$$A_1 = \frac{1}{2} - \frac{1}{4} + \frac{1}{8} - \frac{1}{16} + \frac{1}{32} - \frac{1}{64} + \cdots$$

$$A_1 = A_2 = A_3.$$

$$A_1 + A_2 + A_3 = 1.$$

$$\therefore \quad A_1 = \frac{1}{3}.$$

—James O. Chilaka
Long Island University
Brookville, NY 11548

Finite Groups of 2×2 Integer Matrices

GEORGE MACKIW
Loyola College in Maryland
Baltimore, MD 21210

Introduction The story behind this article begins in a classroom, with a presentation intended to show that the dihedral group D_6 of symmetries of the hexagon can be realized as a group of invertible 2×2 matrices with real number entries. Two matrices that can be used to generate this group are

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

R has multiplicative order six and F has order two. There is geometric motivation for this choice of generators. As in Figure 1, picture a regular hexagon centered at the origin; highlight two of its adjacent radii (v_1 and v_2 in Figure 1). Regard these radii as vectors, to form a basis for $\mathbb{R}^2$. Relative to this basis, the matrix R (for "rotation") represents a counterclockwise rotation through 60°, while F (for "flip") corresponds to a reflection of the hexagon through the y-axis.

The set of matrices $\{F^i R^j | i = 0, 1;\ j = 0, 1, \ldots, 5\}$ forms a group isomorphic to D_6. Familiar relations, such as $FRF = R^{-1}$, can either be checked by multiplying matrices

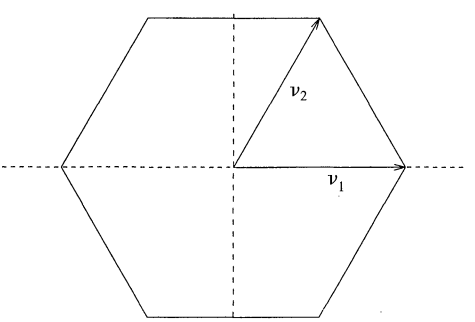

FIGURE 1

or interpreted geometrically. An interesting and attractive feature of this representation of a non-abelian group of order 12 is that all of the matrices have *integer* entries.

Seeing this, a student wondered whether the alternating group A_4, another non-abelian group of order 12, could also be written using integer matrices of size two. I suspected that the answer to this question was well-known, though, sadly, at that moment not by me. Some instinct suggested to me that no such representation was possible, but this was far from proof. To save face, I pointed out that a similar question could be posed for D_4, the group of symmetries of the square. Indeed, elementary arguments show that D_4 can be represented using 2×2 integer matrices. Can the quaternion group, the other non-abelian group of order 8, also be written this way? Better yet, what are *all* the finite groups that can be realized using two by two integer matrices?

Some exploration in the library soon revealed that the possibilities for groups admitting such presentations can be narrowed quite quickly—provided one knows some basic results in the theory of group representations and about degrees of primitive roots of unity over the rationals **[3]**. There remained, then, the challenge of answering the question using only elementary means—say, those available after one semester each of linear and abstract algebra. What follows is an attempt to meet this challenge; an interesting mix of group theory and linear algebra appear along the way.

For any finite group G admitting a matrix representation of the type at hand, the subgroup G^+ of integer matrices of determinant 1 will play a fundamental role. The finite group $SL(2,3)$ of 2×2 matrices of determinant 1 with entries in $\mathbb{Z}_3$, the field with three elements, will prove equally important. In fact, we will show that any such G^+ must be isomorphic to a subgroup of $SL(2,3)$. We will use elementary techniques to find all of the subgroups of $SL(2,3)$, a non-abelian group of order 24. In the process, we will find all possible candidates for a G^+. Once G^+ is known, the structure of the full group G will be easy to determine.

Elements of finite order in $GL(2,\mathbb{Z})$ We denote by $GL(2,\mathbb{Z})$ the group of invertible 2×2 integer matrices whose inverses also have integer entries. We seek to classify the *finite* subgroups of $GL(2,\mathbb{Z})$. If both a matrix A and its inverse have integer entries, then, necessarily, $\det A = \pm 1$, since $\det A^{-1} = 1/(\det A)$. The subset $SL(2,\mathbb{Z})$ of matrices of determinant 1 is a normal subgroup of index two in $GL(2,\mathbb{Z})$.

