The General Linear Group: Finding 2×2 integer matrix representations of finite groups.

Alec Zabel-Mena

April 1, 2020

Abstract

One of the most well known example of a group is the dihedral group of symmetries of an n-gon; usually denoted by D_n or D_{2n}. It is interesting to note then that the dihedral group can be represented by 2×2 matrices; particularly 2×2 integer matrices. In fact Mackiw brings this up in his paper, and poses the question: what are all the finite groups that can be realized using 2×2 integer matrices? It is the goal of this paper to provide a more detailed explanation of Mackiw's paper. The central idea is to build a group of 2×2 integer matrices, and observe its finite subgroup structure. The outcome will be providing a proof to the theorem above; which answers the question of what groups can be represented by such matrices. There are two groups in particular, the "general linear group" and the "special linear group", which will be the two groups of matrices we will be studying. We study the group structures of these two groups, and since we are interested in finite subgroups of matrices, we will build their finite analogues.

1 Introduction

One of the most well known example of a group is the dihedral group of symmetries of an n-gon; usually denoted by D_n or D_{2n}. The basic introduction to this group involves illustrating a regular n-gon, and visualizing two operations that act on its vertices. One operation, τ, flips the n-gon about an axis of symmetry (either vertically or horizontally), the other operation, ρ, rotates the the n-gon about an angle of $2\pi/n$,. You can go even further by embedding the n-gon in the real plane, where its vertices are now points in the plane. We can then visualize our operations τ and ρ as matrix operations, that takes points on the plane to other points on

the plane. Mackiw in a paper (see [4]) provides the matrices:

$$F = \begin{pmatrix} -1 & -1 \\ 0 & 1 \end{pmatrix} \text{ and } R = \begin{pmatrix} 0 & -1 \\ 1 & 1 \end{pmatrix}$$

as operations of the dihedral group; where F represents the flip about the axis of symmetry (about the y-axis [4]) and R represents the rotation about an angle of $2\pi/n$.

It is interesting to note then that the dihedral group can be represented by 2×2 matrices; particularly 2×2 integer matrices. In fact Mackiw brings this up in his paper, and poses the question: what are all the finite groups that can be realized using 2×2 integer matrices? And the main result given is the following theorem:

Theorem. *A finite group G can be represented as a group of 2×2 invertible matrices if and only if G is isomorphic to D_8 or D_{12}.*

It is the goal of this paper to provide a more detailed explanation of Mackiw's paper. The central idea is to build a group of 2×2 integer matrices, and observe its finite subgroup structure. The outcome will be providing a proof to the theorem above; which answers the question of what groups can be represented by such matrices.

There are two groups in particular, the "general linear group" and the "special linear group", which will be the two groups of matrices we will be studying. We study the group structures of these two groups, and since we are interested in finite subgroups of matrices, we will build their finite analogues. We will then go to study the group structure of these finite analogue, in particular, the subgroup structure of the analogue for the special linear group.

In terms of terminology, the usual terminology and notation for group theory, as well as that for linear algebra will be used; i.e. $H \leq G$ means that H is a subgroup of G and $H \trianglelefteq G$ means that H is a normal subgroup of G. We also denote two groups G and H being isomorphic by writing $G \simeq H$. We also use D_{2n} to denote the dihedral group.

2 Preliminaries

To study the general linear group and the special linear group, only elementary knowledge of group theory and linear algebra should be assumed. The most obvious are those from group theory. We recall that for a homomorphism $\phi : G \to H$ the kernel of ϕ is the set $\ker \phi = \{g \in G : \phi(g) = e_H\}$ (e_H the identity element of H); it is well known that $\ker \phi$ is a normal subgroup of G [2], a fact which we will use when proving normality. It is also well

known that the index of a subgroup H in G is defined to be the number of right cosets of H in G, and is denoted $[G : H]$. Particularly if both H and G are finite, then $[G : H] = |G|/|H|$.

As the paper by Mackiw suggest, the most obvious definition to make is that of the dihedral group. The **dihedral group** is the group D_{2n} of elements τ and ρ such that $\tau^2 = \rho^n = e$ and $\tau\rho\tau = \rho^{-1}$, it is well known that this group has $2n$ elements. There are less obvious definitions that we should also go over as well. Let G be a group and let $H \leq G$, Defining $gHg^{-1} = \{ghg^{-1} : h \in H\}$, the **normalizer** of H into G is the set $N(H) = \{g \in G : gHg^{-1} = H\}$.

