MATHEMATICS S–152, Summer 2005
METHODS OF DISCRETE MATHEMATICS
Notes on Vector Spaces over Finite Fields

Last modified: October 5, 2004

1 Two-component vectors over $\mathbb{F}_4$.

There are $4 \times 4 = 16$ of these. They break up into the zero vector plus 5 one-dimensional subspaces ("lines"), each with three nonzero elements. The numbering of the lines below is consistent with the Windows program SL2F.exe, available on the course web site.

Line 1: $\left[\begin{smallmatrix}1\\0\end{smallmatrix}\right]$, $\left[\begin{smallmatrix}x+1\\0\end{smallmatrix}\right]$, and $\left[\begin{smallmatrix}x\\0\end{smallmatrix}\right]$

Line 2: $\left[\begin{smallmatrix}0\\1\end{smallmatrix}\right]$, $\left[\begin{smallmatrix}0\\x+1\end{smallmatrix}\right]$, and $\left[\begin{smallmatrix}0\\x\end{smallmatrix}\right]$

Line 3: $\left[\begin{smallmatrix}1\\x\end{smallmatrix}\right]$, $\left[\begin{smallmatrix}x+1\\1\end{smallmatrix}\right]$, and $\left[\begin{smallmatrix}x\\x+1\end{smallmatrix}\right]$

Line 4: $\left[\begin{smallmatrix}1\\1\end{smallmatrix}\right]$, $\left[\begin{smallmatrix}x+1\\x+1\end{smallmatrix}\right]$, and $\left[\begin{smallmatrix}x\\x\end{smallmatrix}\right]$

Line 5: $\left[\begin{smallmatrix}1\\x+1\end{smallmatrix}\right]$, $\left[\begin{smallmatrix}x+1\\x\end{smallmatrix}\right]$, and $\left[\begin{smallmatrix}x\\1\end{smallmatrix}\right]$

Each subspace corresponds to one of the five edge colors used on the dodecahedron, and the three non-zero vectors in each subspace correspond to the three pairs of edges with a given color.

2 2×2 matrices with elements in $\mathbb{F}_4$

There are $4 \times 4 \times 4 \times 4 = 256$ of these. The ones with non-zero determinant form a group $GL(2, \mathbb{F}_4)$. The ones with determinant 1 form the subgroup $SL(2, \mathbb{F}_4)$. Let's count them.

Along each diagonal of the matrix we have two elements. When the two elements that have a given sum and product are different, we have two possibilities for that diagonal, but when they are the same we have only one. Some combinations of sum and product are impossible.

Example: The product x can arise as $(x+1)^2$ or as $1 \times x$.

- If the sum on a diagonal is 1, there are 0 ways to have product x.
- If the sum on a diagonal is 0, there is only 1 way to have product x. Both entries on the diagonal must be $x+1$.
- If the sum on a diagonal is $x+1$, there are 2 ways to have product x. The entries on the diagonal must be x and 1, and these can occur in either order.

	Sum 0	Sum 1	Sum x	Sum $x+1$	Total
Product 0	1	2	2	2	7
Product 1	1	2	0	0	3
Product x	1	0	0	2	3
Product $x+1$	1	0	2	0	3
Total	4	4	4	4	16

Counting the matrices with determinant 1.

For reasons that will become apparent, we classify them according to the trace, the sum of the elements on the main diagonal. "Main" and "Off" refer to the product of the elements on the main diagonal and the off diagonal respectively. For a matrix to have determinant 1, the product along the main diagonal must be 1 "greater than" (different from) the product on the off-diagonal.

Main	Off	Trace 0	Trace 1	Trace x	Trace $x+1$	Total
0	1	3	6	6	6	$7 \times 3 = 21$
1	0	7	14	0	0	$3 \times 7 = 21$
x	x+1	3	0	0	6	$3 \times 3 = 9$
$x+1$	x	3	0	6	0	$3 \times 3 = 9$
	Total	16	20	12	12	60

The column totals are suggestive. There are 60 elements in the group, the same as in the symmetry group of the dodecahedron/icosahedron. Perhaps the 20 matrices with trace 1 are the order 3 elements, and the 24 with trace x or $x+1$ are the order 5 elements. The identity matrix has trace 0, and the remaining 15 matrices with trace 0 could be the order 2 elements.

3 What are the eigenvalues of these matrices?

$\left[\begin{smallmatrix} a & b \\ c & d \end{smallmatrix}\right] - \lambda \left[\begin{smallmatrix} 1 & 0 \\ 0 & 1 \end{smallmatrix}\right]$ must have determinant 0,
so $\det \left[\begin{smallmatrix} a-\lambda & b \\ c & d-\lambda \end{smallmatrix}\right] = 0$
or

$$(a-\lambda)(d-\lambda) - bc = 0$$

or

$$\lambda^2 - (a+d)\lambda + ad - bc = 0.$$

But $ad - bc$ is the determinant, which is 1.

The coefficient of λ, the trace, determines the eigenvalues.

Trace 0: $\lambda^2 + 1 = 0$ has one solution $\lambda = 1$.

One such matrix (the identity) has two eigenvectors. The other 15 of these have a single line of eigenvectors. The other four lines get exchanged in pairs. So as a permutation of the lines, such a matrix behaves like a permutation with order 2, of the form (12)(34).

Trace 1: $\lambda^2 + \lambda + 1 = 0$ has two solutions, $\lambda = x$ and $\lambda = x + 1$.

