REPRESENTATIONS OF $GL_2(\mathbb{F}_q)$

PATRICIA BRENT

Abstract. In order to explore Representation Theory as a logical follow-up to group theory, I attempt to enumerate the irreducible representations of $GL_2(\mathbb{F}_q)$. In order to do so, I first introduce the idea of a representation and provide a simple example. Next, I prove the existance of an irreducible decomposition for a given representation and introduce a useful result of characters. Finally, four types of the representations desired are shown to completely describe all irreducible representations of $GL_2(\mathbb{F}_q)$.

Contents

1. Introduction

Representation theory, simply put, brings group theory into the domain of linear algebra. In a representation, group elements are associated to matrices, whose properties (determinant, trace, eigenvalues, etc.) can be used to further inform a description of the group under consideration. Representations may also provide geometric intuition for abstract groups or, on a more advanced level, aid in understanding Galois groups and Lie algebras.

Definition 1.1. Given a group $\mathcal{G}$ and a vector space $\mathcal{V}$ (typically considered over $\mathbb{C}$), a representation $\rho : \mathcal{G} \to \mathcal{V}$ is defined to be a homomorphism from $\mathcal{G}$ into the group of endomorphisms of $\mathcal{V}$. This latter group is $GL(\mathcal{V})$.

In order to provide an elementary example of a representation, we will consider a well-known family of groups: namely, the dihedral groups. I will denote its members by $\mathcal{D}_{2n}$, where $2n$ is the order of the group.[1] Letting $\mathcal{G} = \mathcal{D}_6$ and $\mathcal{V} = \mathbb{C}^2$, then, we may consider the representation below, with group elements defined by the presentation specified.

[1]The reason for this notation will become clear momentarily.

Example 1. Consider $\mathcal{D}_6 = \langle (r,s) | r^3 = 1; s^2 = 1; rs = sr^{-1} \rangle$ and let $\rho : \mathcal{D}_6 \to GL_2(C^2)$ be defined by

$$s \to \begin{bmatrix} 1 & 0 \\ 0 & -1 \end{bmatrix}$$

$$r \to \begin{bmatrix} -1/2 & \sqrt{3}/2 \\ -\sqrt{3}/2 & -1/2 \end{bmatrix}$$

To better understand this representation, it may be helpful to consider $\mathcal{D}_6$ according to its geometric definition as the rigid motions of an equilateral triangle (i.e. an n-gon, for $n = 3$). In this case, one may picture the triangle with one point on the positive x-axis and the other two in the second and third quadrants, respectively. The matrix r represents rotation by $\pi/3$ radians; this is easily checked via the standard matrix for rotation by θ. The element s corresponds to a matrix for reflection across the x axis. Observation shows that these matrices both permute vertices of the triangle (noncommutatively) and satisfy the order constraints of the abstract definition.

2. Irreducibility

Given two representations into the endomorphisms of vector spaces $\mathcal{V}$ and $\mathcal{W}$, respectively, there exist representations of the same group into $\mathcal{V} \oplus \mathcal{W}$ and $\mathcal{V} \otimes \mathcal{W}$. The same is true of alternating and symmetric powers of any representation space $\mathcal{V}$ as well as the dual space $\mathcal{V}^*$. In light of these larger representations, a natural question to ask is whether, given a representation, it is possible to break it down into a direct sum of somehow smaller or simpler representations. This concept, known as (ir)reducibility, turns out to provide an intuitive organization of all possible representations for a given group. Before we rush forward, however, it behooves us to formalize our terms.

Definition 2.1. A representation $\rho : \mathcal{G} \to GL(\mathcal{V})$ is *irreducible* if $\mathcal{V}$ is not 0 and contains no $\mathcal{G}$-stable subspaces.

By $\mathcal{G}$-stable subspace we mean simply a subspace of $\mathcal{V}$ fixed by all the elements in the image of $\mathcal{G}$ by ρ. As it turns out, if we *can* find just such a stubborn subspace, the representation space can be broken down into two $\mathcal{G}$-stable pieces (and potentially more, until we obtain an irreducible decomposition).