We also recall elementary definitions from linear algebra. The essential definitions include those of the trace of a matrix, and eigenvalues of a matrix. Let $A = (a_{ij})$ be an $n \times n$ matrix, the the **trace** of A is the scalar $\operatorname{Trace} A = a_{11} + a_{22} + \cdots + a_{nn}$ [3]; that is, the trace is the sum of the diagonal entries of the matrix. Like wise, if A is a matrix over a field F, then a scalar $\lambda \in F$ is an **eigenvalue** if the matrix $A - \lambda I$ is not invertible. That is $\det(A - \lambda I) = 0$. Given a vector v, v is an **eigenvector** if $Av = \lambda v$ [3]. We call A a diagonal matrix if $(a_{ij}) = 0$ for $i \neq j$ (i.e. it is a matrix who's only nonzero entries are the diagonal ones) [2]. Two matrices A and B are **similar** if for an invertible matrix X, $XAX^{-1} = B$ We call A **diagonalizable** if A is similar to a diagonal matrix [3].

Lastly we would like to define an n-th **root of unity** to be a complex number ω such that $\omega^n = 1$ and $\omega^m \neq 1$ for $0 < m < n$. Aside from these definitions, and a basic understanding of both linear and abstract algebra, not much else is needed to begin the study of groups of matrices. There are some additional groups we would like to consider aside from D_{2n}, namely the Quaternion group $\mathbb{H}$, Whose elements are numbers of the form $a + bi + cj + dk$ where $i^2 = j^2 = k^2 = ijk = -1$ and $ij = k, jk = i, ki = j$ [2], and the Klein-4 group $\mathbb{Z}/2\mathbb{Z} \times \mathbb{Z}/2\mathbb{Z}$. Really all that there is to know about these two groups here is that $\mathbb{H}$ is nonabelian, and is generated by two elements A, B where $BAB^{-1} = A^{-1}$, and $|\mathbb{Z}/2\mathbb{Z} \times \mathbb{Z}/2\mathbb{Z}| = 4$ contains 3 subgroups of order 2 [1].

3 The groups $GL(2, \mathbb{Z})$ and $SL(2, \mathbb{Z})$

We begin by observing sets of 2×2 matrices. Let $GL(2, \mathbb{Z})$ be the group of invertible 2×2 integer matrices whose inverses have integer entries [4]; We would like to be able to see what kind of elements are in this group; i.e, what are the properties of a matrix that warrant group membership. If $A \in GL(2, \mathbb{Z})$, then A has an inverse A^{-1} with integer entries, hence A^{-1} is also in $GL(2, \mathbb{Z})$. Observe that since $A \in GL(2, \mathbb{Z})$ then $\det A \neq 0$, necessarily, we also have that $\det A^{-1} \neq 0$. Moreover, observe that $\det I = \det AA^{-1} = \det A \det A^{-1} = 1$ Then since both A and A^{-1} are integer matrices, it must be that $\det A = \det A^{-1} = \pm 1$; hence we make our first

observation of $GL(2,\mathbb{Z})$ namely that $GL(2,\mathbb{Z}) = \{A \in \mathbb{Z}^2 : \det A = \pm 1\}$. This observation has an immediate consequence. Let $SL(2,\mathbb{Z}) = \{A \in GL(2,\mathbb{Z}) : \det A = 1\}$. It's easy to show that $SL(2,\mathbb{Z})$ is a subgroup of $GL(2,\mathbb{Z})$ by using the fact that $\det A = 1$, we can go a step further and assert that $SL(2,\mathbb{Z}) \trianglelefteq GL(2,\mathbb{Z})$ i.e. normal in $GL(2,\mathbb{Z})$ for: Define the homomorphism $\phi : GL(2,\mathbb{Z}) \to \mathbb{Z}$ by taking $A \to \det A$. Then $\ker \phi = \{A \in GL(2,\mathbb{Z}) : \det A = 1\} = SL(2,\mathbb{Z})$. Since kernels are normal, this makes $SL(2,\mathbb{Z})$ normal. We can also observe that for every $A \in GL(2,\mathbb{Z})$, $ASL(2,\mathbb{Z})$ and $A^{-1}SL(2,\mathbb{Z})$ are the only two distinct right cosets of $SL(2,\mathbb{Z})$ in $GL(2,\mathbb{Z})$ and so $[GL(2,\mathbb{Z}) : SL(2,\mathbb{Z})] = 2$.

