Matrix Groups

Many groups have matrices as their elements. The operation is usually either matrix addition or matrix multiplication.

Example. Let G denote the set of all 2×3 matrices with real entries. (Remember that "2×3" means the matrices have 2 *rows* and 3 *columns*.) Here are some elements of G:

$$\begin{bmatrix} 1 & 2 & 3 \\ 4 & 5 & 6 \end{bmatrix}, \quad \begin{bmatrix} 0 & 0 & 0 \\ 0 & 0 & 0 \end{bmatrix}, \quad \begin{bmatrix} 1.17 & -2.46 & \pi\sqrt{3} \\ 147.2 & \dfrac{22}{7} & 0 \end{bmatrix}.$$

Show that G is a group under matrix addition.

If you add two 2×3 matrices with real entries, you obtain another 2×3 matrix with real entries:

$$\begin{bmatrix} a & b & c \\ d & e & f \end{bmatrix} + \begin{bmatrix} u & v & w \\ x & y & z \end{bmatrix} = \begin{bmatrix} a+u & b+v & c+w \\ d+x & e+y & f+z \end{bmatrix}.$$

That is, addition yields a binary operation on the set.
You should know from linear algebra that matrix addition is associative.
The identity element is the 2×3 zero matrix:

$$\begin{bmatrix} 0 & 0 & 0 \\ 0 & 0 & 0 \end{bmatrix} + \begin{bmatrix} a & b & c \\ d & e & f \end{bmatrix} = \begin{bmatrix} a & b & c \\ d & e & f \end{bmatrix}, \quad \begin{bmatrix} a & b & c \\ d & e & f \end{bmatrix} + \begin{bmatrix} 0 & 0 & 0 \\ 0 & 0 & 0 \end{bmatrix} = \begin{bmatrix} a & b & c \\ d & e & f \end{bmatrix}.$$

The inverse of a 2×3 matrix under this operation is the matrix obtained by negating the entries of the original matrix:

$$\begin{bmatrix} a & b & c \\ d & e & f \end{bmatrix} + \begin{bmatrix} -a & -b & -c \\ -d & -e & -f \end{bmatrix} = \begin{bmatrix} 0 & 0 & 0 \\ 0 & 0 & 0 \end{bmatrix}, \quad \begin{bmatrix} -a & -b & -c \\ -d & -e & -f \end{bmatrix} + \begin{bmatrix} a & b & c \\ d & e & f \end{bmatrix} = \begin{bmatrix} 0 & 0 & 0 \\ 0 & 0 & 0 \end{bmatrix}.$$

Notice that I *don't* get a group if I try to apply matrix addition to the set of *all* matrices with real entries. This does not define a binary operation on the set, because matrices of different dimensions can't be added.

In general, the set of $m \times n$ matrices with real entries — or entries in $\mathbb{Z}$, $\mathbb{Q}$, $\mathbb{C}$, or $\mathbb{Z}_n$ for $n \geq 2$ form a group under matrix addition.

As a special case, the $n \times n$ matrices with real entries forms a group under matrix addition. This group is denoted $M(n, \mathbb{R})$. As you might guess, $M(n, \mathbb{Q})$ denotes the group of $n \times n$ matrices with rational entries (and so on). $\square$

Example. Let G be the group of 3×4 matrices with entries in $\mathbb{Z}_3$ under matrix addition.

(a) What is the order of G?

(b) Find the inverse of $\begin{bmatrix} 1 & 1 & 2 \\ 0 & 2 & 1 \end{bmatrix}$ in G.

(a) A 3×4 matrix has $3 \cdot 4 = 12$ entries. Each entry can be any one of the 3 elements of $\mathbb{Z}_3$. Therefore, there are $3^{12} = 531441$ elements. $\square$

(b)

$$\begin{bmatrix} 1 & 1 & 2 \\ 0 & 2 & 1 \end{bmatrix} + \begin{bmatrix} 2 & 2 & 1 \\ 0 & 1 & 2 \end{bmatrix} = \begin{bmatrix} 0 & 0 & 0 \\ 0 & 0 & 0 \end{bmatrix}.$$

Hence, the inverse is $\begin{bmatrix} 2 & 2 & 1 \\ 0 & 1 & 2 \end{bmatrix}$. $\square$

Example. Let

$$G = \left\{ \begin{bmatrix} 0 & x \\ 0 & y \end{bmatrix} \,\middle|\, x, y \in \mathbb{R} \right\}.$$

In words, G is the set of 2×2 matrices with real entries having zeros in the first column. Show that G is a group under matrix addition.