If a matrix $A \in GL(2,\mathbb{Z})$ has order n, then $A^n = I$ (the identity matrix), so the eigenvalues of A must be nth roots of unity. We claim that such an A must be diagonalizable. If not, then A must have a repeated eigenvalue, say λ. Let v be an eigenvector of A with eigenvalue λ, and choose any vector w so that $\{v, w\}$ is a basis for the complex vector space $\mathbb{C}^2$. Relative to this basis, the matrix of the linear transformation determined by A is of the form $\begin{pmatrix} \lambda & a \\ 0 & b \end{pmatrix}$, for some complex numbers a and b, with $a \neq 0$. Because the characteristic polynomial of A is $(x - \lambda)^2$, we see that $b = \lambda$. Direct computation of powers shows that the matrix $\begin{pmatrix} \lambda & a \\ 0 & \lambda \end{pmatrix}$, which is similar to A over $\mathbb{C}$, has infinite order. But A has finite order, so we have a contradiction. (A shorter but less elementary proof can by given by appealing to the Jordan canonical form.)

One consequence of diagonalizability is that if A has order 2, and $\det A = 1$, then A must be the matrix $\begin{pmatrix} -1 & 0 \\ 0 & -1 \end{pmatrix}$. In other words, $SL(2,\mathbb{Z})$ has a unique element of order 2. Suppose that A has order greater than 2. Since 1 and -1 are the only complex roots of unity which are also real and $A^2 \neq I$, at least one eigenvalue, λ, of A is not real. Moreover, since the characteristic polynomial of A has integer (and

therefore real) coefficients, the eigenvalues of A must be complex conjugates λ and $\bar{\lambda}$, with $\lambda\bar{\lambda} = 1$. But the product of the eigenvalues of a matrix is its determinant, so $\det A = 1$. Thus every element in $GL(2, \mathbb{Z})$ of order greater than 2 has determinant 1.

Reduction mod 3: a mapping into $SL(2,3)$ Our goal is to classify finite subgroups G of $GL(2, \mathbb{Z})$. For any such G, G^+, the subset of elements of determinant 1 in G, is a subgroup of G, with index either 1 or 2. Since G^+ is a finite subset of $SL(2, \mathbb{Z})$, it is tempting to reduce the elements of G^+ mod p, for various primes p. The groups $SL(2, p)$, for p prime, are finite counterparts of $SL(2, \mathbb{Z})$; each consists of 2×2 matrices of determinant 1 over $\mathbb{Z}_p$, the integers mod p. The natural projection from $\mathbb{Z}$ to $\mathbb{Z}_p$ extends to a homomorphism from $SL(2, \mathbb{Z})$ into $SL(2, p)$; it will prove useful to examine the image of G^+ under such a mapping. Indeed, the case $p = 3$ provides a wealth of information.

Suppose that the matrix A, $A \neq I$, is in the kernel of the mapping $G^+ \to SL(2, 3)$. Since $\begin{pmatrix} -1 & 0 \\ 0 & -1 \end{pmatrix}$, the unique matrix of order two, is not congruent to the identity mod 3, A must have order greater than 2. Also $\operatorname{tr}(A)$, the trace of A, must be an integer with $\operatorname{tr} A \equiv 2 \pmod 3$. But the eigenvalues of A are ω and $\bar{\omega}$, where ω is a (non-real) nth root of unity, so $|\operatorname{tr}(A)| = |\omega + \bar{\omega}| < |\omega| + |\bar{\omega}| = 2$. The only possibility, therefore, is $\operatorname{tr}(A) = -1$, and it follows that A has the form $A = \begin{pmatrix} a & b \\ c & -1-a \end{pmatrix}$, for some integers a, b, and c. Now, $b \equiv c \equiv 0 \pmod 3$ since A is in the kernel of the mapping, and so bc must be divisible by 9. Because A is in G^+, $-a(1+a) - bc = 1$. This relation, taken mod 9, yields $a^2 + a + 1 \equiv 0 \pmod 9$; a direct check shows that no such integer a exists. We have established the following result.