The group $GL(2,\mathbb{Z})$ is called the **general linear group** of degree 2, and its normal subgroup $SL(2,\mathbb{Z})$ is called the **special linear group** of degree 2 [1]. We can likewise define the following $GL(n,\mathbb{Z})$ to be the general linear group of degree n. Here, the degree denotes the dimension of the matrix, so $GL(3,\mathbb{Z})$ would refer to the group of all 3×3 invertible integer matrices. Since we are only interested in studying groups of 2×2 integer matrices, we restrict ourselves to $n = 2$.

The goal of studying $GL(2,\mathbb{Z})$ and $SL(2,\mathbb{Z})$ is to be able to classify their finite subgroups [4]. It is then sensible to look at finite elements of these two groups. If we consider a matrix $A \in GL(2,\mathbb{Z})$ of order n, then $A^n = I$, and looking at the eigenvalues of A, they must be n-th roots of unity and hence complex. We claim then that A must be diagonalizable, for if not, then A has repeated eigenvalues. Let λ be such an eigenvalue, and let v be the associated eigenvector. We then choose any vector w such that $\{w, v\}$ is a basis over $\mathbb{C}^2$. Then the matrix of the linear transformation determined by A has the form $T = \begin{pmatrix} \lambda & a \\ 0 & b \end{pmatrix}$ With $a \neq 0, b \in \mathbb{C}$. The characteristic polynomial (that is the polynomial determined by $\det(A - \lambda I) = 0$) is $(x - \lambda)^2$, we get that $b = \lambda$. We see that T is of infinite order, and similar to A, and so A also has infinite order, a contradiction since $\operatorname{ord} A = n$. Thus A must be diagonalizable. One direct observation we can make from this, is if $A \in SL(2,\mathbb{Z})$ and $\operatorname{ord} A = 2$, then $A = \begin{pmatrix} -1 & 0 \\ 0 & -1 \end{pmatrix}$. This proves that $SL(2,\mathbb{Z})$ has a unique element of order 2. This also says that there is one element of order 2, in $GL(2,\mathbb{Z})$ with $\det = 1$. What can we observe of elements with order greater than 2?

Proposition 3.1 ([4])**.** *Every element of $GL(2,\mathbb{Z})$ of order greater than 2 has determinant 1.*

Proof. Let A have order greater than 2, We have that ± 1 are the only complex roots of unity that are also real, and since $A^2 \neq I$, then at least one eigenvalues of A is not real. We also have that the characteristic polynomial has integer coefficients, then the eigenvalues are complex conjugates $\lambda, \bar{\lambda}$; so $\lambda\bar{\lambda} = 1$. Thus $\det A = 1$. ∎

This means that any element of order 2 in $GL(2,\mathbb{Z})$ has determinant $\det = -1$, with the exception of the unique element of order 2 of $SL(2,\mathbb{Z})$.

4 The Groups $GL(2,3)$ and $SL(2,3)$

One advantage of groups of integer matrices, is that: much how we can reduce $\mathbb{Z}$ to $\mathbb{Z}/p\mathbb{Z}$ for some prime p, we can do the same to these groups of integer matrices. We usually reduce $\mathbb{Z}$ to $\mathbb{Z}/p\mathbb{Z}$ by taking $a \to a \mod p$. We use this same map. Define $GL(2,p) = \{A \in (\mathbb{Z}/p\mathbb{Z})^2 : \det A \equiv \pm 1 \mod p\}$ and $SL(2,p) = \{A \in GL(2,p) : \det A \equiv 1 \mod p\}$; then we take $GL(2,\mathbb{Z}) \to GL(2,p)$ and $SL(2,\mathbb{Z}) \to SL(2,p)$ by taking $A \to A \mod p$. Hence, just how we go from $\mathbb{Z}$ which is infinite, to $\mathbb{Z}/p\mathbb{Z}$, which is finite, we form finite counterparts of $GL(2,\mathbb{Z})$ and $SL(2,\mathbb{Z})$. This is a good step forward into classifying finite subgroups of the general and special linear groups. In fact, if we consider when $p = 3$, and look to the group $SL(2,3)$, we get a useful result.