First,

$$\begin{bmatrix} 0 & x_1 \\ 0 & y_1 \end{bmatrix} + \begin{bmatrix} 0 & x_2 \\ 0 & y_2 \end{bmatrix} = \begin{bmatrix} 0 & x_1 + x_2 \\ 0 & y_1 + y_2 \end{bmatrix} \in G.$$

That is, if you add two elements of G, you get another element of G. Hence, matrix addition gives a binary operation on the set G.

From linear algebra, you know that matrix addition is associative.

The zero matrix $\begin{bmatrix} 0 & 0 \\ 0 & 0 \end{bmatrix}$ is the identity under matrix addition; it's an element of G, since its first column is all-zero.

Finally, the additive inverse of an element $\begin{bmatrix} 0 & x \\ 0 & y \end{bmatrix} \in G$ is $\begin{bmatrix} 0 & -x \\ 0 & -y \end{bmatrix}$, which is also an element of G. Thus, every element of G has an inverse.

All the axioms for a group have been verified, so G is a group under matrix addition. $\square$

Example. Consider the set of matrices

$$G = \left\{ \begin{bmatrix} 1 & x \\ 0 & 1 \end{bmatrix} \,\middle|\, x \in \mathbb{R}, \quad x \ge 0 \right\}.$$

(Notice that x must be *nonnegative*). Is G a group under matrix multiplication?

First, suppose that $x, y \in \mathbb{R}$, $x, y \ge 0$. Then

$$\begin{bmatrix} 1 & x \\ 0 & 1 \end{bmatrix} \begin{bmatrix} 1 & y \\ 0 & 1 \end{bmatrix} = \begin{bmatrix} 1 & x + y \\ 0 & 1 \end{bmatrix}.$$

Now $x + y \ge 0$, so $\begin{bmatrix} 1 & x + y \\ 0 & 1 \end{bmatrix} \in G$. Therefore, matrix multiplication gives a binary operation on G.

I'll take for granted the fact that matrix multiplication is associative.

The identity for multiplication is $\begin{bmatrix} 1 & 0 \\ 0 & 1 \end{bmatrix}$, and this is an element of G.

However, not all elements of G have inverses. To give a specific counterexample, suppose that for $x \ge 0$

$$\begin{bmatrix} 1 & x \\ 0 & 1 \end{bmatrix} \begin{bmatrix} 1 & 2 \\ 0 & 1 \end{bmatrix} = \begin{bmatrix} 1 & 0 \\ 0 & 1 \end{bmatrix}$$

Then

$$\begin{bmatrix} 1 & x + 2 \\ 0 & 1 \end{bmatrix} = \begin{bmatrix} 1 & 0 \\ 0 & 1 \end{bmatrix}.$$

Hence, $x + 2 = 0$ and $x = -2$. This contradicts $x \geq 0$. Hence, the element $\begin{bmatrix} 1 & 2 \\ 0 & 1 \end{bmatrix}$ of G does not have an inverse.

Therefore, G is *not* a group under matrix multiplication. □

Example. $GL(n, \mathbb{R})$ denotes the set of invertible $n \times n$ matrices with real entries, the **general linear group**. Show that $GL(n, \mathbb{R})$ is a group under matrix multiplication.

First, if $A, B \in GL(n, \mathbb{R})$, I know from linear algebra that $\det A \neq 0$ and $\det B \neq 0$. Then

$$\det(AB) = (\det A) \cdot (\det B) \neq 0.$$

Hence, so $AB \in GL(n, \mathbb{R})$. This proves that $GL(n, \mathbb{R})$ is closed under matrix multiplication.

I will take it as known from linear algebra that matrix multiplication is associative.

The identity matrix is the $n \times n$ matrix

$$I = \begin{bmatrix} 1 & 0 & \cdots & 0 \\ 0 & 1 & \cdots & 0 \\ \vdots & \vdots & \ddots & \vdots \\ 0 & 0 & \cdots & 1 \end{bmatrix}.$$

It is the identity for matrix multiplication: $AI = A = IA$ for all $A \in GL(n, \mathbb{R})$.

