induces a G-isomorphism $V/\ker S \to \operatorname{im} S$.

These follow from the analogous statements for modules over a ring and from the fact that a representation of G is the same as a module over the *group ring* $E[G]$ (see [Lan02, Ch. XVIII, §1]). An immediate, but important consequence of the first property is the following.

PROPOSITION 2.1.9 (Schur's lemma). Suppose V and W are representations of G, and $S\colon V \to W$ is a nonzero G-homomorphism.

- If W is irreducible, then S is surjective.
- If V is irreducible, then S is injective.
- If V and W are both irreducible, then S is an isomorphism.

Proof. The image of S is a nonzero subrepresentation of W, so $\operatorname{im} S = W$ if W is irreducible. Likewise, the kernel is a proper subrepresentation of V, so $\ker S = 0$ if V is irreducible. The last assertion follows from the previous two. □

We will continuously make use of the previous two propositions without explicitly referring back to them.

As mentioned before, the irreducible representations of a group are in some sense the building blocks of all representations. The irreducible representations making up a given representation are called its *irreducible constituents*. More precisely, let $V \neq 0$ be a representation. Define the multiset $\operatorname{Irr}(V)$ recursively as follows: if V is irreducible, $\operatorname{Irr}(V) = \{V\}$. Otherwise, by induction on the dimension it follows that any nonzero representation contains an irreducible subrepresentation, so let

$W \subset V$ be as such. Then we set $\operatorname{Irr}(V) = \{W\} \cup \operatorname{Irr}(V/W)$. The Jordan-Hölder theorem says that the resulting multiset $\operatorname{Irr}(V)$ does not depend on the choice of irreducible subrepresentation at each step. We will only need a special case of this theorem, namely when the representation has two irreducible constituents. Such a representation is said to have *length* 2. A proof of the more general statement can be found in [Eti+11, Theorem 3.7.1], albeit formulated in a slightly different way than here.

THEOREM 2.1.10 (Jordan-Hölder for length 2). Let (ρ, V) be a representation, such that it has an irreducible subrepresentation W for which V/W is likewise irreducible. Let $W' \subset V$ be any irreducible subrepresentation. Then V/W' is again irreducible, and either $W \cong W'$ and $V/W \cong V/W'$, or $W' \cong V/W$ and $V/W' \cong W$.

Proof. Consider $W \cap W'$. It is a subrepresentation of both W and W', which are irreducible. Thus if $W \cap W' \neq 0$, we must have $W = W \cap W' = W'$ and therefore also $V/W = V/W'$. If instead $W \cap W' = 0$, the natural maps $W \to V/W'$ and $W' \to V/W$ are injective, since they both have kernel $W \cap W'$. In particular the map $W' \to V/W$ is nontrivial and because V/W is irreducible, it is surjective. Hence $W' \cong V/W$, from which it also follows that $\dim(W) = \dim(V/W')$. Consequently, the injective map $W \to V/W'$ must also be surjective, so $W \cong V/W'$. □

COROLLARY 2.1.11. Let (ρ, V) be a representation of length 2. Then any quotient of V by a nontrivial proper subrepresentation is irreducible and isomorphic to an irreducible constituent of V.

Proof. Let $W' \subset V$ be a nontrivial proper subrepresentation. Let $W \subset W'$ be an irreducible subrepresentation. Then we have a nontrivial surjective map $V/W \to V/W'$, and by Theorem 2.1.10 the domain is irreducible, so the map is also injective, and therefore an isomorphism. Thus $\operatorname{Irr} V = \{W, V/W\} = \{W, V/W'\}$, so V/W' is an irreducible constituent. □

Remark 2.1.12. It is not generally true that two representations with the same irreducible constituents are isomorphic. A simple counterexample is to let $G = \mathbf{Z}/p\mathbf{Z}$ and $V = \mathbf{F}_p^2$ with the trivial action (i.e. $\rho_V(g)v = v$ for all $g \in G$ and $v \in V$), and $W = \mathbf{F}_p^2$ with the action $\rho_W(g)w = \left(\begin{smallmatrix} 1 & g \\ 0 & 1 \end{smallmatrix}\right) w$. If we let M denote the one-dimensional representation with the trivial action of G, then $\mathbf{F}_p \left(\begin{smallmatrix} 1 \\ 0 \end{smallmatrix}\right) \subset W$ is a subrepresentation isomorphic to M whose quotient is also isomorphic to M, so $\operatorname{Irr} W = \{M, M\}$. But the same is true for V, even though V and W are not isomorphic. However, the claim that the irreducible constituents determine the representation *is* true when the order of G is not divisible by the characteristic of the underlying field E. This

follows from a result known as Maschke's theorem ([Lan02, Ch. XVIII, Theorem 1.2]).

We end this section with two lemmas about representations over $\mathbf{F}_q$ of certain groups. For the first of these we require a new definition.

Definition 2.1.13. Let (ρ, V) be a representation of G. Then the space of G-*invariants* is $V^G := \{v \in V \mid \rho(g)v = v \text{ for all } g \in G\}$.

Said differently, V^G is the largest subspace that G acts trivially on.

LEMMA 2.1.14. Let H be a finite p-group and (ρ, V) a nonzero representation of H over $\mathbf{F}_q$. Then $V^H \neq 0$.

Since $0 \in V^H$, the assertion of the lemma is that there is always a nonzero vector which is fixed by every element of the group.

Proof. Because H acts on V by invertible linear transformations, it acts on $V \setminus \{0\}$. Denote by $\mathrm{Orb}(v) := \{\rho(h)v \mid h \in H\}$ and $\mathrm{Stab}(v) = \{h \in H \mid \rho(h)v = v\}$ the orbit and the stabilizer of $v \in V \setminus \{0\}$, respectively. Then $V \setminus \{0\}$ is the disjoint union of the different orbits, and hence the size of $V \setminus \{0\}$ is the sum of the orbit sizes. Since $\#(V \setminus \{0\}) = q^{\dim V} - 1$ is not divisible by p, there must be a vector $v \neq 0$ for which $\#\mathrm{Orb}(v)$ is not divisible by p. But by the orbit-stabilizer theorem, we have $\#\mathrm{Orb}(v) \cdot \#\mathrm{Stab}(v) = \#H$, so $\#\mathrm{Orb}(v)$ is a power of p. The only such power which is not divisible by p is $p^0 = 1$, which precisely means that $v \in V^H$. □

LEMMA 2.1.15. Let H be an abelian group such that every element has order dividing $q - 1$. Then any irreducible representation of H over $\mathbf{F}_q$ has dimension 1.

Proof. Suppose (ρ, V) is an irreducible representation of H over $\mathbf{F}_q$. Let $h \in H$. Because $h^q = h$, we also have $\rho(h)^q = \rho(h)$, so the minimal polynomial of $\rho(h)$ divides $x^q - x = \prod_{\alpha \in \mathbf{F}_q}(x - \alpha)$. In particular the minimal polynomial has a linear factor. By the Cayley-Hamilton theorem, the minimal polynomial divides the characteristic polynomial. Hence the latter also has a linear factor, meaning that $\rho(h)$ has an eigenvalue λ.

Because H is abelian, for any $g \in H$ we have $\rho(g)\rho(h) = \rho(h)\rho(g)$, thus $\rho(h)$ is an H-homomorphism $V \to V$. It follows that the eigenspace $\ker(\rho(h) - \lambda \cdot \mathrm{Id})$ is a nonzero subrepresentation of V, so it must be the whole space. This means that $\rho(h) = \lambda \cdot \mathrm{Id}$. Because h was arbitrary, we see that any element acts as scalar multiplication. But this implies that any subspace is stable; hence V must not have any nontrivial subspaces, showing that V is one-dimensional. □

§2.2 Contragredient and induced representations

Recall that for a vector space V over E, the dual space $V^* := \mathrm{Hom}(V, E)$ is the space of all linear functionals on V. If W is another vector space and $A\colon V \to W$ a linear map, its transpose is the map $A^\intercal\colon W^* \to V^*$ given by $A^\intercal\psi = \psi \circ A$. It has the property that for a chain of linear maps $X \xrightarrow{A} V \xrightarrow{B} W$, we have $(A \circ B)^\intercal = B^\intercal \circ A^\intercal$. Given now a representation of G, we can use the dual space the construct a new representation.

Definition 2.2.1. Let (ρ, V) be a representation of G. The *contragredient* representation is the representation (ρ^*, V^*) where ρ^* is defined by

$$\rho^*(g) = \rho(g^{-1})^\intercal.$$

In other words, if $\psi \in V^*$ and $g \in G$, then $\rho^*(g)\psi$ is the functional $\psi \circ \rho(g^{-1})$. The inverse on g is necessary to make this a representation, because transposing reverses the direction of composition: indeed, for $g, h \in G$ we have

$$\rho^*(gh) = \rho(h^{-1}g^{-1})^\intercal = (\rho(h^{-1})\rho(g^{-1}))^\intercal = \rho(g^{-1})^\intercal\rho(h^{-1})^\intercal = \rho^*(g)\rho^*(h).$$

It is immediate from the definition that if V and W are representations and $S\colon V \to W$ is a G-homomorphism, then so is $S^\intercal\colon W^* \to V^*$.