Theorem 4.1 ([4])**.** *Let G be a finite subgroup of $GL(2,\mathbb{Z})$, and let $G^+ = G \cap SL(2,\mathbb{Z})$, then the map $G^+ \to SL(2,3)$ is a homomorphism and is 1-1.*

Proof. Now, if G is a finite subgroup, and $G^+ = G \cap SL(2,\mathbb{Z})$, we have that G^+ is the subset of elements of $\det = 1$. Hence $G^+ \leq SL(2,\mathbb{Z})$. Then take the map $\psi : G^+ \to SL(2,\mathbb{Z})$ by $A \to A \mod 3$; then ψ is a homomorphism.Let $A \in \ker\psi$. Let α be the unique element of order 2 of $SL(2,\mathbb{Z})$, we notice then that $\alpha \not\equiv I \mod 3$, so A must have order greater than 2. We also get that $\operatorname{Trace} A \equiv 2 \mod 3$. Let ω and $\bar{\omega}$ be the complex eigenvalues of A, where ω is an n-th root of unity. We have now that the trace of a matrix is also equal to the sum of its eigenvalues [2], so: $|\operatorname{Trace} A| = |\omega + \bar{\omega}| \leq |\omega| + |\bar{\omega}| \equiv 2 \mod 3$, thus $\operatorname{Trace} A = -1$. So we get that $A = \begin{pmatrix} a & b \\ c & -1-a \end{pmatrix}$. Since $A \in \ker\psi$, $b = c \equiv 0 \mod 3$, and hence $bc \equiv 0 \mod 3$. We also have that since $A \in G^+$, we get $-a(1+a) - bc = 1$, reducing this modulo 3 we get $a^2 + a + 1 \equiv 0 \mod 3$, whose only solution is $a = 1$. We have established that if $A \in \ker\psi$, then $A = I$; therefore ψ is 1-1. ∎

What this theorem says that G^+ taken modulo 3 (a similar argument can be made for any prime p) is a subgroup of $SL(2,3)$. We now have a finite analogue of a subgroup in $SL(2,3)$. All that is left to consider is the orders of both $GL(2,p)$ and $SL(2,p)$. We do this by recalling a fundamental theorem from group theory:

Theorem 4.2 (The Fundamental Theorem of Group Homomorphisms [2])**.** *Let G and H be groups and let $\phi : G \to H$ be a homomorphism of G onto H. Then $G/\ker\phi \simeq H$*

Consider now the homomorphism $\phi : GL(2,p) \to U(\mathbb{Z}/p\mathbb{Z})$ (Where $U(\mathbb{Z}/p\mathbb{Z})$ is the group of units of $\mathbb{Z}/p\mathbb{Z}$) by $A \to \det A$. Then by similar arguments to that used for $SL(2,\mathbb{Z})$, it follows that $\ker\phi = SL(2,p)$ (and $SL(2,p) \trianglelefteq GL(2,p)$) by this same homomorphism. Thus by the fundamental theorem of group homomorphisms:

$$GL(2,p)/SL(2,p) \simeq U(\mathbb{Z}/p\mathbb{Z}) \tag{1}$$

Therefore:

$$\frac{|GL(2,p)|}{|SL(2,p)|} = |U(\mathbb{Z}/p\mathbb{Z})| = p-1 \tag{2}$$

This give us that:

$$|SL(2,p)| = \frac{|GL(2,p)|}{p-1} \tag{3}$$

All that is left is to count $GL(2,p)$:

Let $A = \begin{pmatrix} a & b \\ c & d \end{pmatrix} \in GL(2,p)$. We have that $|(\mathbb{Z}/p\mathbb{Z})^2| = p^2$. Notice that $\det A = 0$ precisely when $ad = bc$. We have that a, b, c, d clearly cannot all be 0, so to exclude the possibility that $\det A = 0$, we arrive to $p^2 - 1$ possible entries for the column $\begin{pmatrix} a \\ c \end{pmatrix}$. Now if we fix a and c, we notice that $b = (c^{-1}a)d$ and $d = (a^{-1}c)b$ which are multiples of $\begin{pmatrix} a \\ c \end{pmatrix}$, and since $a, c \in \mathbb{Z}/p\mathbb{Z}$, there are p such multiples So we find that there are $p^2 - p$ possible entries for the column $\begin{pmatrix} b \\ d \end{pmatrix}$. Thus there are $(p^2-1)(p^2-p)$ possible entries for any matrix in $GL(2,p)$, that is $|GL(2,p)| = (p^2-1)(p^2-p)$. Then we get that:

$$SL(2,p) = \frac{(p^2-1)(p^2-p)}{p-1} = p(p^2-1) \tag{4}$$

In particular, when $p = 3$, $|SL(2,3)| = 24$.

This is perhaps the most important result of our study of groups of matrices. With the order of $SL(2,p)$ known, we can enumerate all its elements, and discern some facts about its subgroups; we also have a way of directly knowing the index of a given subgroup in $SL(2,p)$; this will prove useful when further observing the subgroup structure of $GL(2,\mathbb{Z})$.

5 Subgroups of $GL(2,\mathbb{Z})$ and $SL(2,3)$

We are now in a position to find subgroups of $SL(2,p)$; we wish to consider however, only $SL(2,3)$ and its subgroups.

Lemma 5.1 ([4])**.** *The following are true:*

(1) $SL(2,3)$ *contains a unique element of order 2.*

(2) Let $T = \{\begin{pmatrix} 1 & a \\ 0 & 1 \end{pmatrix} : a \in \mathbb{Z}/3\mathbb{Z}\}$*. Then* T *is a subgroup of order 3, and its normalizer* $N(T)$ *is a cyclic group of order 6.*

(3) $SL(2,3)$ *contains a subgroup of order 8 isomorphic to the quaternion group* $\mathbb{H}$*.*

Proof. 1. By the diagonalization argument used for $SL(2,\mathbb{Z})$, it follows that there is a unique element α of order 2 in $SL(2,3)$.

2. Let $T = \{\begin{pmatrix} 1 & a \\ 0 & 1 \end{pmatrix} : a \in \mathbb{Z}/3\mathbb{Z}\}$. Then $a \equiv 0, 1, 2 \mod 3$, hence the only possible elements of T are I, $\begin{pmatrix} 1 & 1 \\ 0 & 1 \end{pmatrix}$ and $\begin{pmatrix} 1 & 2 \\ 0 & 1 \end{pmatrix} = \begin{pmatrix} 1 & 1 \\ 0 & 1 \end{pmatrix}^{-1}$. Hence T is a subgroup, and $|T| = 3$. Now fix a and consider $N(T) = \{g \in SL(2,3) : gTg^{-1} = T\}$. $\det g = bd - ac = 1$ (for integers b, c, d modulo 3), then $b = d^{-1}$, and $c = 0$ necessarily So g and g^{-1} must have the form:
$$g = \begin{pmatrix} b & a \\ 0 & b \end{pmatrix} \text{ and } g^{-1} = \begin{pmatrix} b & 0 \\ -a & b \end{pmatrix}$$
Then if $gTg^{-1} = T$, then $b = \pm 1$ (the necessary relations for a follow). Now since there are 3 choices for a, and 2 choices for b, we get there are 6 possible choices for $g \in N(T)$, hence $|N(T)| = 6$. Choosing g to be: $g = \begin{pmatrix} -1 & 2 \\ 0 & -1 \end{pmatrix}$ with $b = -1$ and $a = 2$, we get that $g^6 = I$. Thus g is a generator for $N(T)$.

3. Let $A = \begin{pmatrix} 0 & 1 \\ -1 & 0 \end{pmatrix}$ and $B = \begin{pmatrix} -1 & -1 \\ -1 & 1 \end{pmatrix}$, we see that $\operatorname{ord} A = \operatorname{ord} B = 4$, and $A^2 = B^2 = \begin{pmatrix} -1 & 0 \\ 0 & -1 \end{pmatrix}$ and $BAB^{-1} = A^{-1}$, thus A and B both generate $\mathbb{H}$.

