Chapter 8

Groups of Matrices

Let F be a field, such as one of the examples $\mathbb{Q}, \mathbb{R}, \mathbb{C}, \mathbb{Z}_p$ described earlier. Then we can form $n \times n$ matrices

$$A = \begin{pmatrix} a_{11} & a_{12} & \dots \\ a_{21} & a_{22} & \dots \\ \dots \end{pmatrix}$$

with entries in F. If B is another $n \times n$ matrix, we can form their product $C = AB$ which is another $n \times n$ matrix with entries

$$c_{ij} = a_{i1}b_{1j} + a_{i2}b_{2j} + \dots a_{in}b_{nj}$$

The identity matrix

$$I = \begin{pmatrix} 1 & 0 & \dots \\ 0 & 1 & \dots \\ \dots \end{pmatrix}$$

has entries

$$\delta_{ij} = \begin{cases} 1 & \text{if } i = j \\ 0 & \text{otherwise} \end{cases}$$

Lemma 8.1. *Matrix multiplication is associative and I is the identity for it, i.e. $AI = IA = A$.*

An $n \times n$ matrix A is *invertible* if there exists an $n \times n$ matrix A^{-1} such that $AA^{-1} = A^{-1}A = I$. Then

Theorem 8.2. *The set of invertible $n \times n$ matrices with entries in F forms a group called the* general linear group *$GL_n(F)$.*

For 2×2 matrices there is a simple test for invertibility. We recall that the determinant

$$det \begin{pmatrix} a & b \\ c & d \end{pmatrix} = ad - bc$$

and

$$e\begin{pmatrix} a & b \\ c & d \end{pmatrix} = \begin{pmatrix} ea & eb \\ ec & ed \end{pmatrix}$$

Theorem 8.3. *Let $A = \begin{pmatrix} a & b \\ c & d \end{pmatrix}$ be matrix over a field F, then A is invertible if and only $det(A) \neq 0$. In this case,*

$$A^{-1} = (det(A))^{-1}\begin{pmatrix} d & -b \\ -c & a \end{pmatrix}$$

Proof. Let $\Delta = det(A)$, and let $B = \begin{pmatrix} d & -b \\ -c & a \end{pmatrix}$. Then an easy calculation gives

$$AB = BA = \Delta I.$$

If $\Delta \neq 0$, then $\Delta^{-1}B$ will give the inverse of A by the above equation.

Suppose that $\Delta = 0$ and A^{-1} exists. Then multiply both sides of the above equation by A^{-1} to get $B = \Delta A^{-1} = 0$. This implies that $A = 0$, and therefore that $0 = AA^{-1} = I$. This is impossible. □

For larger matrices, there are various ways to compute the inverse which you learned in a linear algebra class. We won't review all this. Instead, we look at special cases, where the inverse is easy to understand. An $n\times n$ matrix $A = (a_{ij})$ is *upper triangular* if $a_{ij} = 0$ when $j > i$ i.e. if all the nonzero entries are on or above the diagonal. Let $UT_n(F)$ be the set of upper triangular matrices such that all entries on the diagonal are nonzero.

Theorem 8.4. *Every matrix in $UT_n(F)$ is invertible. In fact, the inverse of any matrix lies in $UT_n(F)$. If $A, B \in UT_n(F)$ then $AB \in UT_n(F)$.*

Proof. We will only sketch the proof of the first statement. Let $A \in UT_n(F)$. Let us try to discover the formula for the inverse $B = A^{-1}$ assuming that it exists. Writing out $BA = I$ yields

$$b_{11}a_{11} = 1 \Rightarrow b_{11} = a_{11}^{-1}$$

$$b_{21}a_{11} = 0 \Rightarrow b_{21} = 0$$

$$\ldots$$

$$b_{11}a_{12} + b_{12}a_{22} = 0 \Rightarrow b_{12} = -b_{11}a_{12}a_{22}^{-1}$$

$$b_{22}a_{22} = 1 \Rightarrow b_{22} = a_{22}^{-1}$$

$$b_{32}a_{22} = 0 \Rightarrow b_{32} = 0$$

$$\ldots$$

$$b_{11}a_{13} + b_{12}a_{23} + b_{13}a_{33} = 0 \Rightarrow b_{13} = -(b_{11}a_{13} + b_{12}a_{23})a_{33}^{-1}$$

$$\ldots$$

Now one can check that this formula for B does give the inverse and that it lies in $UT_n(F)$.