Each of these 20 matrices has two lines of eigenvectors and permutes the other three lines cyclically. Such a matrix behaves like a permutation of order 3, of the form (123).

Trace x or $x+1$: $\lambda^2 + x\lambda + 1 = 0$ or $\lambda^2 + (x+1)\lambda + 1 = 0$ has no solutions over the field $\mathbb{F}_4$. (There is no sign error in the coefficient of λ, since $-x$ is the same as x in $\mathbb{F}_4$.

Each of these 24 matrices has no eigenvectors and permutes all five lines cyclically, like a permutation of order 5, of the form (12345).

4 The isomorphism between the symmetry group of the dodecahedron and $SL(2, \mathbb{F}_4)$.

See the attached hand-drawn diagram 3. A vector is associated with each edge, and a matrix is associated with each face, vertex, or edge. The geometric effect of the rotation associated with each matrix is found by letting the matrix act on the vector for each edge. When this vector is an eigenvector, the edge is moved to another edge of the same color, labeled with a vector that is proportional to the original vector.

5 The isomorphism in action.

An order 5 element $\left[\begin{smallmatrix} 0 & 1 \\ 1 & x \end{smallmatrix}\right]$
This does rotations about an axis through the central pentagon. Let it act on a representative vector from each of the lines L_1, L_2, L_3, L_4, L_5.

On L_1, $\left[\begin{smallmatrix} 0 & 1 \\ 1 & x \end{smallmatrix}\right]\left[\begin{smallmatrix} 1 \\ 0 \end{smallmatrix}\right] = \left[\begin{smallmatrix} 0 \\ 1 \end{smallmatrix}\right]$ which belongs to L_2.

On L_2, $\left[\begin{smallmatrix} 0 & 1 \\ 1 & x \end{smallmatrix}\right]\left[\begin{smallmatrix} 0 \\ 1 \end{smallmatrix}\right] = \left[\begin{smallmatrix} 1 \\ x \end{smallmatrix}\right]$ which belongs to L_3.

On L_3, $\left[\begin{smallmatrix} 0 & 1 \\ 1 & x \end{smallmatrix}\right]\left[\begin{smallmatrix} 1 \\ x \end{smallmatrix}\right] = \left[\begin{smallmatrix} x \\ x \end{smallmatrix}\right]$ which belongs to L_4.

On L_4, $\left[\begin{smallmatrix} 0 & 1 \\ 1 & x \end{smallmatrix}\right]\left[\begin{smallmatrix} x \\ x \end{smallmatrix}\right] = \left[\begin{smallmatrix} x \\ 1 \end{smallmatrix}\right]$ which belongs to L_5.

On L_5, $\left[\begin{smallmatrix} 0 & 1 \\ 1 & x \end{smallmatrix}\right]\left[\begin{smallmatrix} x \\ 1 \end{smallmatrix}\right] = \left[\begin{smallmatrix} 1 \\ 0 \end{smallmatrix}\right]$ which belongs to L_1.

So $L_1 \to L_2 \to L_3 \to L_4 \to L_5 \to L_1$ and the matrix corresponds to the permutation (1 2 3 4 5).

An order 3 element $\left[\begin{smallmatrix} x & 1 \\ 0 & x+1 \end{smallmatrix}\right]$
This does rotations about an axis through the rightmost vertex central pentagon. Let it act first on a representative vector of the line L_2.

On L_2, $\left[\begin{smallmatrix} x & 1 \\ 0 & x+1 \end{smallmatrix}\right]\left[\begin{smallmatrix} 1 \\ 0 \end{smallmatrix}\right] = \left[\begin{smallmatrix} 1 \\ x+1 \end{smallmatrix}\right]$ which belongs to L_5.

On L_5, $\left[\begin{smallmatrix} x & 1 \\ 0 & x+1 \end{smallmatrix}\right]\left[\begin{smallmatrix} 1 \\ x+1 \end{smallmatrix}\right] = \left[\begin{smallmatrix} 1 \\ x \end{smallmatrix}\right]$ which belongs to L_3.

On L_3, $\left[\begin{smallmatrix} x & 1 \\ 0 & x+1 \end{smallmatrix}\right]\left[\begin{smallmatrix} 1 \\ x \end{smallmatrix}\right] = \left[\begin{smallmatrix} 0 \\ 1 \end{smallmatrix}\right]$ which belongs to L_2.

So $L_2 \to L_5 \to L_3 \to L_2$ and the matrix corresponds to the permutation (2 5 3).

On L_4, $\left[\begin{smallmatrix} x & 1 \\ 0 & x+1 \end{smallmatrix}\right]\left[\begin{smallmatrix} x \\ x \end{smallmatrix}\right] = \left[\begin{smallmatrix} 1 \\ 1 \end{smallmatrix}\right]$ which also belongs to L_4. This vector is an eigenvector with eigenvalue $x + 1$.

On L_1, $\left[\begin{smallmatrix} x & 1 \\ 0 & x+1 \end{smallmatrix}\right]\left[\begin{smallmatrix} 1 \\ 0 \end{smallmatrix}\right] = \left[\begin{smallmatrix} x \\ 0 \end{smallmatrix}\right]$ which also belongs to L_1. This vector is an eigenvector with eigenvalue x.

An order 2 element $\left[\begin{smallmatrix} 1 & 0 \\ x+1 & 1 \end{smallmatrix}\right]$
This does a 180 degree rotation about an axis through the $\left[\begin{smallmatrix} 0 \\ 1 \end{smallmatrix}\right]$ edge of the central pentagon. Let it act first on a representative vector of the line L_2.