Theorem 2.2. *Given a linear representation $\rho : \mathcal{G} \to \mathcal{V}$ and $\mathcal{W}$ a $\mathcal{G}$-stable subspace of $\mathcal{V}$, there exists a $\mathcal{G}$-stable complement $\mathcal{W}'$ of $\mathcal{W}$ in $\mathcal{V}$.*

Proof. Take any complement of $\mathcal{W}$ and call it $\mathcal{W}'$. Let p be the projection of $\mathcal{V}$ onto $\mathcal{W}$ such that the kernel of p is $\mathcal{W}'$. Now, as suggested by Serre, we define p^0 to be the *averaging function*[2] of the conjugates of p by elements of $\mathcal{G}$, where g is the order of $\mathcal{G}$ and is assumed not to divide the characteristic of the field over which $\mathcal{V}$ is a vector space.

$$p^0 = \frac{1}{g} \sum_{t \in G} (\rho_t \cdot p \cdot \rho_t^{-1})$$

Note that, by definition, p maps $\mathcal{V}$ into $\mathcal{W}$, and ρ_t maps $\mathcal{W}$ into itself. It follows that $p_t^{-1} x \in \mathcal{W}$ for all $x \in \mathcal{W}$. Then, since p acts as the identity on $\mathcal{W}$,

$$p \cdot \rho_t^{-1} x = \rho_t^{-1} x$$

[2]Note that the averaging function is fixed by the action of elts. of $\mathcal{G}$.

Composition on both sides by ρ_t gives:

$$\rho_t \cdot p \cdot \rho_t^{-1} x = x, \text{i.e.} p^0 x = x$$

Since p^0 acts identically on $\mathcal{W}$ and (because it includes p) sends elements of $\mathcal{V}$ to $\mathcal{W}$, it is also a projection of $\mathcal{V}$ onto $\mathcal{W}$. Then, taking $\mathcal{W}'$ to be the kernel of p^0, we have a complement of $\mathcal{W}$ which turns out via a few short calculations[4] to be $\mathcal{G}$-stable. □

By thus establishing the reducibility of any given representation to irreducible parts, we obtain a set of atomic pieces that uniquely determine the given representation, up to isomorphism. With this conception in mind, we may return to the question of finding all possible representations for a given group. It will be the goal of this paper to investigate the irreducible representations of $\mathcal{G} = GL_2(\mathbb{F}_q)$ for finite q. Finite fields are simple to define but can behave counterintuitively with regard to geometry. In addition, representations involving matrices over finite fields have given rise to a number of unexpected finite simple groups, including the Monster Group. Thus, by selecting this particular $\mathcal{G}$, we can investigate an interesting, non-commutative group while considering only two-dimensional matrices so that calculations remain reasonable.

3. Characters

One extremely useful way of finding these irreducible representations comes from character theory. In general, a character χ is a homomorphism, from $\mathcal{G}$ to a field (commonly $\mathbb{C}$), satisfying certain properties. In the case of $GL_2(\mathbb{F}_q)$, we may consider a map onto $GL_n(\mathbb{C})$. Taking the trace of these matrices allows us to consider single-dimensional elements of a more familiar field which nonetheless interact similarly to the original matrices.

Definition 3.1. Given a representation ρ of a group $\mathcal{G}$, the character χ_ρ is defined for each $g \in \mathcal{G}$ as the trace of the matrix $\rho(g)$. Recall that the trace does not depend on a choice of basis elements.

Theorem 3.2. *Given characters χ_{ρ_i} and χ_{ρ_j} of representations ρ_i and ρ_j, define an inner product $(\chi_{\rho_i}, \chi_{\rho_j}) = \frac{1}{g}\sum_{t\in\mathcal{G}} \chi_{\rho_i}(t)\cdot\overline{\chi_{\rho_j}(t)}$ where g is the order of $\mathcal{G}$. Then the following statements hold:*
(i) χ_{ρ_i} is irreducible[3] $\iff (\chi_{\rho_i}, \chi_{\rho_i}) = 1$
(ii) If χ_{ρ_i} and χ_{ρ_i} are irreducible with $i \neq j$, then $(\chi_{\rho_i}, \chi_{\rho_j}) = 0 \iff \chi_{\rho_i} \ncong \chi_{\rho_i}$[4]

This theorem and the next are given as a simple consequence of often much more complicated derivations, none of which is immediately relevant to the topic at hand; for this reason, proofs are omitted[1, 3]. However, to solidify the idea, I will provide a few examples for the specific groups we will be considering in the next section.