If $H \subset G$ is a subgroup, we would like to be able to turn representations of G into representations of H, and vice versa. For the former, the obvious choice is to associate to a representation (ρ, V) of G its restriction $(\rho|_H, V)$. Turning a representation of H into a representation of the full group G requires a bit more work. Ideally, we would want to do this in a way that is 'inverse' to the restriction. Of course, this is impossible, since we lose too much information when restricting. Instead, we try to find something that is as 'close as possible' to an inverse in some sense (i.e. it is adjoint to restriction).

Definition 2.2.2. Suppose G is finite, $H \subset G$ a subgroup, and (ρ, V) a representation of H. The *induced* representation $(\mathrm{Ind}_H^G\rho, \mathrm{Ind}_H^G V)$ is given by

$$\mathrm{Ind}_H^G V = \{f\colon G \to V \mid f(hx) = \rho(h)f(x) \text{ for all } h \in H, x \in G\}$$

with the action defined by letting $\mathrm{Ind}_H^G\rho(g)f$ be the function defined by

$$\mathrm{Ind}_H^G\rho(g)f\colon x \mapsto f(xg).$$

We will also denote this function as $f(\_\, g)$

Finiteness of G guarantees that the space of all functions $G \to V$ is finite dimen-

sional, so certainly $\mathrm{Ind}_H^G V$ is as well. We will check that this is in fact a representation. To avoid clutter, for now we write ρ' for $\mathrm{Ind}_H^G \rho$. Then for $g_1, g_2, x \in G$ and $f \in \mathrm{Ind}_H^G V$ we have that $(\rho'(g_1 g_2)f)(x) = f(x g_1 g_2) = (\rho'(g_2)f)(x g_1) = (\rho'(g_1)\rho'(g_2)f)(x)$, as desired. Seeing as H acts on G by left multiplication and H acts on V via ρ, we can think of $\mathrm{Ind}_H^G V$ as being precisely those functions $G \to V$ which 'preserve' the action of H.

Example 2.2.3. If $H = G$, then for $f \in \mathrm{Ind}_H^G V$ we have $f(g) = \rho(g)f(e)$ for any $g \in G$, where $e \in G$ is the identity. Consequently, the map $\mathrm{Ind}_H^G V \to V$ given by $f \mapsto f(e)$ is an isomorphism of representations.

Example 2.2.4. If $H = \{e\}$ and V is the unique one-dimensional representation of H, then $\mathrm{Ind}_H^G V$ is isomorphic to the regular representation $E^{(G)}$ described in Example 2.1.3 via the map $f \mapsto \sum_{g \in G} f(g^{-1})g$. More generally, if we let H be any subgroup and V the trivial one-dimensional representation of H, then $\mathrm{Ind}_H^G V$ is isomorphic to $E^{(G/H)}$, where G acts on G/H by $(g, g'H) \mapsto (gg')H$.

Before moving to the important result that this is indeed the 'best possible way' to undo the restriction, we make the following remarks. Let $\{\alpha_i\}$ for $i = 1, \ldots, [G : H]$ be a system of representatives for the right-cosets $H\backslash G$. Then a function $f \in \mathrm{Ind}_H^G V$ is entirely determined by the values $f(\alpha_i)$. Indeed, for $g \in G$ we can write $g = h\alpha_i$ for some $i \in \{1, \ldots, [G : H]\}$ and $h \in H$, and then $f(g) = f(h\alpha_i) = \rho(h)f(\alpha_i)$.

An immediate consequence of this is that the map $\mathrm{Ind}_H^G V \to \bigoplus_{i=1}^{[G:H]} V$ given by $f \mapsto f(\alpha_i)$ is injective. It is also surjective: for any set of $[G : H]$ elements $v_i \in V$, we can define $f \colon G \to V$ by $f(h\alpha_i) = \rho(h)v_i$ for $1 \leq i \leq [G : H]$ and $h \in H$. Then $f \in \mathrm{Ind}_H^G V$ and $f(\alpha_i) = v_i$. As a consequence, we find that $\dim \mathrm{Ind}_H^G V = [G : H] \cdot \dim V$.

The above shows that in some sense, the induced representation is built out of copies of V. One can also check that the action of G permutes these copies of V. Given a representation (τ, W) of G, we might therefore hope that we can use this decomposition and the action of G to turn H-homomorphisms $V \to W$ into G-homomorphisms $\mathrm{Ind}_H^G V \to W$. In fact, the following theorem tells us exactly this!

THEOREM 2.2.5 (Frobenius reciprocity). Let G be a finite group, $H \subset G$ a subgroup. Furthermore, let (τ, W) be a representation of G, and (ρ, V) a representation of H. Then there is a natural injective linear map

$$\mathrm{Hom}_H(\rho, \tau|_H) \hookrightarrow \mathrm{Hom}_G(\mathrm{Ind}_H^G \rho, \tau).$$

This injection is in fact an isomorphism, but seeing as we do not need this full statement, we will only prove the weaker version stated above.

Proof. Just as before, fix a set of representatives $\{\alpha_i\}$ for $H\backslash G$. For $S \in \mathrm{Hom}_H(\rho, \tau|_H)$, define the map $\tilde{S}\colon \mathrm{Ind}_H^G V \to W$ by

$$\tilde{S}(f) = \sum_{i=1}^{[G:H]} \tau(\alpha_i^{-1}) S(f(\alpha_i)).$$

Then $\tilde{S}$ is a linear map. To show it is G-equivariant, we will first show it is independent of the choice of representatives. For fixed i, if β_i is another representative of $H\alpha_i$, there is some $h \in H$ with $\beta_i = h\alpha_i$. Hence we see that

$$\tau(\beta_i^{-1}) S(f(\beta_i)) = \tau(\alpha_i^{-1} h^{-1}) S(f(h\alpha_i)) = \tau(\alpha_i^{-1})\tau(h^{-1}) S(\rho(h) f(\alpha_i))$$

$$= \tau(\alpha_i^{-1})\tau(h^{-1})\tau(h) S(f(\alpha_i)) = \tau(\alpha_i^{-1}) S(f(\alpha_i))$$

and it follows that $\tilde{S}(f)$ is independent of the chosen representatives.

Now, let $g \in G$ and $f \in \mathrm{Ind}_H^G V$. The set $\{\alpha_i g^{-1}\}$ is again a set of representatives for $H\backslash G$, so that

$$\tilde{S}(\mathrm{Ind}_H^G \rho(g) f) = \sum_{i=1}^{[G:H]} \tau(\alpha_i^{-1}) S(f(\alpha_i g)) = \sum_{i=1}^{[G:H]} \tau(g\alpha_i^{-1}) S(f(\alpha_i)) = \tau(g)\tilde{S}(f).$$

The assignment $S \mapsto \tilde{S}$ is a linear map $\mathrm{Hom}_H(\rho, \tau|_H) \to \mathrm{Hom}_G(\mathrm{Ind}_H^G \rho, \tau)$. To show it is injective, suppose that $\tilde{S}$ is the zero map and let $v \in V$. Via the isomorphism $\mathrm{Ind}_H^G V \cong \bigoplus_{i=1}^{[G:H]} V$ we can find an $f \in \mathrm{Ind}_H^G V$ such that $f(\alpha_1) = v$ and $f(\alpha_i) = 0$ for $i \neq 1$. We then have $0 = \tilde{S}(f) = \tau(\alpha_1^{-1}) S(v)$, so $S(v) = 0$. Since v was arbitrary, it follows that $S = 0$. □

§2.3 Tensor products

In this section we define the tensor product of representations. We briefly explain the concept of the tensor product for regular vector spaces. We refer the reader to [Lan02, Ch. XVI] for more details and proofs of assertions.

Let V_1, V_2 be (finite dimensional) vector spaces over E. We call a vector space W together with a bilinear map $\varphi\colon V_1 \times V_2 \to W$ a *tensor product* of V_1 and V_2 if for every vector space W' and bilinear map $\varphi'\colon V_1 \times V_2 \to W'$, there is a unique linear map $S\colon W \to W'$ such that $\varphi' = S \circ \varphi$. An important theorem is that a tensor product always exists, and it is unique up to unique isomorphism. For this reason we speak of *the* tensor product, and denote it $V_1 \otimes V_2$, with the corresponding bilinear map denoted by $(v_1, v_2) \mapsto v_1 \otimes v_2$. By definition, to define a linear map

$S\colon V_1 \otimes V_2 \to W$, it suffices to give a bilinear map $\varphi\colon V_1 \times V_2 \to W$, and then S is uniquely defined by the condition $S(v_1 \otimes v_2) = \varphi(v_1, v_2)$.

From the definition one can show that the space $V_1 \otimes V_2$ is spanned by the elements of the form $v_1 \otimes v_2, v_1 \in V_1, v_2 \in V_2$, the so-called simple tensors (it is a common misconception that every element is of this form; this is generally not true). More specifically, if $e_1, \ldots, e_n$ is a basis for V_1 and $\epsilon_1, \ldots, \epsilon_m$ is a basis for V_2, then $\{e_i \otimes \epsilon_j \mid 1 \leq i \leq n, 1 \leq j \leq m\}$ is a basis for $V_1 \otimes V_2$. In particular $\dim(V_1 \otimes V_2) = \dim V_1 \cdot \dim V_2$. An important consequence of this is that if V is vector space over the field E, the map $E \otimes V \to V$ given by $\alpha \otimes v \mapsto \alpha v$ is an isomorphism. From now on, we will always make this identification.