■

Now since $[SL(2,3) : N(T)] = 4$, The subgroup T (as in the lemma) has 4 distinct conjugates T_1, T_2, T_3, T_4, and the normalizers of these conjugates yield 4 cyclic subgroups each of order 6, where each contains the unique element of order 2 and a subgroup of order 3 [4]. Then these 4 subgroups of order 6, plus the quaternion group $\mathbb{H}$ enumerate $SL(2,3)$. In particular, $SL(2,3)$ has: eight elements of order 6, eight elements of order 3, the unique element of order 2, six elements of order 4, and the identity element. We are now in a position to prove:

Theorem 5.2 ([4]). *$SL(2,3)$ contains:*

(1) No subgroup of order 12.

(2) A unique subgroup of order 8.

(3) No nonabelian subgroup of order 6.

(4) cyclic subgroups of orders 3,4 and 6.

(5) No subgroup isomorphic to the Klein 4 group

(6) A unique subgroup of order 2.

Proof. In the paper of [4], only the assertions (1), (2), and (4) are established. Hence we will prove the assertions (3), (5), and (6).

Let $G \leq SL(2,3)$ be a nonabelian group of order 6 (the $[SL(2,3) : G] = 4$), and let α be the unique element of order 2. Since $|G| = 6$, G must contain α, on the other hand, no element $g \in G$ has order 6, as that would make it a generator. Now again by the order of G, G contains as well an element of order 3, hence choose $G \in G$ with $\operatorname{ord} g = 3$. Since α and g are elements of G then so is $g\alpha$; notice then that $(g\alpha)^6 = (g^3)^2(\alpha^2)^3 = I$, making $g\alpha$ a generator. This is a contradiction to the assumption that G has no generating element. Thus $g\alpha$ make G cyclic and hence an abelian group.

We now take the unique element α, since $\operatorname{ord} \alpha = 2$, it is its own inverse, hence $(\alpha) = \{I, \alpha\}$ is a cyclic subgroup of order 2. Now since α is unique, there is no other element of order 2 in $SL(2,3)$, thus (α) is the only subgroup of order 2.

We can use assertion (6) to prove assertion (5). Recall that $\mathbb{Z}/2\mathbb{Z} \times \mathbb{Z}/2\mathbb{Z}$ has three subgroups of order 2. If $G \leq SL(2,3)$ such that $G \simeq \mathbb{Z}/2\mathbb{Z} \times \mathbb{Z}/2\mathbb{Z}$, then G also has three subgroups of order 2; which contradicts assertion (6). There can be no subgroup isomorphic to the Klein 4 group. ■

We can now go on to observe the subgroups of $GL(2,\mathbb{Z})$. We observe first that the only nonabelian groups of $SL(2,3)$ are $SL(2,3)$ itself and the quaternion group $\mathbb{H}$. Then:

Proposition 5.3. *Let $G \leq GL(2,\mathbb{Z})$. Then G^+ is cyclic.*

Proof. Suppose not; and suppose first that $G^+ \simeq \mathbb{H} \leq SL(2,3)$. Take the homomorphism $\phi : G^+ \to SL(2,2)$. We then have that $|SL(2,2)| = 6$, so $\ker \phi$ contains an element of order 4, hence let A be such an element. Then A has eigenvalues i and $-i$, hence $\operatorname{Trace} a = 0$, that is: $A = \begin{pmatrix} a & b \\ c & -a \end{pmatrix}$. Since $A \in \ker \phi$, $b = c \equiv 0 \mod 2$, and hence $bc \equiv 0 \mod 4$. Then

we get $\det a = -a^2 - bc = 1$, reducing modulo 4 we get that $a^2 \equiv -1 \mod 4$. Now again by the location of A, we must have that $a \not\equiv 0 \mod 2$ and so $a \not\equiv 0 \mod 4$, which makes a odd. However this is a contradiction of the fact that $a^2 \equiv -1 \mod 4$, as every odd number is congruent to $1 \mod 4$, thus $G^+ \not\simeq \mathbb{H}$.