We have to prove the last statement. Suppose that $A, B \in UT(n)$. Let $C = AB$. If $i > k$, then

$$c_{ik} = \sum_j a_{ij} b_{jk} = a_{ii} b_{ik} + a_{i,i+1} b_{i+1,k} + \ldots = 0$$

and

$$c_{ii} = \sum_j a_{ij} b_{ji} = a_{ii} b_{ii} \neq 0$$

which shows that $C \in UT_n(F)$. □

Definition 8.5. *A subset S of a group G is called a subgroup if*

1. *S contains the identity,*
2. *S is closed under multiplication (or whatever the operation is called in G): if $g, h \in S$ then $gh \in S$,*
3. *S is closed under inversion: if $g \in S$ then $g^{-1} \in S$.*

Since clearly $I \in UT_n(F)$, the previous theorem shows that $UT(n)$ is a subgroup of $GL_n(F)$. It is worth observing that

Proposition 8.6. *A subgroup is a group.*

Given an $n \times n$ matrix $A = (a_{ij})$, the *transpose* is the $n \times n$ matrix $A^T = (a_{ji})$. An $n \times n$ matrix A is *orthogonal* if

$$AA^T = I$$

Lemma 8.7. *If A is orthogonal then $A^{-1} = A^T$.*

Proof. The matrix equation $AA^T = I$ is equivalent to $\sum_j a_{ij} a_{jk} = \delta_{ik}$. This implies $A^T A = I$, which together with the first equation implies that $A^{-1} = A^T$. □

The following will be proved in your homework.

Theorem 8.8. *The set of orthogonal matrices forms a subgroup of $GL_n(F)$.*

Let us finally go back to one of the earliest themes, which is the symmetry group of a triangle. But now we do this using matrices, which will actually be messier than what we did before. We place an equilateral triangle in the plane with vertices given by column vectors $A = (1,0)^T$, $B = (\cos\frac{2\pi}{3}, \sin\frac{2\pi}{3})^T = (-\frac{1}{2}, \frac{\sqrt{3}}{2})^T$ and $C = (\cos\frac{4\pi}{3}, \sin\frac{4\pi}{3})^T = (-\frac{1}{2}, -\frac{\sqrt{3}}{2})^T$. The rotation $A \to B \to C$ is given by the matrix

$$R = \begin{pmatrix} \cos\frac{2\pi}{3} & -\sin\frac{2\pi}{3} \\ \sin\frac{2\pi}{3} & \cos\frac{2\pi}{3} \end{pmatrix}$$

There is a second rotation

$$R^2 = \begin{pmatrix} \cos\frac{4\pi}{3} & -\sin\frac{4\pi}{3} \\ \sin\frac{4\pi}{3} & \cos\frac{4\pi}{3} \end{pmatrix}$$

and of course the identity, which is given by the identity matrix I. Finally there are the three flips F_{AB}, F_{BC} and F_{AC}, where F_{AB} interchanges AB etc. The second one is easy to work explicitly

$$F = F_{BC} = \begin{pmatrix} 1 & 0 \\ 0 & -1 \end{pmatrix}$$

For the other two flips, we recall that they are given by

$$FR = \begin{pmatrix} \cos\frac{2\pi}{3} & \sin\frac{2\pi}{3} \\ \sin\frac{2\pi}{3} & -\cos\frac{2\pi}{3} \end{pmatrix}$$