Now, suppose that $S\colon V_1 \to W_1$ and $S'\colon V_2 \to W_2$ are linear maps. We can define a new linear map $S \cdot S' : V_1 \otimes V_2 \to W_1 \otimes W_2$ by $(S \cdot S')(v_1 \otimes v_2) = Sv_1 \otimes S'v_2$. The map $(S, S') \mapsto S \cdot S'$ is bilinear, so it induces a linear map $\mathrm{Hom}(V_1, W_1) \otimes \mathrm{Hom}(V_2, W_2) \to \mathrm{Hom}(V_1 \otimes V_2, W_1 \otimes W_2)$ sending $S \otimes S' \mapsto S \cdot S'$. This map is in fact an isomorphism, and from now on we will always identify these two spaces in this way. Accordingly the map $S \cdot S'$ will simply be denoted $S \otimes S'$. It also gives rise to the following definition.

Definition 2.3.1. If (ρ_1, V_1) and (ρ_2, V_2) are representations of a group G, we define the tensor product representation $(\rho_1 \otimes \rho_2, V_1 \otimes V_2)$ by

$$(\rho_1 \otimes \rho_2)(g) = \rho_1(g) \otimes \rho_2(g).$$

Note that if $\psi_1 \in V_1^*$ and $\psi_2 \in V_2^*$, then as above we can view $\psi_1 \otimes \psi_2$ as a map $V_1 \otimes V_2 \to E \otimes E = E$, in other words, an element of $(V_1 \otimes V_2)^*$. If V_1 and V_2 are representations, then the above vector space isomorphism $V_1^* \otimes V_2^* \to (V_1 \otimes V_2)^*$ is in fact also an isomorphism of representations. The bottom line is that the contragredient of a tensor product is the tensor product of the contragredients.

Lastly, we mention that everything that was done above also works for tensor products of n spaces $V_1 \otimes \cdots \otimes V_n$, which are defined similarly to tensor products of two spaces by replacing bilinear maps by multilinear ones.

3 The main theorem for $\mathrm{GL}_2(\mathbf{F}_p)$

From now on, we will write $G = \mathrm{GL}_2(\mathbf{F}_p)$, and all representations in this chapter will be over the field $\mathbf{F}_p$. Our goal is prove the main theorem of this thesis: the classification of all irreducible representations of $\mathrm{GL}_2(\mathbf{F}_p)$ over $\mathbf{F}_p$. The proof is based on the outline given in [BR]. It is divided into roughly 3 steps, corresponding to the 3 sections in this chapter. The first is of course to define the representations which will make up our classification, and prove they are irreducible and pairwise non-isomorphic. Secondly, we induce one-dimensional representations of B to get the so called *parabolic induction* representations of G. We show that the irreducible constituents of the parabolic inductions are indeed among the representations defined in step 1. Lastly, we show that any irreducible representation of G contains a B-stable subspace. Frobenius reciprocity then allows us to conclude that any irreducible representation of G is a quotient of a parabolic induction, which by step 2 gives the classification.

§3.1 The symmetric tensor powers

We first define the representations which will be the subject of our main result. They are known as the *symmetric tensor power* representations.

For $k \in \mathbf{Z}_{\geq 0}$, let $V_k = \mathbf{F}_p x^k \oplus \mathbf{F}_p x^{k-1}y \oplus \cdots \oplus \mathbf{F}_p y^k$ be the vector space degree k homogeneous polynomials in two variables. We make it into a representation of G by defining ρ_k by

$$\rho_k \begin{pmatrix} a & b \\ c & d \end{pmatrix} P = P(ax + cy, bx + dy)$$

for $\left(\begin{smallmatrix} a & b \\ c & d \end{smallmatrix}\right) \in G$. If $\chi \colon G \to \mathbf{F}_p^\times$ is a homomorphism, which we regard as a one-dimensional representation of G acting on the vector space $\mathbf{F}_p$, we get for any representation (ρ, V) a new representation $\chi \otimes \rho$ acting on the vector space $\mathbf{F}_p \otimes V = V$. Because by Proposition 1.0.4 all such χ are of the form $\det^r$, in addition to the

V_k we get the 'twisted' representations $(\rho_{k,r}, V_{k,r}) := (\det^r \otimes \rho_k, V_k)$. So we have for $P \in V_{k,r}$ and $g \in G$ that $\rho_{k,r}(g)P = \det(g)^r \cdot \rho_k(g)P$.

Example 3.1.1. Let $p = 5$, $k = 3$ and $r = 1$. For $P = x^3 - xy^2$, we have that $\rho_{3,1}\left(\begin{smallmatrix} 2 & 2 \\ 3 & 1 \end{smallmatrix}\right) P = (2 \cdot 1 - 3 \cdot 2)^1 \cdot ((2x + 3y)^3 - (2x + 3y)(2x + y)^2) = x^2y - y^3$, which happens to also equal $\rho_{3,1}\left(\begin{smallmatrix} 0 & 1 \\ 1 & 0 \end{smallmatrix}\right) P$.

We sometimes also write V_k to refer to simply the vector space of degree k homogeneous polynomials in two variables, without any specific action of G. The representations defined above are not all irreducible and distinct. The following two propositions provide conditions for when they are.

PROPOSITION 3.1.2. If $0 \leq k \leq p - 1$, then $V_{k,r}$ is irreducible.

Proof. Because the tensor product of any irreducible representation with a one-dimensional representation is again irreducible, it suffices to show this for $r = 0$. We calculate the space V_k^U of U-invariants. If P is in this space, we have that $\rho_k\left(\begin{smallmatrix} 1 & b \\ 0 & 1 \end{smallmatrix}\right) P = P(x, bx + y) = P(x, y)$ for all $b \in \mathbf{F}_p$. Write $f(y) = P(x, y) - P(x, 0)$, which we consider as a polynomial in y over the integral domain $\mathbf{F}_p[x]$. Then since P has degree $k < p$, the degree of f is also strictly less than p. Seeing as $f(bx) = 0$ for all $b \in \mathbf{F}_p$, we find that f has at least p different roots, and hence $f = 0$. Thus $P(x, y) = P(x, 0)$, and it follows that $P \in \mathbf{F}_p x^k$. As we also have $\mathbf{F}_p x^k \subset V_k^U$, we find that $V_k^U = \mathbf{F}_p x^k$.

Now let $W \subset V_{k,r}$ be a subrepresentation. We want to show that $W = 0$ or $W = V_k$. Since $W^U \subset V_k^U = \mathbf{F}_p x^k$, we have in particular that either $W^U = 0$ or $x^k \in W$. Because U is a p-group, by Lemma 2.1.14, the first case implies $W = 0$. It therefore suffices to show that $x^k \in W$ implies $W = V_k$.

Define $e_i = \binom{k}{i} x^{k-i} y^i$ for $0 \leq i \leq k$. Because $k < p$, the binomial coefficient is not divisible by p and the e_i form a basis for V_k. Consider the linear map on $V_{k,r}$ given by $e_j \mapsto \sum_{i=0}^k j^i e_i$. On the given basis, the matrix corresponding to this map is $(j^i)_{i,j=0}^k$. This is a so-called Vandermonde matrix, for which there is a well known expression for the determinant (see for instance [Lan02, Ch. XIII, p. 516]), namely $\prod_{0 \leq i < j \leq k}(j - i) \neq 0$. Hence the vectors $\sum_{i=0}^k j^i e_i = (x + jy)^k$ for $0 \leq j \leq k$ form a basis. Lastly, note that if $x^k \in W$, then $(x + jy)^k = \rho_k\left(\begin{smallmatrix} 1 & 0 \\ j & 1 \end{smallmatrix}\right) x^k \in W$, so that in this case W contains a basis for V_k, from which it follows that $W = V_k$. □

PROPOSITION 3.1.3. The representations $V_{k,r}$ and $V_{k',r'}$ are isomorphic if and only if $k = k'$ and $p - 1 | r - r'$.

Proof. The given conditions are clearly sufficient. Assume now that $S \colon V_{k,r} \to V_{k',r'}$

is an isomorphism. Because $\dim V_{k,r} = k+1$, we get that $k = k'$. As S is a G-homomorphism, it must map $V_{k,r}^U = \mathbf{F}_p x^k$ to $V_{k,r'}^U = \mathbf{F}_p x^k$, so $Sx^k = \lambda x^k$ for some $\lambda \in \mathbf{F}_p^\times$. Let $a \in \mathbf{F}_p^\times$ be a generator. Then

$$S\rho_{k,r}\begin{pmatrix} a & 0 \\ 0 & 1 \end{pmatrix} x^k = S(a^r(ax)^k) = a^{r+k}\lambda x^k,$$

and since S is a G-homomorphism, this must also equal

$$\rho_{k,r'}\begin{pmatrix} a & 0 \\ 0 & 1 \end{pmatrix} Sx^k = \lambda\rho_{k,r'}\begin{pmatrix} a & 0 \\ 0 & 1 \end{pmatrix} x^k = \lambda a^{r'+k}x^k.$$

It follows that $a^r = a^{r'}$ and hence $p-1 | r-r'$. □

Lastly, we need the following result giving the contragredient of the symmetric tensor power representations.