THEOREM 1. *Let G be a finite subgroup of $GL(2, \mathbb{Z})$ and let $G^+ = G \cap SL(2, \mathbb{Z})$. Then the mapping from G^+ to $SL(2, 3)$ is an injective homomorphism.*

Thus G^+ is isomorphic to a subgroup of $SL(2, 3)$, so the latter group merits a closer look.

The order of $SL(2,3)$ We will compute the order of $SL(2, p)$ for any prime p, and then specialize to $p = 3$. Clearly, $SL(2, p)$ is a subgroup of $GL(2, p)$, the full group of invertible 2×2 matrices with entries in $\mathbb{Z}_p$. For any prime p, the orders of $GL(2, p)$ and $SL(2, p)$ are related by $|SL(2, p)| = |GL(2, p)|/(p-1)$. This can be seen by applying the fundamental theorem of group homomorphisms to the mapping ϕ: $GL(2, p) \to Z_p^*$, given by $\phi(A) = \det(A) \bmod p$, where Z_p^* is the multiplicative group of non-zero elements of $\mathbb{Z}_p$ (Z_p^* has order $p-1$). The kernel of ϕ is $SL(2, p)$.

The order of $GL(2, p)$ can be found by a direct count. A matrix in this group can have any of the $(p^2 - 1)$ non-zero vectors in Z_p^2 as its first column; the second column can be any vector other than one of the p multiples of the first column—a total of $p^2 - p$ choices. This shows that $|GL(2, p)| = (p^2 - 1)(p^2 - p)$; therefore $|SL(2, p)| = p(p^2 - 1)$. In particular, $SL(2, 3)$ has order 24.

$SL(2,3)$ and its subgroups We now proceed to find the subgroups of this group.

LEMMA.

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

(2) *$T = \left\{ \begin{pmatrix} 1 & a \\ 0 & 1 \end{pmatrix} | a \in Z_3 \right\}$ is a subgroup of order 3. Its normalizer, $N(T)$, is a cyclic group of order six.*

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

Proof. The argument used above to show that $SL(2,\mathbb{Z})$ has a unique element of order two can be used here to establish (1).

In (2), T is clearly a subgroup of order 3. Direct computation shows that elements of $N(T)$ must be of the form $\begin{pmatrix} b & a \\ 0 & b \end{pmatrix}$, where $a \in \mathbb{Z}_3$ and b is either 1 or -1. The matrix $\begin{pmatrix} -1 & -1 \\ 0 & -1 \end{pmatrix}$ has order six and generates $N(T)$.

For (3), let $A = \begin{pmatrix} 0 & 1 \\ -1 & 0 \end{pmatrix}$ and $B = \begin{pmatrix} -1 & -1 \\ -1 & 1 \end{pmatrix}$. Direct calculation shows that A and B have order 4, $A^2 = B^2 = \begin{pmatrix} -1 & 0 \\ 0 & -1 \end{pmatrix}$ (the unique element of order two), and $BAB^{-1} = A^{-1}$. Thus A and B generate a quaternion group of order 8.

Let T be defined as in the Lemma. In any finite group, the number of conjugates of a subgroup is the index in the group of the normalizer of the subgroup (for example, see [**4**, p. 52]). Since $N(T)$ has index 4 in $SL(2,3)$, the subgroup T has four distinct conjugates $T_1, \ldots, T_4$ in $SL(2,3)$. The normalizers of these four conjugates of T yield four distinct cyclic subgroups of order 6: $S_i = N(T_i)$, $i = 1, \ldots, 4$. Each S_i contains the unique element of order two and a single subgroup of order three. Thus, if $i \neq j$, $|S_i \cap S_j| = 2$.

These four subgroups of order six thus account for 18 elements of $SL(2,3)$: 8 elements of order 6, 8 elements of order 3, the single element of order 2, and the identity. The quaternion subgroup from the Lemma above contributes 6 elements of order four. We have now enumerated all 24 of the elements of $SL(2,3)$. In particular, $SL(2,3)$ contains no elements of order 8 or 12. We can now describe the subgroup structure of $SL(2,3)$.