On L_2, $\left[\begin{smallmatrix} 1 & 0 \\ x+1 & 1 \end{smallmatrix}\right]\left[\begin{smallmatrix} 0 \\ 1 \end{smallmatrix}\right] = \left[\begin{smallmatrix} 0 \\ 1 \end{smallmatrix}\right]$ which belongs to L_2. The eigenvalue is 1.

On L_3, $\left[\begin{smallmatrix} 1 & 0 \\ x+1 & 1 \end{smallmatrix}\right]\left[\begin{smallmatrix} 1 \\ x \end{smallmatrix}\right] = \left[\begin{smallmatrix} 1 \\ 1 \end{smallmatrix}\right]$ which belongs to L_4.

On L_4, $\left[\begin{smallmatrix} 1 & 0 \\ x+1 & 1 \end{smallmatrix}\right]\left[\begin{smallmatrix} 1 \\ 1 \end{smallmatrix}\right] = \left[\begin{smallmatrix} 1 \\ x \end{smallmatrix}\right]$ which belongs to L_3. So lines L_3 and L_4 are transposed.

On L_5, $\left[\begin{smallmatrix} 1 & 0 \\ x+1 & 1 \end{smallmatrix}\right]\left[\begin{smallmatrix} 1 \\ x+1 \end{smallmatrix}\right] = \left[\begin{smallmatrix} 1 \\ 0 \end{smallmatrix}\right]$ which belongs to L_1.

On L_1, $\left[\begin{smallmatrix} 1 & 0 \\ x+1 & 1 \end{smallmatrix}\right]\left[\begin{smallmatrix} 1 \\ 0 \end{smallmatrix}\right] = \left[\begin{smallmatrix} 1 \\ x+1 \end{smallmatrix}\right]$ which belongs to L_5. So lines L_5 and L_1 are transposed. This matrix corresponds to the permutation (1 5)(3 4).

6 2-component vectors over $\mathbb{Z}_5$

It is convenient to name the equivalence classes [0], [1], [2], [−2] (the same as [3]) and [−1] (the same as [4]).

There are $5 \times 5 = 25$ vectors. One is the zero vector, and the other 24 divide into 6 subspaces (lines), each with 4 nonzero vectors.

Line 1: $\left[\begin{smallmatrix}1\\0\end{smallmatrix}\right]$, $\left[\begin{smallmatrix}2\\0\end{smallmatrix}\right]$, $\left[\begin{smallmatrix}-2\\0\end{smallmatrix}\right]$and $\left[\begin{smallmatrix}-1\\0\end{smallmatrix}\right]$
Every point on this line satisfies the equation $y = 0$.

Line 2: $\left[\begin{smallmatrix}0\\1\end{smallmatrix}\right]$, $\left[\begin{smallmatrix}0\\2\end{smallmatrix}\right]$, $\left[\begin{smallmatrix}0\\-2\end{smallmatrix}\right]$and $\left[\begin{smallmatrix}0\\-1\end{smallmatrix}\right]$
Every point on this line satisfies the equation $x = 0$.

Line 3: $\left[\begin{smallmatrix}1\\1\end{smallmatrix}\right]$, $\left[\begin{smallmatrix}2\\2\end{smallmatrix}\right]$, $\left[\begin{smallmatrix}-2\\-2\end{smallmatrix}\right]$and $\left[\begin{smallmatrix}-1\\-1\end{smallmatrix}\right]$
Every point on this line satisfies the equation $y = x$.

Line 4: $\left[\begin{smallmatrix}1\\2\end{smallmatrix}\right]$, $\left[\begin{smallmatrix}2\\-1\end{smallmatrix}\right]$, $\left[\begin{smallmatrix}-2\\1\end{smallmatrix}\right]$and $\left[\begin{smallmatrix}-1\\-2\end{smallmatrix}\right]$
Every point on this line satisfies the equation $y = 2x$.

Line 5: $\left[\begin{smallmatrix}1\\-2\end{smallmatrix}\right]$, $\left[\begin{smallmatrix}2\\1\end{smallmatrix}\right]$, $\left[\begin{smallmatrix}-2\\-1\end{smallmatrix}\right]$and $\left[\begin{smallmatrix}-1\\2\end{smallmatrix}\right]$
Every point on this line satisfies the equation $y = -2x$.

Line 6: $\left[\begin{smallmatrix}1\\-1\end{smallmatrix}\right]$, $\left[\begin{smallmatrix}2\\-2\end{smallmatrix}\right]$, $\left[\begin{smallmatrix}-2\\2\end{smallmatrix}\right]$and $\left[\begin{smallmatrix}-1\\1\end{smallmatrix}\right]$
Every point on this line satisfies the equation $y = -x$.

Each line can be associated with an axis that passes through two opposite pentagonal faces of the dodecahedron.

The numbering of the lines is consistent with the Windows program GL2Z5.exe on the course Web site.

7 2×2 matrices with elements in $\mathbb{Z}_5$

There are $5 \times 5 \times 5 \times 5 = 625$ of these.

The ones with non-zero determinant form a group $GL(2, \mathbb{Z}_5)$.

The ones with determinant 1 form the subgroup $SL(2, \mathbb{Z}_5)$.

Let's count them.

Along each diagonal of the matrix we have two elements. When the two elements that have a given sum and product are different, we have two possibilities for that diagonal, but when they are the same we have only one. Some combinations of sum and product are impossible.

Example: The product 1 can arise as 1×1, as -1×-1, or as 2×-2.