LEMMA 3.1.4. For $0 \le k \le p-1$, the contragredient of $V_{k,r}$ is isomorphic to $V_{k,-k-r}$.

Proof. We will call an element of V_k *simple* if it can be written as a product of degree 1 polynomials. Since all monomials are simple, the simple elements span V_k. If $v = \prod_{i=1}^k v_i$ is an simple element and $g \in G$, note that $\rho_{k,r}(g)v = \det(g)^r \prod_{i=1}^k \rho_1(g)v_i$.

To construct our isomorphism, we will use a special universal property of the space V_k. Namely, given any vector space W and symmetric multilinear map $\phi\colon V_1^k \to W$ (meaning that for any permutation $\sigma \in S_k$ we have $\phi(v_1,\dots,v_k) = \phi(v_{\sigma(1)},\dots,v_{\sigma(k)})$), there is a unique linear map $\tilde{\phi}\colon V_k \to W$ such that for any simple element $v = \prod_{i=1}^k v_i$, we have $\tilde{\phi}(v) = \phi(v_1,\dots,v_k)$ (see [FH04, Appendix B, Section 2]).[1]

We define a bilinear form on V_1 by $\langle \alpha x + \beta y, \gamma x + \delta y\rangle = \alpha\gamma + \beta\delta$. A straightforward verification shows that for $v_1, v_2 \in V_1$ and $g \in G$, we have $\langle v_1, \rho_1(g)v_2\rangle = \langle \rho_1(g^\intercal)v_1, v_2\rangle$. Let $v_1,\dots,v_k \in V_1$, and define a map $\psi_{v_1,\dots,v_k}\colon V_1^k \to \mathbf{F}_p$ by

$$\psi_{v_1,\dots,v_k}(u_1,\dots,u_k) = \sum_{\sigma\in S_k}\prod_{j=1}^k \langle v_{\sigma(j)}, u_j\rangle.$$

[1] Comparing this with the defining property of tensor products, it is now clear why the $V_{k,r}$ are called symmetric tensor power representations.

This is a symmetric multilinear map, so by the above property it gives rise to a unique linear map, also denoted by $\psi_{v_1,\dots,v_k}$, which satisfies

$$\psi_{v_1,\dots,v_k}\left(\prod_{i=1}^{k} u_i\right) = \sum_{\sigma\in S_k}\prod_{j=1}^{k}\langle v_{\sigma(j)}, u_j\rangle.$$

Now, note that the assignment $V_1^k \to V_k^*$ given by $(v_1,\dots,v_k)\mapsto \psi_{v_1,\dots,v_k}$ is again multilinear and symmetric. Hence, we get a linear map $V_k \to V_k^*$, this time denoted by $v\mapsto\psi_v$, such that if $v=\prod_{i=1}^k v_i$ is simple, $\psi_v = \psi_{v_1,\dots,v_k}$.

Write $z = \left(\begin{smallmatrix} 0 & -1 \\ 1 & 0\end{smallmatrix}\right)$. We now define a G-homomorphism $S\colon V_{k,-k-r}\to V_{k,r}^*$ by declaring that for $v\in V_k$,

$$S(v) = \psi_{\rho_k(z)v}.$$

We show that this map is indeed G-equivariant. Let $g\in G$. Since the simple elements span V_k, it suffices to check equivariance for $v=\prod_{i=1}^k v_i$ simple. We find that

$$\begin{aligned}\rho_{k,-k-r}(g)v &= \det(g)^{-k-2r}\rho_{k,r}(g)v\\ &= \rho_{k,r}(\det(g)^{-1}g)v\\ &= \rho_{k,r}(z^{-1}g^{-\intercal}z)v.\end{aligned}$$

The last line follows from the observation that $g^{-\intercal} = \det(g)^{-1}zgz^{-1}$. Our map S sends the element $\rho_{k,r}(z^{-1}g^{-\intercal}z)v$ to $\psi_{\rho_{k,r}(g^{-\intercal}z)v}$. As mentioned at the start, we have $\rho_{k,r}(g^{-\intercal}z)v = \det(g^{-1})^r\prod_{i=1}^k\rho_1(g^{-\intercal}z)v_i$, so this gets mapped to

$$\det(g^{-1})^r\sum_{\sigma\in S_k}\langle\rho_{1,0}(g^{-\intercal}z)v_{\sigma(1)},\text{-}\rangle\cdots\langle\rho_{1,0}(g^{-\intercal}z)v_{\sigma(k)},\text{-}\rangle \tag{3.1}$$

Letting the above functional act on a simple element $u=\prod_{i=1}^k u_i$, this becomes

$$\det(g^{-1})^r\sum_{\sigma\in S_k}\prod_{j=1}^{k}\langle\rho_1(g^{-\intercal}z)v_{\sigma(j)},u_j\rangle$$

$$= \det(g^{-1})^r\sum_{\sigma\in S_k}\prod_{j=1}^{k}\langle\rho_1(z)v_{\sigma(j)},\rho_1(g^{-1})u_j\rangle.$$

We recognize that this is precisely the functional $\psi_{\rho_k(z)v}$ acting on the element $\det(g^{-1})^r\prod_{i=1}^k\rho_1(g^{-1})u_i = \rho_{k,r}(g^{-1})\prod_{i=1}^k u_i$. Hence the functional (3.1) is equal to

$$\psi_{\rho_k(z)v}\circ\rho_{k,r}(g^{-1}) = \rho_{k,r}^*(g)S(v),$$

which proves equivariance.

Lastly, we need to show the map is indeed bijective. We have that $\psi_{y^k}(y^k) = k!$ and since $k < p$, this is not divisible by p, so $\psi_{y^k} = S(x^k)$ is not the 0 functional. This shows that the map S is not identically 0, and because $V_{k,-k-r}$ is irreducible, S is injective and hence surjective by dimension considerations. □

Remark 3.1.5. Given a vector space V, we can define a new space $\mathrm{Sym}^k V$ called its k-th symmetric power. It is called that because it satisfies a universal property similar to that of tensor products, but with symmetric multilinear maps. The second paragraph of the above proof is the observation that $V_k = \mathrm{Sym}^k V_1$. The idea of the proof comes from the more general fact that there is a natural isomorphism $\mathrm{Sym}^k(V^*) \to (\mathrm{Sym}^k V)^*$ given by a certain sum over the symmetric group just as above, see [Kna96, Corollary A.22].

§3.2 Parabolic induction

To show that the representations from the previous section exhaust all possible irreducible representations of G, we need to discuss a different type of representation of G. Recall that $\chi_{r,s} \colon B \to \mathbf{F}_p^\times$ denotes the character given by $\chi_{r,s}\left(\begin{smallmatrix} a & b \\ 0 & d \end{smallmatrix}\right) = a^r d^s$. We think of it as a one-dimensional representation on the vector space $\mathbf{F}_p$. In this section we will study the induced representation of this character, which is called a parabolic induction. It has dimension $[G : B] = p + 1$ by Proposition 1.0.3.

LEMMA 3.2.1. The contragredient of $\mathrm{Ind}_B^G \chi_{r,s}$ is isomorphic to $\mathrm{Ind}_B^G \chi_{-r,-s}$.

Proof. To ease the notation a little, we write $\tilde{\chi} = \mathrm{Ind}_B^G \chi$. Choose a set of representatives $\{\alpha_i\}$ for the right-cosets $B\backslash G$. Define a map $S \colon \tilde{\chi}_{-r,-s} \to (\tilde{\chi}_{r,s})^*$ by letting $S(f_1)$ be the functional defined by $f_2 \mapsto \sum_{i=1}^{p+1} f_1(\alpha_i) f_2(\alpha_i)$. Then S is linear. We now first show that S is independent of the chosen set of representatives. Assume β_i is another representative of $B\alpha_i$, so that there exist $h_i \in B$ such that $\beta_i = h_i \alpha_i$. Then by definition of the induced representation, we have

$$\sum_{i=1}^{p+1} f_1(\beta_i) f_2(\beta_i) = \sum_{i=1}^{p+1} f_1(h_i\alpha_i) f_2(h_i\alpha_i)$$

$$= \sum_{i=1}^{p+1} \chi_{-r,-s}(h_i) f_1(\alpha_i) \chi_{r,s}(h_i) f_2(\alpha_i) = \sum_{i=1}^{p+1} f_1(\alpha_i) f_2(\alpha_i).$$

Now, to show S is equivariant, let $g \in G$. Then

$$(\tilde{\chi}^*_{r,s}(g)S(f_1))(f_2) = S(f_1)(\tilde{\chi}_{r,s}(g^{-1})f_2) = \sum_{i=1}^{p+1} f_1(\alpha_i)f_2(\alpha_i g^{-1}).$$

Then as $\{\alpha_i g\}$ is again a set of right-coset representatives, this is the same as

$$\sum_{i=1}^{p+1} f_1(\alpha_i g)f_2(\alpha_i) = S(f(\_g))f_2 = S(\tilde{\chi}_{-r,-s}(g)f_1)f_2.$$

Lastly, since both representations have the same dimension, it suffices to show S is injective. We have a basis $\{f_j \mid 1 \le j \le p+1\}$ for $\mathrm{Ind}_B^G \chi_{r,s}$ given by

$$f_j(h\alpha_i) = \begin{cases} \chi_{r,s}(h) & i = j, \\ 0 & i \neq j, \end{cases}$$

for all $h \in B$. Now suppose that for some f we have that $S(f)$ is identically 0, meaning that in particular, $S(f)(f_j) = f(\alpha_j)$ is 0 for all j. But since a function in the induced representation is determined by its values on a set of right-coset representatives, we must have that f is identically 0. □

We now utilize this result, together with Lemma 3.1.4 giving the contragredient of the symmetric powers to find the irreducible constituents of the parabolic induction. This in turn will be one of the main ingredients in the proof of the classification next section.

