Algebra of binary operations: It is important not to confuse ordinary algebra with the algebra which depends on the properties listed above. It is easy to assume, for example, that $a * b = b * a$, (because $ab = ba$ in multiplicative algebra) but commutativity must be proved first. In algebra, if $ab = ac$ then it follows that $b = c$ (or that $a = 0$). What if $a * b = a * c$?

This is known as the *left cancellation law.* $b * a = c * a \Rightarrow b = c$ is known as the *right cancellation law.* You might like to write out the steps involved.

$a * b = a * c$

$a^{-1} * (a * b) = a^{-1} * (a * c)$ …if a has an inverse

$(a^{-1} * a) * b = (a^{-1} * a) * c$ …if * is associative

$e * b = e * c$ …if the identity exists

$b = c$

So $b = c$ only if the operation * has all the properties on the right.

The general equation $a * x = b$ is solved like this:

$a * x = b$

$a^{-1} * (a * x) = a^{-1} * b$

$(a^{-1} * a) * x = a^{-1} * b$

$e * x = a^{-1} * b$

$x = a^{-1} * b$

These steps can be taken if the properties above hold and also if S is closed under *; if it isn't, we do not know that $a^{-1} * b$ is necessarily in S.

~	*a*	*b*	*c*	*d*
a	*a*	*b*	*c*	*d*
b	*b*	*a*	*d*	*a*
c	*d*	*c*	*a*	*b*
d	*c*	*d*	*b*	*a*

Consider the Cayley table on the left, representing the operation ~ on the set {*a,b,c,d*}. Which of the following properties are demonstrated: closure, the existence of an identity element, an inverse for every element, associativity, commutativity?

The set is closed under ~ because only *a, b, c, d* appear in the body of the table. The identity element is *a* because it generates both a row and a column which equate to the headings *a, b, c, d*. *a, c* and *d* are self-inverse, but there is a problem with *b*. We note that $b \sim d = a$ (the identity), but so does $b \sim b$. Furthermore, $d \sim b \neq a$. So *b* does not have a unique inverse. Associativity can only be proved by testing every triple of elements, but it can be disproved by a counter-example. $(d \sim c) \sim b = a$ but $d \sim (c \sim b) = b$ thus proving ~ is not associative. The table is not symmetrical about the leading diagonal, so ~ is not commutative.

We can also look at the set properties for an infinite set. Consider, for example, natural numbers under addition. Addition is always both associative and commutative. Closure exists because the addition of natural numbers always leads to another natural number. The identity is 0 since $x + 0 = x$ for all natural numbers. However, there are no inverses since that would require negative numbers.

S = $\left\{ \begin{pmatrix} 1 & a \\ 0 & 1 \end{pmatrix} \mid a \in Z \right\}$. Show that S under the operation of matrix multiplication is closed and commutative.

$$\begin{pmatrix} 1 & a \\ 0 & 1 \end{pmatrix}\begin{pmatrix} 1 & b \\ 0 & 1 \end{pmatrix} = \begin{pmatrix} 1 & b+a \\ 0 & 1 \end{pmatrix} \in \text{S} \quad (\text{since } b + a \in \mathbb{Z}) \quad \therefore \text{ closed}$$

$$\begin{pmatrix} 1 & b \\ 0 & 1 \end{pmatrix}\begin{pmatrix} 1 & a \\ 0 & 1 \end{pmatrix} = \begin{pmatrix} 1 & a+b \\ 0 & 1 \end{pmatrix} = \begin{pmatrix} 1 & b+a \\ 0 & 1 \end{pmatrix} \quad \therefore \text{ commutative}$$

Note that matrix multiplication in general is not commutative, although it is associative.

You might also like to show that there is an identity and that every element in S has an inverse.