- If the sum on a diagonal is 1 or -1, there are 0 ways to have product 1.

- If the sum on a diagonal is 2 or -2, there is only 1 way to have product 1. Both entries on the diagonal must be equal (1 or -1).
- If the sum on a diagonal is 0, there are 2 ways to have product 1. The entries on the diagonal must be 2 and -2, and these can occur in either order.

	Sum -2	Sum -1	Sum 0	Sum 1	Sum 2	Total
Product -2	0	2	0	2	0	4
Product -1	0	1	2	1	0	4
Product 0	2	2	1	2	2	9
Product 1	1	0	2	0	1	4
Product 2	2	0	0	0	2	4
Total	5	5	5	5	5	25

For determinant 1 the product along the main diagonal ("Main") must be 1 greater than the product along the off diagonal ("Off).

We classify the matrices according to the trace, the sum of the elements on the main diagonal.

Main	Off	Trace -2	Trace -1	Trace 0	Trace 1	Trace 2	Total
-2	2	0	8	0	8	0	$4 \times 4 = 16$
-1	-2	0	4	8	4	0	$4 \times 4 = 16$
0	-1	8	8	4	8	8	$4 \times 9 = 36$
1	0	9	0	18	0	9	$9 \times 4 = 36$
2	1	8	0	0	0	8	$4 \times 4 = 16$
	Total	25	20	30	20	25	120

The column totals are mildly encouraging. There are 120 elements in the group, twice as many as in the symmetry group of the dodecahedron/icosahedron. Perhaps the 40 matrices with trace 1 or -1 are the order 3 elements, and the 30 with trace 1 are the order 2 elements. The identity matrix has trace 2, its negative has trace -2, and the remaining 48 matrices with trace -2 or 2 could be the order 2 elements.

8 What are the eigenvalues?

Since the determinant is 1, the coefficient of λ, the trace, determines the eigenvalues. An eigenvalue λ must satisfy the equation λ^2 - (trace)λ + 1 =

0.

Trace 0: $\lambda^2 + 1 = 0$ has two solutions, $\lambda = 2$ and $\lambda = -2$.

There are two lines of eigenvectors. The other four lines are exchanged in pairs. These are the order 2 elements, corresponding to permutations like (12)(34); there are $30 = 2 \times 15$ of them.

Trace 1 or -1: Neither $\lambda^2 + \lambda + 1 = 0$ nor $\lambda^2 - \lambda + 1 = 0$ has any solutions, so there are no eigenvectors.

Each of these 40 matrices permutes the lines cyclically in sets of 3. Such a matrix behaves like a permutation of order 3, of the form (123)(456).

Trace 2 or -2: $\lambda^2 - 2\lambda + 1 = 0$ or $\lambda^2 + 2\lambda + 1 = 0$ has a double root, 1 or -1.

Special cases are the identity $\left[\begin{smallmatrix} 1 & 0 \\ 0 & 1 \end{smallmatrix}\right]$ and its negative $\left[\begin{smallmatrix} -1 & 0 \\ 0 & -1 \end{smallmatrix}\right]$. Every vector is an eigenvector for either of these matrices.

The remaining 48 matrices each have one eigenvector and permute the remaining five lines cyclically, like a permutation of order 5, of the form (12345).

We now have precisely twice too many matrices of each order:
1+1 identity
15+15 of order 2
20+20 of order 3
24+24 of order 5

Fortunately, the identity matrix and its negative form a self-conjugate subgroup of order 2, and the quotient group will have $120/2 = 60$ elements.

The elements of the quotient group are two-element cosets, pairs of matrices that differ by an overall minus sign, like $\left[\begin{smallmatrix} 1 & 0 \\ 0 & 1 \end{smallmatrix}\right]$ and $\left[\begin{smallmatrix} -1 & 0 \\ 0 & -1 \end{smallmatrix}\right]$
or

$\left[\begin{smallmatrix} 2 & 1 \\ -1 & 0 \end{smallmatrix}\right]$ and $\left[\begin{smallmatrix} -2 & -1 \\ 1 & 0 \end{smallmatrix}\right]$.

It is useful to have an arbitrary rule to select one of the two elements from each coset as the standard representative of that coset. If the trace is nonzero, choose the matrix with positive trace. Otherwise, choose the matrix for which the sum of the off-diagonal elements is positive.

When you multiply two cosets, multiply the representative matrices. If the product is not the standard representative of its coset, just change all the signs to get the other element in the coset.

Using pairs of matrices like this, so that matrices that differ by an overall minus sign are regarded as equivalent, changes the group into the "projective special linear group" $PSL(2, \mathbb{Z}_5)$. In general "projective" means "take the

quotient by the center, the self-conjugate subgroup that consists of multiples of the identity."

9 The isomorphism between the symmetry group of the dodecahedron and $PSL(2, \mathbb{Z}_5)$.

See the attached hand-drawn diagram 4. A vector is associated with each pair of faces, and a matrix is associated with each face, vertex, or edge. The geometric effect of the rotation associated with each matrix is found by letting the matrix act on the vector for each face. When this vector is an eigenvector, the face is moved to another face of the same color.

10 The second isomorphism in action.

An order 5 element $\left[\begin{smallmatrix} 0 & 1 \\ -1 & 2 \end{smallmatrix}\right]$
This does rotations about an axis through the pentagon L_3. Let it act on a representative vector from each of the lines L_1, L_2, L_4, L_6, L_5.