PROPOSITION 3.2.2. If $0 \le k \le p-1$, we have

$$\mathrm{Irr}(\mathrm{Ind}_B^G \chi_{r,r+k}) = \{V_{k,r}, V_{p-1-k,r+k}\}.$$

Proof. Define a map $\phi\colon V_{k,r} \to \mathrm{Ind}_B^G \chi_{r,r+k}$ as follows: we let $\phi(P)$ be the function that maps $g \in G$ to $(\rho_{k,r}(g)P)(0,1)$. We check that the function $\phi(P)$ actually lies in the space of the induced representation. For $g \in G$ and $h = \left(\begin{smallmatrix} a & b \\ 0 & d \end{smallmatrix}\right) \in B$, we have that

$$\begin{aligned} \phi(P)(hg) &= (\rho_{k,r}(h)\rho_{k,r}(g)P)(0,1) = \det(h)^r(\rho_{k,r}(g)P)(0,d) \\ &= a^r d^{r+k}(\rho_{k,r}(g)P)(0,1) = \chi_{r,r+k}(h)\phi(P)(g). \end{aligned}$$

Now for $g \in G$, we have that $\phi(\rho_{k,r}(g)P)$ is the function $h \mapsto (\rho_{k,r}(hg)P)(0,1)$, which is of course precisely $\phi(P)(\_g)$, so ϕ is a G-homomorphism.

Since the representation $V_{k,r}$ is irreducible for $0 \le k \le p-1$ and ϕ is nontrivial, it is injective. For this reason, in the rest of the proof we regard $V_{k,r}$ as a subrepresentation of $\mathrm{Ind}_B^G \chi_{r,r+k}$, with ϕ being the inclusion.

In the same way as above we get a nontrivial G-homomorphism

$$V_{p-1-k,-r} \to \mathrm{Ind}_B^G \chi_{-r,p-1-k-r} = \mathrm{Ind}_B^G \chi_{-r,-r-k}.$$

Taking the transpose of this map gives a nontrivial homomorphism

$$(\mathrm{Ind}_B^G \chi_{-r,-r-k})^* \to V_{p-1-k,-r}^*,$$

and by Lemmas 3.1.4 and 3.2.1, this amounts to a nontrivial homomorphism

$$\mathrm{Ind}_B^G \chi_{r,r+k} \to V_{p-1-k,-p+1+k+r} = V_{p-1-k,r+k}.$$

Because the codomain is irreducible, this map is surjective. Call its kernel W. We now look at the composition

$$V_{k,r} \hookrightarrow \mathrm{Ind}_B^G \chi_{r,r+k} \twoheadrightarrow V_{p-1-k,r+k}.$$

This map must either be 0 or an isomorphism, and the latter is seen to be impossible by Proposition 3.1.3. Hence $V_{k,r}$ is contained in W, and by comparing dimensions they must be equal. Thus we see that we get an isomorphism $\mathrm{Ind}_B^G \chi_{r,r+k}/V_{k,r} \cong V_{p-1-k,r+k}$, proving the proposition. □

§3.3 The final steps

We need one last lemma before we can move on to our main result.

LEMMA 3.3.1. Any nonzero representation of G contains a B-stable subspace of dimension one.

Proof. Let (ρ, V) be a nonzero representation of G. We will consider V^U, which is nonzero by Lemma 2.1.14. Recall that T is the subgroup of diagonal matrices in G. Note that

$$\begin{pmatrix} 1 & b \\ 0 & 1 \end{pmatrix} \begin{pmatrix} a & 0 \\ 0 & d \end{pmatrix} = \begin{pmatrix} a & 0 \\ 0 & d \end{pmatrix} \begin{pmatrix} 1 & a^{-1}db \\ 0 & 1 \end{pmatrix},$$

in other words, T is contained in the normalizer of U. Hence if $t \in T$, $u \in U$, then we can write $ut = tu'$ for some $u' \in U$. Thus for $v \in V^U$, we have

$$\rho(u)\rho(t)v = \rho(t)\rho(u')v = \rho(t)v,$$

which shows that again $\rho(t)v \in V^U$. It follows that V^U is stable under T. Let W be any irreducible T-subrepresentation of V^U. It is one-dimensional by Lemma 2.1.15. Seeing as we have

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

we can write any $h \in B$ as $h = tu$ for $t \in T, u \in U$. Then for $v \in W$ we have that $\rho(h)v = \rho(t)v \in W$, so W is indeed B-stable. □

At last, we finally arrive at the main theorem of this thesis. Basically all the work has already been done, and all that is left is to put everything together.

THEOREM 3.3.2. The representations $(\rho_{k,r}, V_{k,r})$ with $0 \leq k \leq p-1$, $0 \leq r \leq p-2$ are irreducible, pairwise non-isomorphic, and any irreducible representation of G is isomorphic to one of these.

Proof. The first parts where already shown in Proposition 3.1.2 and 3.1.3. For the last part, let (ρ, V) be any irreducible representation of G. By Lemma 3.3.1, it has a one-dimensional B-stable subspace, which is of the form $\chi_{r,s}$ by Proposition 1.0.2. By changing s by multiples of $p-1$ we may assume $k := s - r$ lies between 0 and $p-1$. This means we have an injective map $S \in \mathrm{Hom}_B(\chi_{r,r+k}, \rho|_B)$, namely the inclusion. By Frobenius reciprocity (Theorem 2.2.5), we get a nonzero G-homomorphism $\tilde{S} \colon \mathrm{Ind}_B^G \chi_{r,r+k} \to V$, which is then surjective by irreducibility of V. Hence V is isomorphic to an irreducible quotient of $\mathrm{Ind}_B^G \chi_{r,r+k}$, which by Corollary 2.1.11 and Proposition 3.2.2 must be one of the representations occurring in the theorem. □

4 Generalization to $\mathrm{GL}_2(\mathbf{F}_q)$

As in Chapter 1, $q = p^n$ is a power of p. We will write $G = \mathrm{GL}_2(\mathbf{F}_q)$, and all representations will be over the field $\mathbf{F}_q$. In this chapter we will adapt the statements of the previous chapter to this group. Most of the results and proofs easily generalize to the new situation, with the exception of Proposition 3.2.2 giving the irreducible constituents of the parabolic inductions.

§4.1 Frobenius twists of representations

We let $\mathrm{Fr}\colon \mathbf{F}_q \to \mathbf{F}_q$ denote the Frobenius automorphism $a \mapsto a^p$. It induces an automorphism of G by applying it to the each entry of a matrix. This automorphism of G is still denoted Fr. Given any representation (ρ, V) of G, we get for an integer j with $0 \leq j \leq n-1$ a new representation $(\rho^{[j]}, V^{[j]})$ given by $\rho^{[j]}(g) = \rho(\mathrm{Fr}^j(g))$. We still let V_k denote the space of homogeneous polynomials in two variables of degree k, this time over the field $\mathbf{F}_q$, with the action of G defined as before. These are generally no longer irreducible, and instead it is their subrepresentations we are interested in.

First we make a small remark: given any integer k with $0 \leq k \leq q-1$, there exist unique integers k_j, $0 \leq j \leq n-1$ with $0 \leq k_j \leq p-1$ such that $k = \sum_{j=0}^{n-1} k_j p^j$. This sum is called the *base p expansion* of k, and the k_j are its *base p digits*.

Lemma 4.1.1. Let $0 \leq k \leq q-1$ and write $k = \sum_{j=0}^{n-1} k_j p^j$ for the base p expansion of k. Then V_k contains a subrepresentation isomorphic to $\bigotimes_{j=0}^{n-1} V_{k_j}^{[j]}$.