Finally, since $GL(n, \mathbb{R})$ *is* the set of *invertible* $n \times n$ matrices, every element of $GL(n, \mathbb{R})$ has an inverse under matrix multiplication. □

Example. $GL(2, \mathbb{Z}_3)$ denotes the set of 2×2 invertible matrices with entries in $\mathbb{Z}_3$. The operation is matrix multiplication — but note that all the arithmetic is performed in $\mathbb{Z}_3$.

For example,

$$\begin{bmatrix} 2 & 1 \\ 1 & 2 \end{bmatrix} \begin{bmatrix} 1 & 1 \\ 2 & 1 \end{bmatrix} = \begin{bmatrix} 1 & 0 \\ 2 & 0 \end{bmatrix}.$$

The proof that $GL(2, \mathbb{Z}_3)$ is a group under matrix multiplication follows the proof in the last example. (In fact, the same thing works with any **commutative ring** in place of $\mathbb{R}$ or $\mathbb{Z}_3$; commutative rings will be discussed later.)

(a) What is the order of $\begin{bmatrix} 1 & 1 \\ 0 & 1 \end{bmatrix}$?

(b) Find the inverse of $\begin{bmatrix} 2 & 1 \\ 2 & 2 \end{bmatrix}$.

(a) Notice that

$$\begin{bmatrix} 1 & 1 \\ 0 & 1 \end{bmatrix}^2 = \begin{bmatrix} 1 & 2 \\ 0 & 1 \end{bmatrix} \quad \text{and} \quad \begin{bmatrix} 1 & 1 \\ 0 & 1 \end{bmatrix}^3 = \begin{bmatrix} 1 & 0 \\ 0 & 1 \end{bmatrix}.$$

Therefore, $\begin{bmatrix} 1 & 1 \\ 0 & 1 \end{bmatrix}$ has order 3 in $GL(2, \mathbb{Z}_3)$. □

(b) Recall the formula for the inverse of a 2×2 matrix:

$$\begin{bmatrix} a & b \\ c & d \end{bmatrix}^{-1} = \frac{1}{ad - bc} \begin{bmatrix} d & -b \\ -c & a \end{bmatrix}.$$

The formula works in this situation, but you have to interpret the fraction as a *multiplicative inverse*:

$$\begin{bmatrix} a & b \\ c & d \end{bmatrix}^{-1} = (ad - bc)^{-1} \begin{bmatrix} d & -b \\ -c & a \end{bmatrix}.$$

Thus,

$$\begin{bmatrix} 2 & 1 \\ 2 & 2 \end{bmatrix}^{-1} = (2^{-1}) \begin{bmatrix} 2 & 2 \\ 1 & 2 \end{bmatrix} = 2\ cdot \begin{bmatrix} 2 & 2 \\ 1 & 2 \end{bmatrix} = \begin{bmatrix} 1 & 1 \\ 2 & 1 \end{bmatrix}.$$

On the other hand, the matrix $\begin{bmatrix} 2 & 1 \\ 1 & 2 \end{bmatrix}$ is not an element of $GL(2, \mathbb{Z}_3)$. It has determinant $2 \cdot 2 - 1 \cdot 1 = 0$, so it's not invertible. □

Example. Show that the following set is a subgroup of $GL(2, \mathbb{R})$:

$$SL(2, \mathbb{R}) = \left\{ A \in GL(2, \mathbb{R}) \,\middle|\, \det A = 1 \right\}$$

Suppose $A, B \in SL(2, \mathbb{R})$. Then

$$\det(AB) = (\det A)(\det B) = 1 \cdot 1 = 1.$$

Hence, $AB \in SL(2, \mathbb{R})$.
Since $\det I = 1$, the identity matrix is in $SL(2, \mathbb{R})$.
Finally, if $A \in SL(2, \mathbb{R})$, then $AA^{-1} = I$ implies that

$$(\det A)(\det A^{-1}) = \det I = 1.$$

But $\det A = 1$, so $\det A^{-1} = 1$, and hence $A^{-1} \in SL(2, \mathbb{R})$.
Therefore, $SL(2, \mathbb{R})$ is a subgroup of $GL(2, \mathbb{R})$. □