THEOREM 2. *$SL(2,3)$ contains*

(1) *no subgroup of order* 12;
(2) *a unique subgroup of order* 8 (*isomorphic to the quaternion group*);
(3) *no non-abelian subgroup of order* 6;
(4) *cyclic subgroups of orders* 3, 4, *and* 6;
(5) *no subgroup isomorphic to Klein's four group*[1];
(6) *a unique subgroup of order* 2.

Proof. Let α be the unique element of order two in $SL(2,3)$. Suppose there were a subgroup H of order 12. Since H has even order, H must contain α [**4**, p. 17, Ex. 2.18]. Since H has index 2, it must contain the square of any element in $SL(2,3)$. If A is any element of order 3, then A is a square since $A = A^4 = (A^2)^2$. Thus, H must contain all eight elements of order 3. Since α commutes with elements of order 3, multiplying them by α produces 8 more elements of order 6 in H. This places at least seventeen elements in H—a contradiction.

To establish (2), recall that $SL(2,3)$ contains only one element of order 2, no element of order 8, and 6 elements of order 4. Thus, any subgroup of order 8 must contain the six elements of order 4 that generate the quaternion subgroup of the Lemma. Assertions (3), (5) and (6) follow from the fact that $SL(2,3)$ contains only one element of order 2. We have established (4) above.

Observe that our analysis of subgroup structure did not require use of the Sylow theorems.

---

[1]Named after the mathematician Felix Klein, this is the non-cyclic group of order four and is isomorphic to $\mathbb{Z}_2 \times \mathbb{Z}_2$.

The finite subgroups of $GL(2,\mathbb{Z})$ There are only two non-cyclic subgroups of $SL(2,3)$: the quaternion subgroup of order 8 and $SL(2,3)$ itself. If G is a finite subgroup of $GL(2,\mathbb{Z})$, we have seen that G^+ is isomorphic to a subgroup of $SL(2,3)$. We now show that G^+ must be cyclic.

Suppose, instead, that G^+ is isomorphic to the quaternion group of order 8. To derive a contradiction, we reduce G^+ mod 2, producing a homomorphism ϕ: $G^+ \to SL(2,2)$. Since $SL(2,2)$ has order 6, the kernel of ϕ must contain an element, A, of order 4. As we observed earlier, the eigenvalues of A are i and $-i$ (two of the complex fourth roots of unity). Thus, A has trace zero, and so must be of the form $\begin{pmatrix} a & b \\ c & -a \end{pmatrix}$ for some integers a and b. Now, $b \equiv c \equiv 0 \pmod 2$ since A is in the kernel of the mapping, so bc is divisible by 4. Since A has determinant 1, $-a^2 - bc = 1$. It follows that $a^2 \equiv -1 \pmod 4$. This is impossible, since the square of every odd integer is congruent to 1 (mod 4).

The same argument rules out the possibility that G^+ is isomorphic to $SL(2,3)$, since such a G^+ would have a subgroup isomorphic to the quaternion group of order 8. Theorem 8 says, therefore, that G^+ must be isomorphic to one of the groups

$$C_1, C_2, C_3, C_4, \text{ or } C_6,$$

where C_i denotes the cyclic group of order i.

The structure of G itself now follows readily. Our earlier discussion shows that, among elements of finite order in $GL(2,\mathbb{Z})$, only elements of order two have determinant -1. If $G^+ \neq G$, then G^+ has index 2 in G. Let x be an element of G that is not in G^+. Then all the elements of the coset G^+x must have order 2, since they are matrices of determinant -1. In particular, if y is a generator of the cyclic group G^+, then yx must have order 2. Thus, $(yx)(yx) = 1$ and $xyx^{-1} = y^{-1}$; in other words, conjugating by x inverts G^+. This means that G must then be isomorphic to one of the dihedral groups

$$D_1, D_2, D_3, D_4, \text{ or } D_6.$$

Since all the groups C_i and D_i above are subgroups of one of the dihedral groups D_4 or D_6, and since (as noted at the outset) both D_4 and D_6 can be written using integer matrices, we can summarize our results as follows.