Proof. Define a map $\bigotimes_{j=0}^{n-1} V_{k_j}^{[j]} \to V_k$ by $P_0 \otimes \cdots \otimes P_{n-1} \mapsto \prod_{j=0}^{n-1} P_j(x^{p^j}, y^{p^j})$. Note that the latter polynomial is indeed homogeneous of degree $\sum_{j=0}^{n-1} k_j p^j = k$. To see this is a G-homomorphism, it suffices to check this on simple tensors. In this case,

we have for $g = \left(\begin{smallmatrix} a & b \\ c & d \end{smallmatrix}\right) \in G$ that

$$\rho_{k_0}^{[0]}(g)P_0 \otimes \cdots \otimes \rho_{k_{n-1}}^{[n-1]}(g)P_{n-1} \mapsto \prod_{j=0}^{n-1} (\rho_{k_j}^{[j]}(g)P_j)(x^{p^j}, y^{p^j})$$

$$= \prod_{j=0}^{n-1} (\rho_{k_j}(\mathrm{Fr}^j(g))P_j)(x^{p^j}, y^{p^j}) = \prod_{j=0}^{n-1} P_j(a^{p^j}x^{p^j} + c^{p^j}y^{p^j}, b^{p^j}x^{p^j} + d^{p^j}y^{p^j})$$

$$= \prod_{j=0}^{n-1} P_j((ax+cy)^{p^j}, (bx+dy)^{p^j}) = \rho_k(g) \prod_{j=0}^{n-1} P_j(x^{p^j}, y^{p^j}).$$

Lastly, this map is injective, because by uniqueness of the base p expansion the basis elements $\{\bigotimes_{j=0}^{n-1} x^{k_j - i_j} y^{i_j} \mid 0 \leq i_j \leq k_j\}$ all map to distinct polynomials. The image of the map is now our desired subrepresentation. □

PROPOSITION 4.1.2. If $0 \leq k_j \leq p-1$ for all j between 0 and $n-1$, then the representation $\det^r \otimes \bigotimes_{j=0}^{n-1} V_{k_j}^{[j]}$ is irreducible.

Proof. Just as before it suffices to show this for $r = 0$. We again let $k = \sum_{j=0}^{n-1} k_j p^j$. Using the same technique as in the beginning of the proof of Proposition 3.1.2, we see that $V_k^U = \mathbf{F}_q x^k$. Denote by V the subrepresentation described in Lemma 4.1.1. Suppose $W \subset V \subset V_k$ is a subrepresentation. Then we have $W^U \subset V_k^U = \mathbf{F}_q x^k$, and in particular either $W^U = 0$ or $x^k \in W$. By Lemma 2.1.14, the first case implies $W = 0$. It now suffices to show that if $x^k \in W$, then $W = V$.

Let $\lambda_0, \ldots, \lambda_{q-1}$ be an enumeration of $\mathbf{F}_q$. For $0 \leq i \leq q-1$, write $v_i = \binom{k}{i} x^{k-i} y^i$. We also define $e_m = \sum_{i=0}^{q-1} \lambda_m^i v_i$, so written compactly we have that

$$\begin{pmatrix} e_0 \\ \vdots \\ e_{q-1} \end{pmatrix} = A \begin{pmatrix} v_0 \\ \vdots \\ v_{q-1} \end{pmatrix}$$

where $A = (\lambda_m^i)_{m,i=0}^{q-1}$. As before, this is a Vandermonde matrix, with determinant $\prod_{0 \leq m < m' \leq q-1} (\lambda_{m'} - \lambda_m) \neq 0$, and hence A is invertible. This means we can write all the v_i as linear combinations of the e_m. Because $e_m = (x + \lambda_m y)^k = \rho_k \left(\begin{smallmatrix} 1 & 0 \\ \lambda_m & 1 \end{smallmatrix}\right) x^k$, we have that if $x^k \in W$, then also $e_m \in W$ for $m = 0, \ldots, q-1$ and hence $v_i \in W$ for $i = 0, \ldots, q-1$. Thus to show that $x^k \in W$ implies $W = V$, it suffices to show that the v_i span V.

For an integer i, denote its base p digits by i_j. Let $I = \{i \mid i_j \leq k_j \text{ for all } j\}$. This means that if $i \in I$, then $x^{k-i} y^i \in V$, because it can be written as $\prod_{j=0}^{n-1} x^{(k_j - i_j)p^j} y^{i_j p^j}$.

Note also that $\#I = \prod_{j=0}^{n-1}(k_j+1) = \dim V$. It is a consequence of Lucas's theorem, which says that $\binom{k}{i} \equiv \prod_j \binom{k_j}{i_j} \bmod p$ (see [Fin47, Theorem 1]) that also $I = \{i \mid \binom{k}{i} \not\equiv 0 \bmod p\}$, and hence $v_i = 0$ if and only if $i \notin I$, so $\operatorname{Span}\{v_i \mid 0 \leq i \leq q-1\} = \operatorname{Span}\{x^{k-i}y^i \mid i \in I\}$. Because this is the span of $\#I = \dim V$ linearly independent elements of V, they must indeed span V. □

PROPOSITION 4.1.3. For $0 \leq k_j, k'_j \leq p-1$ for all j, the representations $\det^r \otimes \bigotimes_{j=0}^{n-1} V_{k_j}^{[j]}$ and $\det^{r'} \otimes \bigotimes_{j=0}^{n-1} V_{k'_j}^{[j]}$ are isomorphic if and only if $k_j = k'_j$ for all j and $q-1 | r-r'$.

Proof. The given conditions are clearly sufficient. Write $k = \sum_{j=0}^{n-1} k_j p^j$ and define k' similarly. Using Lemma 4.1.1 we can view $\det^r \otimes \bigotimes_{j=0}^{n-1} V_{k_j}^{[j]}$ as a subrepresentation of $V_{k,r}$. Denote this subrepresentation by V, and denote by V' the analogous subrepresentation of $V_{k',r'}$. Assume that $S\colon V \to V'$ is an isomorphism. Then S must map $V^U = \mathbf{F}_q x^k$ to $V'^U = \mathbf{F}_q x^{k'}$, and hence $Sx^k = \lambda x^{k'}$ for some $\lambda \in \mathbf{F}_q^\times$. Let $a \in \mathbf{F}_q^\times$ be a generator. Then

$$S\rho_{k,r}\begin{pmatrix} a & 0 \\ 0 & a^{-1} \end{pmatrix} x^k = S((ax)^k) = a^k \lambda x^{k'},$$

and since S is a G-homomorphism, this must also equal

$$\rho_{k',r'}\begin{pmatrix} a & 0 \\ 0 & a^{-1} \end{pmatrix} Sx^k = \lambda \rho_{k',r'}\begin{pmatrix} a & 0 \\ 0 & a^{-1} \end{pmatrix} x^{k'} = \lambda a^{k'} x^{k'}.$$

From this it follows that $a^k = a^{k'}$ and hence $q-1 | k-k'$. Because $0 \leq k, k' \leq q-1$ we get that $k = k'$, or one of k and k' is 0 and the other is $q-1$. However, in the latter case V and V' do not have the same dimension, so $k = k'$. Then since base p expansions are unique, we must have $k_j = k'_j$ for all j. Similarly, by considering instead the action of $\left(\begin{smallmatrix} a & 0 \\ 0 & 1 \end{smallmatrix}\right)$, we get that $q-1 | r-r'$. □

Even though we do not use it later, for completeness we mention the following result giving the contragredients of the above representations.

PROPOSITION 4.1.4. For $0 \leq k_j \leq p-1$, the contragredient of $\det^r \otimes \bigotimes_{j=0}^{n-1} V_{k_j}^{[j]}$ is isomorphic to $\det^{-r-\sum k_j p^j} \otimes \bigotimes_{j=0}^{n-1} V_{k_j}^{[j]}$.

Proof. Because the contragredient of a tensor product is the tensor product of the contragredients, it suffices to show that $(\det^r)^* \cong \det^{-r}$ and $(V_{k_j}^{[j]})^* \cong \det^{-k_j p^j} \otimes$

$V_{k_j}^{[j]}$. Thinking again of $\det^r$ acting on the space $\mathbf{F}_q$, the first isomorphism is given by $\psi \mapsto \psi(1)$. The map in the proof of 3.1.4 gives a bijective G-homomorphism $S\colon \det^{-k_j} \otimes V_{k_j} \to V_{k_j}^*$. Then for $g \in G$, we have

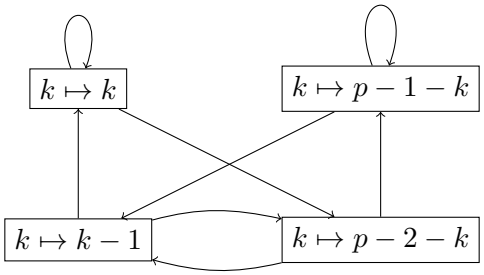
$$S \circ \det^{-k_j p^j}(g)\rho_{k_j}^{[j]}(g) = S \circ \det^{-k_j}(\mathrm{Fr}^j(g))\rho_{k_j}(\mathrm{Fr}^j(g)) = \rho_{k_j}^*(\mathrm{Fr}^j(g)) \circ S = (\rho_{k_j}^{[j]})^*(g) \circ S$$

and we are done. □

§4.2 Parabolic induction revisited

Again letting $\chi_{r,s}\colon B \to \mathbf{F}_q^\times$ denote the character given by $\chi_{r,s}\left(\begin{smallmatrix} a & b \\ 0 & d \end{smallmatrix}\right) = a^r d^s$, we can consider the induced representation of dimension $[G : B] = q + 1$. To proceed with the proof, we need a generalization of Proposition 3.2.2 giving the irreducible constituents of the parabolic induction. Sadly, in the more general case this representation no longer has length 2, and the previous technique of using the contragredients no longer works. A description of the irreducible constituents is still possible, but the proof is out of the scope of this thesis. The original result is due to Fred Diamond [Dia07, Proposition 1.1], and the following formulation is taken from [Roz14, Section 2.7].