On L_1, $\left[\begin{smallmatrix} 0 & 1 \\ -1 & 2 \end{smallmatrix}\right]\left[\begin{smallmatrix} 1 \\ 0 \end{smallmatrix}\right] = \left[\begin{smallmatrix} 0 \\ -1 \end{smallmatrix}\right]$ which belongs to L_2.
On L_2, $\left[\begin{smallmatrix} 0 & 1 \\ -1 & 2 \end{smallmatrix}\right]\left[\begin{smallmatrix} 0 \\ 1 \end{smallmatrix}\right] = \left[\begin{smallmatrix} 1 \\ 2 \end{smallmatrix}\right]$ which belongs to L_4.
On L_4, $\left[\begin{smallmatrix} 0 & 1 \\ -1 & 2 \end{smallmatrix}\right]\left[\begin{smallmatrix} 1 \\ 2 \end{smallmatrix}\right] = \left[\begin{smallmatrix} 2 \\ -2 \end{smallmatrix}\right]$ which belongs to L_6.
On L_6, $\left[\begin{smallmatrix} 0 & 1 \\ -1 & 2 \end{smallmatrix}\right]\left[\begin{smallmatrix} 2 \\ -2 \end{smallmatrix}\right] = \left[\begin{smallmatrix} -2 \\ -1 \end{smallmatrix}\right]$ which belongs to L_5.
On L_5, $\left[\begin{smallmatrix} 0 & 1 \\ -1 & 2 \end{smallmatrix}\right]\left[\begin{smallmatrix} 2 \\ 1 \end{smallmatrix}\right] = \left[\begin{smallmatrix} 1 \\ 0 \end{smallmatrix}\right]$ which belongs to L_1.

So $L_1 \to L_2 \to L_4 \to L_6 \to L_5 \to L_1$ and the matrix corresponds to the permutation (1 2 4 6 5).

On L_3, $\left[\begin{smallmatrix} 0 & 1 \\ -1 & 2 \end{smallmatrix}\right]\left[\begin{smallmatrix} 1 \\ 1 \end{smallmatrix}\right] = \left[\begin{smallmatrix} 1 \\ 1 \end{smallmatrix}\right]$ which belongs to L_3. So L_3 is an eigenvector with eigenvalue 1.

An order 3 element $\left[\begin{smallmatrix} 0 & 1 \\ -1 & 1 \end{smallmatrix}\right]$
This does rotations about the vertex where faces L_1, L_2, and L_3 meet. Let it act first on a representative vector of the line L_1.

On L_1, $\left[\begin{smallmatrix} 0 & 1 \\ -1 & 1 \end{smallmatrix}\right]\left[\begin{smallmatrix} 1 \\ 0 \end{smallmatrix}\right] = \left[\begin{smallmatrix} 0 \\ 1 \end{smallmatrix}\right]$ which belongs to L_2.
On L_2, $\left[\begin{smallmatrix} 0 & 1 \\ -1 & 1 \end{smallmatrix}\right]\left[\begin{smallmatrix} 0 \\ 1 \end{smallmatrix}\right] = \left[\begin{smallmatrix} 1 \\ 1 \end{smallmatrix}\right]$ which belongs to L_3.
On L_3, $\left[\begin{smallmatrix} 0 & 1 \\ -1 & 1 \end{smallmatrix}\right]\left[\begin{smallmatrix} 1 \\ 1 \end{smallmatrix}\right] = \left[\begin{smallmatrix} 1 \\ 0 \end{smallmatrix}\right]$ which belongs to L_1.
So $L_1 \to L_2 \to L_3 \to L_1$. We need to find another cycle.
On L_4, $\left[\begin{smallmatrix} 0 & 1 \\ -1 & 1 \end{smallmatrix}\right]\left[\begin{smallmatrix} 2 \\ 1 \end{smallmatrix}\right] = \left[\begin{smallmatrix} 1 \\ -1 \end{smallmatrix}\right]$ which belongs to L_5.
On L_5, $\left[\begin{smallmatrix} 0 & 1 \\ -1 & 1 \end{smallmatrix}\right]\left[\begin{smallmatrix} 1 \\ -1 \end{smallmatrix}\right] = \left[\begin{smallmatrix} -1 \\ -2 \end{smallmatrix}\right]$ which belongs to L_6.
On L_6, $\left[\begin{smallmatrix} 0 & 1 \\ -1 & 1 \end{smallmatrix}\right]\left[\begin{smallmatrix} 1 \\ 2 \end{smallmatrix}\right] = \left[\begin{smallmatrix} 2 \\ 1 \end{smallmatrix}\right]$ which belongs to L_4.

So $L_4 \to L_5 \to L_6 \to L_4$. The matrix corresponds to the permutation (123)(456).

An order 2 element $\left[\begin{smallmatrix} 0 & -1 \\ 1 & 0 \end{smallmatrix}\right]$
This does a 180 degree rotation about an axis through the midpoint of the edge shared by L_1 and L_2. Let it act first on a representative vector of the line L_1.

On L_1, $\left[\begin{smallmatrix} 0 & -1 \\ 1 & 0 \end{smallmatrix}\right]\left[\begin{smallmatrix} 1 \\ 0 \end{smallmatrix}\right] = \left[\begin{smallmatrix} 0 \\ -1 \end{smallmatrix}\right]$ which belongs to L_2.
On L_2, $\left[\begin{smallmatrix} 0 & -1 \\ 1 & 0 \end{smallmatrix}\right]\left[\begin{smallmatrix} 0 \\ 1 \end{smallmatrix}\right] = \left[\begin{smallmatrix} -1 \\ 0 \end{smallmatrix}\right]$ which belongs to L_1.
We have found the cycle (1 2).

