19. **Prove that the set of all $2 \times 2$ matrices with entries from $\mathbb{R}$ and determinant $+1$ is a group under matrix multiplication.**

**Solution:** Let $G$ be this (putative) group. We first show that $G$ is closed under multiplication. This is easy if we remember a fact from linear algebra: given matrices $A$ and $B$, $\det(AB) = \det(A)\det(B)$. This shows that if $A$ and $B$ are $\in G$, we must have $\det(AB) = 1$ as well, meaning $AB \in G$. We can also check that the identity element in $G$ is just

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

which has determinant $1 \cdot 1 - 0 \cdot 0 = 1$.

Next we show that $G$ has inverses. From linear algebra, we have the formula

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

which works whenever $ad - bc$ (the determinant) is nonzero. This is certainly the case for $A \in G$, so we at least know that the matrix $A^{-1}$ exists. It remains to check that $A^{-1}$ is actually in $G$. This can be checked by computing the determinant, but we can also notice that since

$$AA^{-1} = I,$$

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

$$= 1$$

Thus if $\det(A) = 1$, the above shows that $\det(A^{-1}) = 1$ as well, which means it is in $G$.

The only thing left is the tedious task of showing that matrix multiplication is actually associative. To this end, let $X = \begin{pmatrix} a & b \\ c & d \end{pmatrix}$, $Y = \begin{pmatrix} e & f \\ g & h \end{pmatrix}$, and $Z = \begin{pmatrix} s & t \\ u & v \end{pmatrix}$. We calculate:

$$A(BC) = \begin{pmatrix} a & b \\ c & d \end{pmatrix} \cdot \begin{pmatrix} es + fu & et + fv \\ gs + hu & gt + hv \end{pmatrix}$$

$$= \begin{pmatrix} a(es + fu) + b(gs + hu) & a(et + fv) + b(gt + hv) \\ c(es + fu) + d(gs + hu) & c(et + fv) + d(gt + hv) \end{pmatrix}$$
On the other hand,

\[(AB)C = \begin{pmatrix} ae + bg & af + gh \\ ce + bg & cf + dh \end{pmatrix} \begin{pmatrix} s & t \\ u & v \end{pmatrix} = \begin{pmatrix} (ae + bg)s + (af + gh)u & (ae + bg)t + (af + gh)v \\ (ce + bg)s + (cf + dh)u & (ce + bg)t + (cf + dh)v \end{pmatrix}\]

and by distributing and using commutativity (and associativity) of multiplication of real numbers, we see that each of the four entries is the same. Therefore the two are equal, and \(G\) is a group.

22. Let \(G\) be a group with the property that for any \(x, y, z\) in the group, \(xy = zx\) implies \(y = z\). Prove that \(G\) is Abelian (“Left-right cancellation” implies commutativity.)

Solution: Given \(a, b \in G\), we must show that \(ab = ba\). Multiplying the LHS by \(b\) on the left and the RHS by \(b\) on the right, we certainly have \(bab = bab\), so letting \(x = b, y = ab, z = ba\), the assumption on \(G\) forces \(ab = ba\), as desired.

26. Prove that in a group \((a^{-1})^{-1} = a\) for all \(a\).

Solution: \((a^{-1})^{-1}\) is the unique element in \(G\) such that \((a^{-1})^{-1}a^{-1} = a^{-1}(a^{-1})^{-1} = e\). But since \(a^{-1}\) is \(a\)'s inverse, \(aa^{-1} = a^{-1}a = e\), so \(a = (a^{-1})^{-1}\).

34. Prove that in a group, \((ab)^2 = a^2b^2\) if and only if \(ab = ba\).

Prove that in a group, \((ab)^{-2} = b^{-2}a^{-2}\) if and only if \(ab = ba\).

Solution: The “if” parts follow from problem 23, so assume that \((ab)(ab) = a^2b^2\). Multiplying on the left by \(a^{-1}\), we see that \(bab = ab^2\). But then we can multiply on the right by \(b^{-1}\), which yields \(ba = ab\).

Now suppose that \((ab)^{-1}(ab)^{-1} = b^{-2}a^{-2}\). Since \((ab)^{-1} = b^{-1}a^{-1}\), we have that \((b^{-1}a^{-1})^2 = (b^{-1})^2(a^{-1})^2\). But then the previous result (with \(b^{-1}\) in place of \(a\) and \(a^{-1}\) in place of \(b\)), shows that \(a^{-1}b^{-1} = b^{-1}a^{-1}\). But then the inverses of both sides are the same, so \(ba = ab\).

36. Let \(a\) and \(b\) belong to a group \(G\). Find an \(x\) in \(G\) such that \(xabx^{-1} = ba\).

Solution: It is equivalent to show \(xabx^{-1}a^{-1} = b\), since we have \(b\)'s in the center of both expressions, one easy way to make them equal is to let \(xa = e\), or \(x = a^{-1}\).