Now on the other hand, suppose $G^+ \simeq SL(2,3)$; then G^+ contains a subgroup isomorphic to $\mathbb{H}$, which cannot happen by the above argument. ■

Now since G^+ is cyclic, we have that $|G| \neq 8$ and $|G| \neq 24$, hence G must be isomorphic to one of the following cyclic groups: $(e), C_1, C_2, C_3, C_4$, and C_6. We can now discern more about the structure of G, we showed that in $GL(2,\mathbb{Z})$, the only elements of order 2 are those who have $\det = -1$ (save for the unique element of $SL(2,\mathbb{Z})$ of order 2). We are now in a position to prove the theorem we set out to prove, we first provide a preliminary lemma:

Lemma 5.4. *If $G^+ \neq G$, then $[G : G^+] = 2$.*

Proof. We have that $G \leq GL(2,\mathbb{Z})$, and $G^+ \leq SL(2,\mathbb{Z})$, so $[G : G^+] \leq [GL(2,\mathbb{Z}) : SL(2,\mathbb{Z})] = 2$, so $[G : G^+] = 1$ or $[G : G^+] = 2$. Suppose the former. Then since G is finite and $G^+ = G \cap SL(2\mathbb{Z})$, then G^+ is also finite. Thus:

$$[G : G^+] = \frac{|G|}{|G^+|} = 1$$

So $|G| = |G^+|$, and since $G^+ \subseteq G$, then it must be that $G = G^+$, a contradiction. ■

Theorem 5.5. *A finite group G can be represented as a group of 2×2 invertible matrices if and only if G is isomorphic to D_8 or D_{12}.*

Proof. Let $X \in G$ but not in G^+, then $\det X = -1$, hence $\operatorname{ord} X = 2$. Now consider the coset G^+X, since they consist of matrices of $\det = -1$, then every element of G^+X has order 2. Suppose Y is a generator of X, then $(YX)^2$=I,and since $X = X^{-1}$, we have that $XYX = Y^{-1}$. Now by lemma 5.4, since $[G : G^+]$=2, G is isomorphic to one of the dihedral groups: D_{2i} and G^+ is isomorphic to one of the cyclic groups :C_i for $i = 1, 2, 3, 4, 6$. Then notice that $[D_{2i} : C_i] = 2$. Since D_8 and D_{12} contain the other groups C_i and D_{2i} for $i = 1, 2, 3$, we have that $G \simeq D_8$ or $G \simeq D_{12}$. ■

6 Conclusion

If we want to know whether a group G can be represented by 2×2 integer matrices, it is sufficient to check that $G \simeq D_8$ or that $G \simeq D_{12}$. Hence the task of finding a suitable

integer matrix representation for G reduces to finding an isomorphism from G to the dihedral group of symmetries of a square, or that of a hexagon. However, this analysis is done almost entirely with the real plane in mind. What of 3-space? We may extend the dihedral group to an analogous one in 3-space. Then, if this group does have an integer matrix representation, it must be representable by 3×3 integer matrices. Hence the question now becomes: What are all the finite groups representable by 3×3 integer matrices? What if we choose to extend these notions to $\mathbb{R}^4$, or more generally, $\mathbb{R}^n$? So the question then becomes: Hence the question now becomes: What are all the finite groups representable by $n \times n$ integer matrices?

This suggests that we should study the general linear group and the special linear group in a more general setting; namely letting $GL(n, \mathbb{Z})$ be sets of all $n \times n$ invertible integer matrices whose inverses also have integer entries. Defining $SL(n, \mathbb{Z})$ to be the subgroup of $GL(n, \mathbb{Z})$ of matrices with $\det = 1$, we can generalize the same arguments used for $GL(2, \mathbb{Z})$ and $SL(2, \mathbb{Z})$. and be able to find an answer to a much more broad question. Of course, we would have to first find a group that can be represented by $n \times n$ integer matrices; and such a group may be an n-th dimensional analogue to the dihedral group.

References

[1] Richard M. Foote David S. Dummit. *Abstract Algebra*. John Wiley Sons, Inc., 2004.

[2] I.N. Herstein. *Topics in Algebra*. A Blaisdell Book in The Pure and Applied Sciences. Blaisdell Publishing Company, 1964.

[3] Ray Kunze Kenneth Hoffman. *Linear Algebra*. Prentice-Hall Mathematics Series. Prentice-Hall, Inc., 1961.

[4] George Mackiw. "Finite Groups of 2×2 Integer Matrices". In: *Mathematics Magazine* 69.5 (1996), pp. 356–361.