On L_3, $\left[\begin{smallmatrix} 0 & -1 \\ 1 & 0 \end{smallmatrix}\right]\left[\begin{smallmatrix} 1 \\ 1 \end{smallmatrix}\right] = \left[\begin{smallmatrix} -1 \\ 1 \end{smallmatrix}\right]$ which belongs to L_6.
On L_6, $\left[\begin{smallmatrix} 0 & -1 \\ 1 & 0 \end{smallmatrix}\right]\left[\begin{smallmatrix} -1 \\ 1 \end{smallmatrix}\right] = \left[\begin{smallmatrix} -1 \\ -1 \end{smallmatrix}\right]$ which belongs to L_3.
We have found the cycle (3 6).

On L_4, $\left[\begin{smallmatrix} 0 & -1 \\ 1 & 0 \end{smallmatrix}\right]\left[\begin{smallmatrix} 2 \\ 1 \end{smallmatrix}\right] = \left[\begin{smallmatrix} -1 \\ 2 \end{smallmatrix}\right]$ which still belongs to L_4. We have found an eigenvector with eigenvalue 2.

On L_5, $\left[\begin{smallmatrix} 0 & -1 \\ 1 & 0 \end{smallmatrix}\right]\left[\begin{smallmatrix} -2 \\ 1 \end{smallmatrix}\right] = \left[\begin{smallmatrix} -1 \\ -2 \end{smallmatrix}\right]$ which still belongs to L_5. We have found the other eigenvector, with eigenvalue -2.

So this matrix corresponds to the permutation (12)(36).

11 More quotient groups

Since only the line (subspace), and not the actual vector, is what matters when we let a vector act on a matrix, multiplying every element of a matrix by the same constant does not change the effect of the matrix in permuting lines. The multiples of the identity matrix always form a normal (self-conjugate) subgroup, the center Z (Biggs, p. 272). Any element of Z commutes with every element of the group, so clearly the right cosets and the left cosets of Z are the same.

The quotient group $\frac{GL(2,\mathbb{F}_4)}{Z(\mathbb{F}_4)}$ is called $PGL(2,\mathbb{F}_4)$, the "projective general linear group." Its elements are cosets of $Z(\mathbb{F}_4)$, for example

$$\left\{\left[\begin{smallmatrix} 1 & 0 \\ 0 & 1 \end{smallmatrix}\right], \left[\begin{smallmatrix} x & 0 \\ 0 & x \end{smallmatrix}\right], \left[\begin{smallmatrix} x+1 & 0 \\ 0 & x+1 \end{smallmatrix}\right]\right\}$$

or

$$\left\{\left[\begin{smallmatrix} 1 & x \\ x & x \end{smallmatrix}\right], \left[\begin{smallmatrix} x & x+1 \\ x+1 & x+1 \end{smallmatrix}\right], \left[\begin{smallmatrix} x+1 & 1 \\ 1 & 1 \end{smallmatrix}\right]\right\}$$

Each coset includes precisely one matrix of determinant 1, which can be chosen as the representative, one of determinant x, and one of determinant $x+1$.

$GL(2,\mathbb{F}_4)$ has 180 elements. Its center has 3 elements, and so the quotient group $PGL(2,\mathbb{F}_4)$ has 60 elements. The quotient group is isomorphic to $SL(2,\mathbb{F}_4)$, and we have not found anything new.

For $GL(2,\mathbb{Z}_5)$ the center has 4 elements:

$$\left\{\left[\begin{smallmatrix}1&0\\0&1\end{smallmatrix}\right],\left[\begin{smallmatrix}2&0\\0&2\end{smallmatrix}\right],\left[\begin{smallmatrix}-2&0\\0&-2\end{smallmatrix}\right],\left[\begin{smallmatrix}-1&0\\0&-1\end{smallmatrix}\right]\right\}$$

Notice that in this case not every possible value of the determinant arises: two of the matrices have determinant +1 and two have determinant -1.

$GL(2,\mathbb{Z}_5)$ has 480 elements. Its center has 4 elements, and the quotient group $PGL(2,\mathbb{Z}_5)$ has 120 elements. The elements of $PGL(2,\mathbb{Z}_5)$ consist of 60 cosets for which two of the matrices have determinant +1 and two have determinant -1 and 60 other cosets for which two of the matrices have determinant +2 and two have determinant -2. A simple example of the second case is the coset

$$\left\{\left[\begin{smallmatrix}2&0\\0&1\end{smallmatrix}\right],\left[\begin{smallmatrix}-1&0\\0&2\end{smallmatrix}\right],\left[\begin{smallmatrix}1&0\\0&-2\end{smallmatrix}\right],\left[\begin{smallmatrix}-2&0\\0&-1\end{smallmatrix}\right]\right\}$$

So there are 60 cosets that do not include any matrix of $SL(2,\mathbb{Z}_5)$, and to find them we have to look at matrices with determinant 2 or -2.

12 Classifying the matrices with determinant 2

As before,

	Sum -2	Sum -1	Sum 0	Sum 1	Sum 2	Total
Product -2	0	2	0	2	0	4
Product -1	0	1	2	1	0	4
Product 0	2	2	1	2	2	9
Product 1	1	0	2	0	1	4
Product 2	2	0	0	0	2	4
Total	5	5	5	5	5	25

For determinant 2 the product along the main diagonal ("Main") must be 2 greater than the product along the off diagonal ("Off).