Consider the following directed graph:



(4.1)

A closed path of length n in this graph is a sequence $c = (c_0, \ldots, c_n)$ of nodes such that there is an edge going from c_j to c_{j+1} for $j = 0, \ldots, n-1$ and $c_0 = c_n$. We denote by $\mathcal{C}$ the set of closed paths in this graph of length n. If v is a node in the graph, we identify it with the function displayed at that node. For a path $c \in \mathcal{C}$ we also define the function ℓ_c by

$$\ell_c(k_0,\dots,k_{n-1}) = \begin{cases} \frac{1}{2}\sum_{j=0}^{n-1}(k_j - c_j(k_j))p^j & \text{if } c_{n-1} \text{ is one of the two leftmost nodes in (4.1)} \\ \frac{1}{2}(q-1+\sum_{j=0}^{n-1}(k_j - c_j(k_j))p^j) & \text{otherwise.} \end{cases}$$

Lastly, if $0 \leq k \leq q-1$ is an integer and $k = \sum_{j=0}^{n-1} k_j p^j$ its base p expansion, we set $\ell_c(k) = \ell_c(k_0,\dots,k_{n-1})$.

PROPOSITION 4.2.1. For $0 \leq k_j \leq p-1$ and $k = \sum_{j=0}^{n-1} k_j p^j$, let $\mathcal{C}'$ be the set of all $c \in \mathcal{C}$ such that $0 \leq c_i(k_j) \leq p-1$ for all j. Then we have

$$\mathrm{Irr}(\mathrm{Ind}_B^G \chi_{r,r+k}) = \left\{ \det{}^{r+\ell_c(k)} \otimes \bigotimes_{j=0}^{n-1} V_{c_j(k_j)}^{[j]} \,\middle|\, c \in \mathcal{C}' \right\}.$$

As a sanity check, we will make sure that in the case $n = 1$, this gives the same result as Proposition 3.2.2. In this case, $\mathcal{C}$ has two elements, namely the path c that goes from the node $k \mapsto k$ to itself, and similarly the path c' going from $k \mapsto p-1-k$ to itself. Both of these satisfy the hypotheses for being in $\mathcal{C}'$. For the first of these paths, we have $\ell_c(k) = \frac{1}{2}(k - c(k))p^0 = 0$, and for the second we have $\ell_{c'}(k) = \frac{1}{2}(p-1+(k-c'(k))p^0) = \frac{1}{2}(p-1+k-(p-1-k) = k$. Hence we get the two representations $\det^r \otimes V_k = V_{k,r}$ and $\det^{r+k} \otimes V_{p-1-k} = V_{p-1-k,r+k}$, which is indeed the same as before.

Note that the proof of Lemma 3.3.1 still works in the present context. Thus in exactly the same way as before, we can combine all the above results to finally get to the desired classification.

THEOREM 4.2.2. The representations $\det^r \otimes \bigotimes_{j=0}^{n-1} V_{k_j}^{[j]}$ with $0 \leq k_j \leq p-1$, $0 \leq r \leq q-2$ are irreducible, pairwise non-isomorphic, and any irreducible representation of G is isomorphic to one of these.

5 Representations of $\mathrm{GL}_n(\mathbf{Z}_p)$

In this chapter we introduce the field of p-adic numbers, the ring of p-adic integers, and certain groups of matrices over these. As mentioned in the introduction, representations of these groups are of great interest in number theory. At the end of this chapter we show how these representations are connected to representations of $\mathrm{GL}_n(\mathbf{F}_p)$, hopefully making more clear the importance of everything we have done so far. To save space and time, most properties of the p-adic numbers are presented without proof. Instead, we reference the reader to [Neu99, Ch. II, Sections 1,2]. The latter part concerning p-adic matrix groups and their representations is based on the notes by Florian Herzig [Her15].

§5.1 p-adic numbers, integers and related groups

As always we fix a prime p. We can write any nonzero rational number α uniquely in the form $p^r \frac{a}{b}$ with $r, a, b \in \mathbf{Z}$, $b > 0$ and $p \nmid a, b$. We define the *p-adic valuation* by $v_p(\alpha) = r$. Additionally we set $v_p(0) = \infty$. It is obvious that v_p satisfies $v_p(\alpha\beta) = v_p(\alpha) + v_p(\beta)$ and $v_p(\alpha + \beta) \geq \min\{v_p(\alpha), v_p(\beta)\}$. Next, we define the *$p$-adic absolute value* of a nonzero rational as $|\alpha|_p = p^{-v_p(\alpha)}$, and $|0|_p = 0$. From the properties of v_p it follows that $|\alpha|_p = 0 \iff \alpha = 0$, $|\alpha\beta|_p = |\alpha|_p|\beta|_p$ and $|\alpha+\beta|_p \leq \max\{|\alpha|_p, |\beta|_p\}$. The last property is known as the *ultrametric inequality*, and together with the first it implies that $d_p(\alpha, \beta) = |\alpha - \beta|_p$ is a metric. As with the usual construction of $\mathbf{R}$ as equivalence classes of Cauchy sequences, we can complete $\mathbf{Q}$ with respect to this metric to get the field of *p-adic numbers* $\mathbf{Q}_p$. The p-adic absolute value has a unique extension to all of $\mathbf{Q}_p$, which is still denoted $|\cdot|_p$. The ultrametric inequality still holds, and it implies that the closed unit ball $\{\alpha \in \mathbf{Q}_p \mid |\alpha|_p \leq 1\}$ around 0 is a subring. It is denoted $\mathbf{Z}_p$, and is called the ring of *p-adic integers*, because it is in fact the closure of $\mathbf{Z}$ in $\mathbf{Q}_p$. Its units are precisely those α with $|\alpha|_p = 1$, and the set of elements α with $|\alpha|_p < 1$ is the unique maximal ideal, generated by p. The quotients of powers of this ideal satisfy

$\mathbf{Z}_p/p^r\mathbf{Z}_p \cong \mathbf{Z}/p^r\mathbf{Z}$. In particular, $\mathbf{Z}_p/p\mathbf{Z}_p \cong \mathbf{F}_p$. This algebraic fact manifests itself as an important topological property of the p-adic integers.

LEMMA 5.1.1. $\mathbf{Z}_p$ is compact.

Proof. Because on $\mathbf{Z}_p$ the p-adic metric only takes on the values p^{-r} for $r \in \mathbf{Z}_{\geq 0}$, we have that for $\alpha \in \mathbf{Z}_p$, any open ball around α is of the form $B(\alpha, p^{-r+1})$ for some $r \in \mathbf{Z}_{\geq 0}$, which is the same as the closed ball around α of radius p^{-r}. But this in turn is simply $\alpha + p^r\mathbf{Z}_p$. Thus we see that any open ball is a coset of some ideal $p^r\mathbf{Z}_p$. Because the ideal $p^r\mathbf{Z}_p$ has finite index p^r, it follows that $\mathbf{Z}_p$ can always be covered by finitely many open balls of any given radius. It is therefore totally bounded, and because it is complete (as it is a closed subset of the complete space $\mathbf{Q}_p$), it is compact. □

The newly defined $\mathbf{Q}_p$ and $\mathbf{Z}_p$ are examples of *topological groups*. These are groups G equipped with a topology such that the maps $(g, h) \mapsto gh$ and $g \mapsto g^{-1}$, from $G \times G \to G$ and $G \to G$, respectively, are continuous. Familiar examples of topological groups include $\mathbf{R}^n$ and $\mathbf{C}^n$ under addition. While there is a lot of interesting things to be said about topological groups, we will only mention that which is necessary for the remainder of this chapter. One of the most important properties of topological groups is that they 'look the same' around every point. More precisely, they are *homogeneous*: for every $g, h \in G$ there is a homeomorphism sending g to h, namely left multiplication by hg^{-1}.

For a general topological space X and $x \in X$, a collection $\mathcal{B}$ of neighborhoods of x is called a *fundamental system of neighborhoods of* x if every neighborhood of x contains an element of $\mathcal{B}$. For instance in a metric space, for any sequence of positive real numbers a_n converging to 0, the collection of open balls $\mathcal{B} = \{B(x, a_n)\}$ is a fundamental system of neighborhoods of x. In a topological group, by homogeneity we have that if $\mathcal{B}$ is a fundamental system of neighborhoods of the identity, then the sets gN for $N \in \mathcal{B}$ form a fundamental system of neighborhoods of g. Thus to describe the topology of a topological group, it suffices to give a fundamental system of neighborhoods of the identity.

Definition 5.1.2. A topological group is called a *pro-p-group* if it is compact, Hausdorff and has a fundamental system of neighborhoods of the identity consisting of open normal subgroups of p-power index.

Example 5.1.3. The additive group of p-adic integers $\mathbf{Z}_p$ is a pro-p-group. We already proved in Lemma 5.1.1 that it is compact. As a metric space, it is Hausdorff and a fundamental system of neighborhoods of 0 is given by the open balls around 0. But we have already seen that these open balls are all of the form $p^r\mathbf{Z}_p$, which are

indeed normal subgroups of p-power index.