THEOREM 3. *A finite group G can be represented as a group of invertible 2×2 integer matrices if and only if G is isomorphic to a subgroup of D_4 or D_6.*

Conclusion A more economical presentation could be achieved by using the Sylow theorems in analyzing $SL(2,3)$, and by noting that the minimum polynomial of an element of finite order n in $GL(2,\mathbb{Z})$ must be divisible by the minimal polynomial over the rationals of a primitive nth root of unity. A famous theorem due to Gauss asserts that the degree of a primitive nth root of unity over the rationals is $\phi(n)$, where ϕ is Euler's totient function. In our situation, $\phi(n) = 1$ or 2; this forces $n = 1$, 2, 3, 4, or 6.

The results above are related to a geometric result called the *crystallographic restriction*, which arises in classifying symmetry groups of crystals (see e.g., [**1**, p. 151]). This restriction says that the only rotations admitted by lattices in dimensions 2 or 3 are those through angles $2\pi/n$, where $n = 1$, 2, 3, 4, or 6. Indeed, given a matrix A of the type under consideration, of order $n \geq 3$, we have seen that the eigenvalues of A are precisely $e^{i\theta}$ and $e^{-i\theta}$, with $\theta = 2\pi m/n$ and m and n relatively prime. But the rotation matrix $R = \begin{pmatrix} \cos\theta & -\sin\theta \\ \sin\theta & \cos\theta \end{pmatrix}$ has exactly the same two

distinct eigenvalues. Thus A and R are similar over the complex numbers, and hence also over the real numbers ([**2**, p. 158]); i.e., $CA = RC$ for some invertible real matrix C. The columns of C can be viewed as the basis of a two dimensional lattice L. Since A has integer entries, the relation $RC = CA$ shows that rotating lattice vectors through angle θ produces vectors that are *integer* linear combinations of a basis of L. So the lattice L admits a rotational symmetry and the crystallographic restriction can be invoked to reveal the possible values of n.

Acknowledgment I would like to thank the referee and the editor for many helpful comments.

REFERENCES

1. M. A. Armstrong, *Groups and Symmetry*, Springer-Verlag, New York, NY, 1988.
2. R. A. Horn and C. R. Johnson, *Matrix Analysis*, Cambridge University Press, Cambridge, UK, 1985.
3. M. Newman, *Integral Matrices*, Academic Press, New York, NY, 1972.
4. J. J. Rotman, *An Introduction to the Theory of Groups*, 3rd ed., Allyn and Bacon, Boston, MA, 1984.

Moving Card i to Position j with Perfect Shuffles

SARNATH RAMNATH
Dept. of Computer Science

DANIEL SCULLY
St. Cloud State University
St. Cloud, MN 56301-4489

To perform a perfect riffle shuffle, or faro shuffle, on a deck of $2n$ cards, you cut the deck into two stacks of n cards and interlace them perfectly. This can be done in two ways. If the shuffle leaves the top card on top, it is called an *out* shuffle. If the shuffle moves the top card into the second position, it is called an *in* shuffle.

Perfect shuffles have been of great interest to a wide variety of people for a long time. We have seen references to books on card cheating that described the perfect shuffle back in the eighteenth century. Magicians use perfect shuffles in card tricks (see Marlo [**7**] and [**8**]), and computer scientists use them in parallel processing (see Stone [**12**] and Chen, et al. [**3**]).

For the mathematician, perfect shuffles provide a deep and complex structure from a very simple and natural setting. Mathematics literature on the perfect shuffle ranges from the recreational and nontechnical in Gardner [**5**], Ball and Coxeter [**2**], Adler [**1**], Herstein and Kaplansky [**6**], and Rosenthal [**11**] to the very sophisticated work of Diaconis, Graham, and Kantor [**4**] where the group generated by the in and out shuffles is determined. Generalizations of the perfect shuffle provide more grist for the mathematical mill in Morris and Hartwig [**10**], and Medvedoff and Morrison [**9**].

Moving cards to desired positions through perfect shuffles is of interest to magicians and card cheaters because perfect shuffles appear to be random but are not. It has long been known, and easily proved [**4**], that the top card can be moved to position j (the top card is in position 0) through a sequence of in and out shuffles determined by the base-two representation of j. Reading the base two digits from left to right, simply perform a shuffle for each digit: an in shuffle for a 1 and an out shuffle for a 0. The