We classify the matrices according to the trace, the sum of the elements on the main diagonal.

Main	Off	Trace -2	Trace -1	Trace 0	Trace 1	Trace 2	Total
2	0	18	0	0	0	18	$9 \times 4 = 36$
-2	1	0	8	0	8	0	$4 \times 4 = 16$
-1	2	0	4	8	4	0	$4 \times 4 = 16$
0	-2	8	8	4	8	8	$4 \times 9 = 36$
1	-1	4	0	8	0	4	$4 \times 4 = 16$
	Total	30	20	20	20	30	120

For comparison, count the odd permutations in S_5.

Like (12): there are $\frac{5\times4}{2} = 10$ of these (order 2).

Like (1234): there are $\frac{5\times4\times3\times2}{4} = 30$ of these (order 4).

Like (123)(45): there are $\frac{5\times4\times3}{3} = 20$ of these (order 3).

To determine which trace leads to which order, we use the Cayley-Hamilton theorem, which states that any matrix A satisfies its own characteristic equation.

If n is the smallest integer for which A^n is a multiple of the identity matrix I, then A^n carries every line into itself and the coset containing A, an element of $PGL(2, \mathbb{Z}_5)$, has order n.

When the determinant is 2, the characteristic equation is

λ^2 - (trace)λ + 2 = 0.

Case 1: Trace 0:

$\lambda^2 + 2 = 0$ has no roots in $\mathbb{Z}_5$.

By the Cayley-Hamilton theorem, A satisfies the same equation as λ and so

$$A^2 + 2I = 0$$

.

Thus $A^2 = -2I$. Since this is a multiple of the identity, the coset containing A has order 2. The 20 matrices with trace 0 and determinant 2 fall into 10 cosets, each of which also contains two elements with determinant -2. These 10 cosets correspond to odd permutations like (1 2), which never arise

when we consider the symmetries of the icosahedron.

Case 1: Trace 2:

λ^2 - 2λ + 2 = 0. This can also be written as

λ^2 +3 λ + 2 = $(\lambda + 1)(\lambda + 2) = 0$, so it has two roots, two distinct eigenvalues, two eigenvectors.

By the Cayley-Hamilton theorem, A satisfies the same equation as λ and so

$$A^2 - 2A + 2I = 0$$

.

Thus $A^2 = 2(A - I)$ and

$$A^4 = 4(A - I)^2 = 4(A^2 - 2A + I) = 4(2A - 2I - 2A + I) = -4I = I$$

.

So A has order 4.

Trace -2 works out the same way.

The 60 matrices with trace +2 or -2 fall into 30 cosets that correspond to the 30 order-4 permutations in S_5 like (1 2 3 4).

Case 3: Trace 1:

λ^2 - λ + 2 = 0 has no roots, as can be verified by trying -2, -1, 0, 1, and 2. So again there are no eigenvectors.

By the Cayley-Hamilton theorem, A satisfies the same equation as λ and so

$$A^2 - A + 2I = 0$$

.

Thus $A^2 = A - 2I$.

Then $A^3 = A(A - 2I) = A^2 - 2A = A - 2I - 2A = -A - 2I$.

Finally $A^6 = (A + 2I)^2 = A^2 + 4A + 4I = A - 2I + 4A + 4I = 2I$, so A has order 6.

Trace -1 works out the same way.

The 40 matrices with trace +1 or -1 fall into 20 cosets that correspond to the 20 order-6 permutations in S_5 like (1 2 3)(4 5).

An example with order 6:

The matrix $\left[\begin{smallmatrix} 1 & 2 \\ -1 & 0 \end{smallmatrix}\right]$ has determinant 2 and trace 1, so it should have no eigenvectors and have order 6.

On L_1, $\left[\begin{smallmatrix} 1 & 2 \\ -1 & 0 \end{smallmatrix}\right]\left[\begin{smallmatrix} 1 \\ 0 \end{smallmatrix}\right] = \left[\begin{smallmatrix} 1 \\ -1 \end{smallmatrix}\right]$ which belongs to L_6.
On L_6, $\left[\begin{smallmatrix} 1 & 2 \\ -1 & 0 \end{smallmatrix}\right]\left[\begin{smallmatrix} 1 \\ -1 \end{smallmatrix}\right] = \left[\begin{smallmatrix} -1 \\ -1 \end{smallmatrix}\right]$ which belongs to L_3.
On L_3, $\left[\begin{smallmatrix} 1 & 2 \\ -1 & 0 \end{smallmatrix}\right]\left[\begin{smallmatrix} 1 \\ 1 \end{smallmatrix}\right] = \left[\begin{smallmatrix} -2 \\ -1 \end{smallmatrix}\right]$ which belongs to L_5.
On L_5, $\left[\begin{smallmatrix} 1 & 2 \\ -1 & 0 \end{smallmatrix}\right]\left[\begin{smallmatrix} 1 \\ -2 \end{smallmatrix}\right] = \left[\begin{smallmatrix} 2 \\ -1 \end{smallmatrix}\right]$ which belongs to L_4.
On L_4, $\left[\begin{smallmatrix} 1 & 2 \\ -1 & 0 \end{smallmatrix}\right]\left[\begin{smallmatrix} 1 \\ 2 \end{smallmatrix}\right] = \left[\begin{smallmatrix} 0 \\ -1 \end{smallmatrix}\right]$ which belongs to L_2.
On L_2, $\left[\begin{smallmatrix} 1 & 2 \\ -1 & 0 \end{smallmatrix}\right]\left[\begin{smallmatrix} 0 \\ 1 \end{smallmatrix}\right] = \left[\begin{smallmatrix} 2 \\ 0 \end{smallmatrix}\right]$ which belongs to L_1.