If we identify the set of $n \times n$ matrices $M_n(\mathbf{Q}_p)$ with $\mathbf{Q}_p^{n^2}$ in the obvious way, we get a natural topology on $M_n(\mathbf{Q}_p)$, and hence on $\mathrm{GL}_n(\mathbf{Q}_p)$. With respect to this topology, $M_n(\mathbf{Q}_p)$ becomes a topological group under addition, and $\mathrm{GL}_n(\mathbf{Q}_p)$ under multiplication. If we define $|A|_p = \max_{1\leq i,j\leq n} |a_{ij}|_p$ for $A = (a_{ij}) \in M_n(\mathbf{Q}_p)$, then the topology on $M_n(\mathbf{Q}_p)$ is metrizable by the metric $d_p(A, B) = |A - B|_p$. For a positive integer r, define $K(r) = I + p^r M_n(\mathbf{Z}_p)$, where I is the $n \times n$ identity matrix. Then $K(r)$ is compact, as it is the image of the compact space $M_n(\mathbf{Z}_p) \cong \mathbf{Z}_p^{n^2}$ under the continuous map $A \mapsto I + p^r A$. We have $K(r + 1) \subset K(r) \subset \mathrm{GL}_n(\mathbf{Z}_p)$ for all r. In fact, these are all normal subgroups of $\mathrm{GL}_n(\mathbf{Z}_p)$, because $K(r)$ is precisely the kernel of the natural map $\mathrm{GL}_n(\mathbf{Z}_p) \to \mathrm{GL}_n(\mathbf{Z}_p/p^r\mathbf{Z}_p)$.

LEMMA 5.1.4. The subgroups $K(r)$ of $K(1)$ are all open, have p-power index and form a fundamental system of neighborhoods of the identity, so that $K(1)$ is a pro-p-group.

Proof. Because the p-adic valuation only takes on the values p^r for integer r, we find that $K(r)$ is equal to the set of all $A \in \mathrm{GL}_n(\mathbf{Z}_p)$ with $|A - I|_p < p^{-r+1}$. Hence $K(r)$ is the open ball of radius p^{-r+1} around I, which shows that these subgroups are open and form a fundamental system of neighborhoods of I. To show they have p-power index in $K(1)$, by the multiplicativity of the index it suffices to show that $[K(r) : K(r + 1)]$ is a power of p for all r. To do this, consider the map $K(r) \to M_n(\mathbf{F}_p)$ given by $I + p^r A \mapsto A \bmod p$. The equality $(I + p^r A)(I + p^r B) = I + p^r(A + B + p^r AB)$ shows that this is a group homomorphism, and its kernel is exactly $K(r + 1)$. Hence the index is a divisor of $\#M_n(\mathbf{F}_p) = p^{n^2}$. □

§5.2 Representations of p-adic groups

Because the groups we deal with in this chapter have more structure than just a group structure (namely, a topology), we generally only care about representations of such groups that in some sense 'preserve the topology'.

Definition 5.2.1. A representation (π, V) of a topological group is called *smooth* if the stabilizer subgroup of any vector is open.

Usually the notion of smooth representations is only used for so-called *locally profinite groups* instead of general topological groups. Examples of locally profinite groups are $\mathrm{GL}_n(\mathbf{Q}_p)$ and its closed subgroups, which includes all groups that we are interested in in this chapter.

We have the following lemma regarding mod p representations of pro-p-groups, which is a generalization of an earlier lemma about finite p-groups.

LEMMA 5.2.2. Let H be a pro-p group and (π, V) a smooth, nonzero representation of H over $\mathbf{F}_p$. Then $V^H \neq 0$.

Proof. Choose a nonzero $v \in V$. Then the stabilizer subgroup of v is an open neighborhood of the identity, and hence contains an open normal subgroup N of p-power index. Then $v \in V^N$, so $V^N \neq 0$. Now let $w \in V^N$, $h \in H$ and $g \in N$. By normality of N there exists $g' \in N$ such that $gh = hg'$. Then $\pi(g)\pi(h)w = \pi(h)\pi(g')w = \pi(h)w$, so $\pi(h)w \in V^N$, so V^N is H-stable. Because N acts trivially on V^N, we get a representation (π', V^N) of H/N by $\pi'(h \bmod N) = \pi(h)$. Now H/N is a finite p-group, so by Lemma 2.1.14, there is a nonzero vector $w \in V^N$ such that $\pi(h)w = \pi'(h \bmod N)w = w$ for all $h \in H$, and hence $w \in V^H$. □

We now finally come to the proposition which shows how the representations we have been dealing with in the previous chapters connect to those of this chapter.

PROPOSITION 5.2.3. Let (ρ, V) be an irreducible representation of $\mathrm{GL}_n(\mathbf{F}_p)$ over $\mathbf{F}_p$. Compose the quotient map $\mathrm{GL}_n(\mathbf{Z}_p) \to \mathrm{GL}_n(\mathbf{F}_p)$ with ρ to get a representation (π, V) of $\mathrm{GL}_n(\mathbf{Z}_p)$. Then π is smooth, and any smooth irreducible representation of $\mathrm{GL}_n(\mathbf{Z}_p)$ over $\mathbf{F}_p$ is obtained in this way.

Proof. Let $v \in V$. Denote by $N \subset \mathrm{GL}_n(\mathbf{F}_p)$ the stabilizer in $\mathrm{GL}_n(\mathbf{F}_p)$ of v. Then the stabilizer of v in $\mathrm{GL}_n(\mathbf{Z}_p)$ is the inverse image of N under the quotient map, which is a union of cosets of $\ker(\mathrm{GL}_n(\mathbf{Z}_p) \to \mathrm{GL}_n(\mathbf{F}_p)) = K(1)$. Since $K(1)$ is open (recall that it is the open ball around I of radius 1), so are its cosets and hence so is any union of cosets. Thus π is smooth.

Now suppose π is any smooth irreducible representation of $\mathrm{GL}_n(\mathbf{Z}_p)$. To show that π factors through the quotient map $\mathrm{GL}_n(\mathbf{Z}_p) \to \mathrm{GL}_n(\mathbf{F}_p)$, it suffices to show that the kernel $K(1)$ of this map is contained in the kernel of π, i.e. that $K(1)$ acts trivially on V. As $K(1)$ is a pro-p-group, we must have $V^{K(1)} \neq 0$ by the previous lemma. Let $v \in V^{K(1)}$, $g \in \mathrm{GL}_n(\mathbf{Z}_p)$ and $k \in K(1)$. Then by normality of $K(1)$, there is a $k' \in K(1)$ such that $kg = gk'$. Then $\pi(k)\pi(g)v = \pi(g)\pi(k')v = \pi(g)v$, so $\pi(g)v \in V^{K(1)}$, which shows that $V^{K(1)}$ is $\mathrm{GL}_n(\mathbf{Z}_p)$-stable. By irreducibility of V, we must have $V^{K(1)} = V$, so $K(1)$ acts trivially on V. □

In particular, when $n = 2$, we find that the irreducible smooth representations of $\mathrm{GL}_2(\mathbf{Z}_p)$ over $\mathbf{F}_p$ are given by Theorem 3.3.2.

Bibliography

[BL94] Laure Barthel and Ron Livné. "Irreducible modular representations of GL_2 of a local field". *Duke Mathematical Journal* 75.5 (1994), pp. 261–292.

[BR] Laurent Berger and Sandra Rozensztajn. *Modular representations of $GL_2(\mathbf{F}_p)$*. URL: http://perso.ens-lyon.fr/laurent.berger/autrestextes/GL2promys.pdf (visited on 01/23/2020).

[Bre03] Christophe Breuil. "Sur quelques représentations modulaires et p-adiques de $\mathrm{GL}_2(\mathbf{Q}_p)$:I." *Compositio Mathematica* 138 (2003), pp. 165–188.

[Dia07] Fred Diamond. "A correspondence between representations of local Galois groups and Lie-type groups". *L-Functions and Galois Representations*. London Mathematical Society Lecture Notes. Cambridge University Press, 2007, pp. 187–206.

[Eti+11] Pavel Etinghof et al. *Introduction to Representation theory*. American Mathematical Society, 2011.

[FH04] William Fulton and Joe Harris. *Representation theory*. Springer-Verlag, 2004.

[Fin47] Nathan Fine. "Binomial coefficients modulo a prime". *The American Mathematical Monthly* 54.10 (1947), pp. 589–592.

[Her15] Florian Herzig. "p-modular representations of p-adic groups". *Modular Representation Theory of Finite and p-adic Groups*. Ed. by Wee Teck Gan and Kai Meng Tan. IMS Lecture Series Notes. World Scientific, 2015, pp. 73–108.

[Kna96] Anthony Knapp. *Lie Groups Beyond an Introduction*. 1st ed. Springer-Verlag, 1996.

[Lan02] Serge Lang. *Algebra*. 3rd ed. Springer-Verlag, 2002.

[Lan67] Robert Langlands. *Letter to André Weil*. 1967. URL: http://publications.ias.edu/rpl/section/21 (visited on 05/05/2021).

[Neu99] Jürgen Neukirch. *Algebraic Number Theory*. 1st ed. Springer-Verlag, 1999.

[Roz14] Sandra Rozensztajn. "Asymptotic values of modular multiplicities for GL_2". *Journal de Théorie des Nombres de Bordeaux* 26.2 (2014), pp. 465–482.

[Ser77] Jean-Pierre Serre. *Linear representations of finite groups*. 2nd ed. Springer-Verlag, 1977.