Theorem 3.3. *The number of distinct irreducible representations of a group $\mathcal{G}$ is the number of conjugacy classes of $\mathcal{G}$.*

[3] An irreducible character is a character of an irreducible representation

[4] Two representations are isomorphic if there exists a group-action-preserving isomorphism between the vector spaces into which they map.

In combination, Theorems 3.2 and 3.3 give rise to a disarmingly simple framework for uncovering the irreducible representations of a group. One need only generate a list of possible characters and check their norms and inner products with one another until the number of conjugacy classes is reached. Compared to the arduous process of uncovering all the irreducible representations for a given group and searching for isomorphisms between between them, checking this inner product is computationally uncomplicated, to the extent that it can easily be done by computer.

4. Representations of $GL_2(\mathbb{F}_q)$

To facilitate the search for all possible representations, I will better organize the group itself. The different conjugacy classes of $GL_2(\mathbb{F}_q)$ may each be represented in one of four forms, owing to the reduction of matrices to Jordan Canonical Form. First, we consider matrices with a repeated eigenvalue. If a matrix has minimal polynomial of the form $(x-a)$, it is conjugate to a matrix of the first form; otherwise, it becomes one of the second form. For two different eigenvalues, one obtains the third form. Finally, since it is not unreasonable to consider that $\mathbb{F}_q$ is not algebraically closed, we have the fourth form, which accounts for the possibility of a characteristic polynomial with a root outside $\mathbb{F}_q$.

$$\begin{bmatrix} a & 0 \\ 0 & a \end{bmatrix} (4.1) \quad \begin{bmatrix} a & 1 \\ 0 & a \end{bmatrix} (4.2) \quad \begin{bmatrix} a & 0 \\ 0 & d \end{bmatrix} (4.3) \quad \begin{bmatrix} b & dx \\ d & b \end{bmatrix} (4.4)$$

with entries satisfying $a \neq d$ and $a,\ d \neq 0$ and where x is an element of a second-degree field extension over $\mathbb{F}_q$ as suggested[5]. Calculating the total number of conjugacy classes from these forms is straightforward: there are $q-1$ nonzero elements of $\mathbb{F}_q$ and thus $q-1$ conjugacy classes of each of the first two forms. Similarly, in the third form, there are $q-1$ possible values for a, and selection of a restricts a choice of d. Bearing in mind that interchanging the basis vectors for a matrix is easily accomplished by conjugation, we divide this product by two in order to prevent double-counting classes and arrive at $\frac{1}{2}(q-1)(q-2)$ classes of the third form. Similar logic leads us to believe there are $\frac{1}{2}(q)(q-1)$ classes of the fourth form, which turns out to be correct for slightly more complicated reasons[3, 2]. Then $GL_2(\mathbb{F}_q)$ possesses, all together, q^2-1 conjugacy classes and thus irreducible representations.

4.1. **Type I.** The simplest representations to manage are, as previously suggested, those which are one-dimensional. With this in mind, we turn to a familiar character for the first type of irreducible representation: the determinant. By definition, the determinant takes matrices to single elements of the field whence we obtained the entries of the matrix, and so we have a map from $GL_2(\mathbb{F}_q)$ into $GL_1(\mathbb{F}_q)$. In fact, composing some homomorphism $\phi : \mathbb{F}_q^* \to \mathbb{C}^*$ with the determinant also defines an irreducible character.

Example 2. Letting $q = 2$ or 3, it is simple to check that any character of the form $\phi\circ$ det satisfies Theorem 2.i. For $q = 2$, 1 is the only possible determinant, so the inner product of the character becomes $\frac{1}{g}\sum_{t\in\mathcal{G}} |1^2|$, which is equal to 1 as desired. Letting $q = 3$, the possible values for the determinant are 1 or 2, but each

[5]Note that all such extensions are isomorphic, so one need not specify a choice of x

yields 1 when squared. Thus, we obtain the same sort of sum. In $\mathbb{F}_5$, there are field elements of order greater than two, and so things become more interesting.