So $L_1 \to L_6 \to L_3 \to L_5 \to L_4 \to L_2 \to L_1$ and this matrix corresponds to the permutation (1 6 3 5 4 2) (in S_6, not in S_5).

Examples with other traces:

Trace 0:

The matrix $\left[\begin{smallmatrix} 1 & 2 \\ 1 & -1 \end{smallmatrix}\right]$ has determinant 2 and trace 0, so it should have no eigenvectors and have order 2.

On L_1, $\left[\begin{smallmatrix} 1 & 2 \\ 1 & -1 \end{smallmatrix}\right]\left[\begin{smallmatrix} 1 \\ 0 \end{smallmatrix}\right] = \left[\begin{smallmatrix} 1 \\ 1 \end{smallmatrix}\right]$ which belongs to L_3.
On L_3, $\left[\begin{smallmatrix} 1 & 2 \\ 1 & -1 \end{smallmatrix}\right]\left[\begin{smallmatrix} 1 \\ 1 \end{smallmatrix}\right] = \left[\begin{smallmatrix} -2 \\ 0 \end{smallmatrix}\right]$ which belongs to L_1.
On L_2, $\left[\begin{smallmatrix} 1 & 2 \\ 1 & -1 \end{smallmatrix}\right]\left[\begin{smallmatrix} 0 \\ 1 \end{smallmatrix}\right] = \left[\begin{smallmatrix} 2 \\ -1 \end{smallmatrix}\right]$ which belongs to L_4.
On L_4, $\left[\begin{smallmatrix} 1 & 2 \\ 1 & -1 \end{smallmatrix}\right]\left[\begin{smallmatrix} 1 \\ 2 \end{smallmatrix}\right] = \left[\begin{smallmatrix} 0 \\ -1 \end{smallmatrix}\right]$ which belongs to L_2.
On L_5, $\left[\begin{smallmatrix} 1 & 2 \\ 1 & -1 \end{smallmatrix}\right]\left[\begin{smallmatrix} 1 \\ -2 \end{smallmatrix}\right] = \left[\begin{smallmatrix} 2 \\ -2 \end{smallmatrix}\right]$ which belongs to L_6.
On L_6, $\left[\begin{smallmatrix} 1 & 2 \\ 1 & -1 \end{smallmatrix}\right]\left[\begin{smallmatrix} 1 \\ -1 \end{smallmatrix}\right] = \left[\begin{smallmatrix} -1 \\ 2 \end{smallmatrix}\right]$ which belongs to L_5.

So as a permutation of S_6 this matrix corresponds to (1 3)(2 4)(5 6) and has order 2.

Trace 2:

The matrix $\left[\begin{smallmatrix} 1 & 2 \\ 2 & 1 \end{smallmatrix}\right]$ has determinant 2 and trace 2, so it should have two eigenvectors and have order 4.

On L_1, $\left[\begin{smallmatrix} 1 & 2 \\ 2 & 1 \end{smallmatrix}\right]\left[\begin{smallmatrix} 1 \\ 0 \end{smallmatrix}\right] = \left[\begin{smallmatrix} 1 \\ 2 \end{smallmatrix}\right]$ which belongs to L_4.
On L_4, $\left[\begin{smallmatrix} 1 & 2 \\ 2 & 1 \end{smallmatrix}\right]\left[\begin{smallmatrix} 1 \\ 2 \end{smallmatrix}\right] = \left[\begin{smallmatrix} 0 \\ -1 \end{smallmatrix}\right]$ which belongs to L_2.
On L_2, $\left[\begin{smallmatrix} 1 & 2 \\ 2 & 1 \end{smallmatrix}\right]\left[\begin{smallmatrix} 0 \\ 1 \end{smallmatrix}\right] = \left[\begin{smallmatrix} 2 \\ 1 \end{smallmatrix}\right]$ which belongs to L_5.
On L_5, $\left[\begin{smallmatrix} 1 & 2 \\ 2 & 1 \end{smallmatrix}\right]\left[\begin{smallmatrix} 1 \\ -2 \end{smallmatrix}\right] = \left[\begin{smallmatrix} 2 \\ 0 \end{smallmatrix}\right]$ which belongs to L_1.
On L_3, $\left[\begin{smallmatrix} 1 & 2 \\ 2 & 1 \end{smallmatrix}\right]\left[\begin{smallmatrix} 1 \\ 1 \end{smallmatrix}\right] = \left[\begin{smallmatrix} -2 \\ -2 \end{smallmatrix}\right]$ which again belongs to L_3. This is an eigenvector with eigenvalue -2.
On L_6, $\left[\begin{smallmatrix} 1 & 2 \\ 2 & 1 \end{smallmatrix}\right]\left[\begin{smallmatrix} 1 \\ -1 \end{smallmatrix}\right] = \left[\begin{smallmatrix} -1 \\ 1 \end{smallmatrix}\right]$ which again belongs to L_6. This is an eigenvector with eigenvalue -1.

So as an element of S_6 this matrix corresponds to (1 4 2 5) and has order 4.

Conclusion:

$PGL(2, \mathbb{Z}_5)$ has 120 elements and is isomorphic to S_5.
$PSL(2, \mathbb{Z}_5)$ has 60 elements and is isomorphic to A_5.
.