and FR^2 which can be also be multiplied out. We can see that $FRA = B$, so it must be F_{AB}. Collecting these gives the set

$$T = \{I, R, R^2, F, FR, FR^2\}$$

Lemma 8.9. *T forms a subgroup of $GL_2(\mathbb{R})$.*

Proof. To actually check that it is closed under multiplication, we can be clever about it by noting that $R^3 = I$. Then the product of any two rotations must be one of I, R, R^2. For the remaining products, we note by direct calculation that $F^2 = I$ and $RF = FR^2$. So *any* product of two elements of T can be as expressed as an element of T. It also clear that R and R^2 are inverse, and everything else is its own inverse. □

We say that elements $g_1, g_2, \ldots, g_n$ *generate* a group S, if every element of S is a product of some combination of the g_i's and their inverses. For example, T is generated by R and F. Also $\mathbb{Z}$ is generated by 1.

Theorem 8.10. *Every subgroup of $(\mathbb{Z}, +, 0)$ is of the form $\mathbb{Z}d = \{nd \mid n \in \mathbb{Z}\}$ for some $d \in Z$.*

Proof. Let S be a subgroup. If $S = \{0\} = \mathbb{Z}0$ then we are done. So we can assume that it contains a nonzero element. Since S is closed under $x \mapsto -x$, we can assume that S contains a positive element. By the well ordering principle, we can choose a smallest positive $d \in S$. Since S is a subgroup $nd \in S$ for any $n \in \mathbb{Z}$. We want to show that all elements of S are of this form. Suppose that $s \in S$ is any other nonzero element. If we can show that d divides Then earlier we proved that $gcd(d, s) = md + ns$ for some integers $m, n \in \mathbb{Z}$. Therefore $gcd(d, s) \in S$ because S is a subgroup. Since $gcd(d, s)$ is also positive, $d \leq gcd(d, s)$. This only possible if $d = gcd(d, s)$. So $d|s$ as we hoped. □

8.11 Exercises

1. Prove that the set of orthogonal matrices forms a subgroup, denoted by $O_n(F)$ of $GL_n(F)$. You can use the following rules $(AB)^T = B^T A^T$, $(A^T)^T = A$, $(AB)^{-1} = B^{-1}A^{-1}$ and $(A^{-1})^{-1} = A$.

2. The group $GL_2(\mathbb{Z}_2)$ consists of the following 6 matrices

$$I, \begin{pmatrix} 1 & 0 \\ 1 & 1 \end{pmatrix}, \begin{pmatrix} 0 & 1 \\ 1 & 0 \end{pmatrix}, \begin{pmatrix} 0 & 1 \\ 1 & 1 \end{pmatrix}, \begin{pmatrix} 1 & 1 \\ 1 & 0 \end{pmatrix}, \begin{pmatrix} 1 & 1 \\ 0 & 1 \end{pmatrix}$$

   Determine the subgroups $O_2(\mathbb{Z}_2)$ and $UT_2(\mathbb{Z}_2)$ and write down the multiplication tables.

3. The order of an element $g \in GL_2(\mathbb{Z}_2)$ is the smallest integer $n > 0$ such that $g^n = I$. Find an element of order 2, call it F. Find an element of order 3, call it R. Verify that R and F generate $GL_2(\mathbb{Z}_2)$.

4. A 2×2 matrix is called *elementary* if it can be obtained from I by applying a single elementary row operation which means that

   - A multiple of one row is added to another,
   - One row is multiplied by a nonzero element of the field,
   - Two rows are interchanged.

   Check that an elementary matrix is invertible, and that the inverse is also elementary. Do the set of elementary matrices form a subgroup of $GL_2(F)$?

5. Let p be prime. Prove that a subgroup of $(\mathbb{Z}_p, +, 0)$ must be either 0 or $\mathbb{Z}_p$ itself. Hint: if it is not zero, show that the group contains 1.