First, note that elements of $\mathbb{F}_q^*$ must have finite order, i.e. $x \in \mathbb{F}_q^*$ has $x^n = 1$ for some $n|q-1 < \infty$. Since ϕ is a homomorphism, the same fact must hold for $\phi(x) \in \mathbb{C}^*$. Namely, $\phi(x)$ must be a $q-1^{\text{st}}$ root of 1, which we will denote $\zeta_{q-1}^k = e^{2ki\pi/(q-1)}$ for $1 \leq k \leq n$. For readers without a background in complex analysis, it is my hope the following calculations prove illuminating (as they did for me); more experienced readers may feel free to skip them.
The sum from Theorem 3.2.i becomes

$$\frac{1}{g}\sum_{j=1}^{g} \zeta_{q-1}^j \cdot \overline{\zeta_n^j} \tag{4.5}$$

Making the substitution $e^{ix} = cos(x) + i \cdot sin(x)$ with our original definition for ζ_n yields

$$\frac{1}{g}\sum_{j=1}^{g}(cos(\frac{2ji\pi}{q-1}) + i \cdot sin(\frac{2ji\pi}{q-1}))(cos(\frac{2ji\pi}{q-1}) - i \cdot sin(\frac{2ji\pi}{q-1})) \tag{4.6}$$

Finally, expanding and applying an identity from trigonometry supplies the desired result:

$$= \frac{1}{g}\sum_{j=1}^{g} cos^2(\frac{2ji\pi}{q-1}) + sin^2(\frac{2ji\pi}{q-1}) = \frac{1}{g}\sum_{j=1}^{g} 1 = 1 \tag{4.7}$$

Thus we see that characters of this type are clearly irreducible. Further, since $\mathbb{F}_q^*$ is cyclic, any homomorphism ϕ is determined by where it sends a cyclic generator of the group. There are $q-1$ roots of unity and thus possible maps (given a generator). Suppose, however, that a and b each generate $\mathbb{F}_q^*$, and let n be the power such that $a^n = b$. Whatever maps are produced by b are thus also produced by a, so that one need only consider the maps obtained from a single cyclic generator. Thus Type I yields precisely $q-1$ irreducible characters.

4.2. **Type II.** In order to introduce the next type of character, we define, as before, some homomorphism $\phi : \mathbb{F}_q \to \mathbb{C}^*$. Instead of composing ϕ with the determinant, however, the character will simply take on the value of $\phi(ad)$, i.e. the value of the homomorphism evaluated at the product of the elements on the main diagonal. Note, however, that this definition does not give rise only to irreducble characters. A Type II character on $\mathcal{G}$ might be considered as a character of Type I on the Borel subgroup $\mathcal{B} \subset GL_2(\mathbb{F}_q)$, which consists of matrices of the form

$$\begin{bmatrix} a & b \\ 0 & d \end{bmatrix} \text{ with } a, b, d \in \mathbb{F}_q \tag{4.8}$$

For elements of the Borel subgroup, the product ad is the determinant. Thus, in order to restrict Type II characters so that we only obtain new, irreducible representations, we must remove Type I characters from this collection. Once again, we are left with $q-1$ unique irreducible representations.

4.3. **Remaining Types.** The constructions of Types III and IV rely heavily on the introduction of Cartan subgroups, which derive from conjugates of basis vector matrices for a quadratic extension $\mathcal{K}$ of $\mathbb{F}_q$[3]. As one might hope, there are precisely $\frac{1}{2}(q-1)(q-2)$ characters of Type III and $\frac{1}{2}q(q-1)$ of Type IV, corresponding nicely to the third and fourth conjugacy classes above[2]. Thus we obtain q^2-1 irreducible representations of $GL_2(\mathbb{F}_q)$; by Theorem 3.3, we have found all of them.

General Type	Number of Irr. Representations
Type I	$q-1$
Type II	$q-1$
Type III	$\frac{1}{2}(q-1)(q-2)$
Type IV	$\frac{1}{2}q(q-1)$

References

[1] D. S. Dummit and R. M. Foote. Abstract Algebra, Third Edition. John Wiley & Sons, Inc. 2004.
[2] W. Fulton and J. Harris. Representation Theory: A First Course. Springer. 1991.
[3] Serge Lang. Algebra, Third Edition. Addison-Wesley. 1993.
[4] J.-P. Serre. Linear Representations of Finite Groups. Springer-Verlag. 1977.