Binary Operations

The Cartesian cross product of set A with set B, where neither A nor B is the empty set, is defined to be the set of all ordered pairs (x, y) such that $x \in A$ and $y \in B$. The symbol for the cross product above is $A \times B$.

Examples:

1) $\{a, b, c\} \times \{b, d\} = \{(a, b), (a, d), (b, b), (b, d), (c, b), (c, d)\}$

2) If $S = \{1, 5\}$, $S \times S = \{(1, 1), (1, 5), (5, 1), (5, 5)\}$

3) The Cartesian cross product of the set of all real numbers with itself is geometrically represented as the Cartesian coordinate system used throughout mathematics beginning with graphs in elementary algebra.

A binary operation on a set S is a function f whose domain is a subset of $S \times S$ and whose range is a subset of S. We will denote this:

$$f : S \times S \rightarrow S$$

You have used numerous binary operations during your education. Addition in the real number system is a binary operation. Matrix multiplication is a binary operation. The intersection of sets is a binary operation. There are countless examples of binary operations you have used.
For example, if f represents real numbers subtraction (i.e. $f(a, b) = a - b$) then $f(2, 5) = -3$ while $f(5, 2) = 3$. You may wonder why we define the domain of f to possibly not be all of $S \times S$. There are practical considerations that might prove troublesome in our development of abstract algebra. For example, suppose f represents real number division. Specifically, f is defined by $f(a, b) = \frac{a}{b}$. $f(3, 0)$ would not be a real number. Hence, if S is the set of real numbers, the domain of f is a subset of $S \times S$. Possibly it has crossed your mind to redefine S as the set of non-zero reals (you already think like a mathematician). Now the domain of f is all of $S \times S$. However, we lose the useful result that $\frac{0}{4} = 0$ since 0 is no longer an element of S! On the other hand, the range of a binary operation need not be the entire set S. Suppose S is again the set of all real numbers. Let's define $f : S \times S \rightarrow S$ by $F(a, b) = |a| + |b|$. For example, $f(\text{-}4, 6) = 10$. Note that -8 is not an element in the range of f.

Please note that some of the operations you have studied in mathematics are not binary operations. The dot product of two vectors in 2-space results in a real number called a scalar. To be a binary operation, the dot product would have to produce a vector in 2-space.

The definition of a binary operation is somewhat cumbersome to use and we will need some type of simplified notation. To continue to use function notation to represent a binary operation is not practical. We will instead use ★ to represent a generic binary operation.

$$a \bigstar b \text{ will replace } f(a, b)$$

When contemplating the creation of a new binary operation, one of the most important considerations we will confront is the issue of "well defined". A binary operation is well defined if and only if (iff) whenever $x = q$ and $y = t$ then $x \bigstar y = q \bigstar t$. The binary operations you have previously studied in mathematics are virtually all "well defined". Further, if a binary operation is not well defined, we will have no use for it in this course.

An example can be illuminating. If you are like me, when addition of fractions was introduced in grade school, you would have preferred that $\frac{a}{b} + \frac{c}{d}$ resulted in $\frac{a+c}{b+d}$. Could addition of fractions have been defined this way? We know that $\frac{1}{3} = \frac{2}{6}$ and $\frac{1}{2} = \frac{7}{14}$. Therefore, if addition of fractions as proposed above was well defined: $\frac{1}{3} + \frac{1}{2}$ would equal $\frac{2}{6} + \frac{7}{14}$. However, $\frac{2}{5}$ does <u>not</u> equal $\frac{9}{20}$ and this operation is <u>not</u> well defined.

Unless "well defined" is a specific issue to be contemplated in a homework problem or development of material in the text, we will adopt the convention that whenever a "binary operation" is referred to it will mean a "well defined binary operation".

Let's look at an example of the use of "well defined" in a procedure you have used frequently. In high school algebra, you were asked to solve equations like: $2x = 16$. You were probably told to multiply both sides by $\frac{1}{2}$ and the procedure probably looked like:

$$\begin{aligned} 2x &= 16 \\ \frac{1}{2} \cdot 2x &= \frac{1}{2} \cdot 16 \\ x &= 8 \end{aligned}$$

Let's examine closely the second step. Why is $\frac{1}{2} \cdot 2x$ equal to $\frac{1}{2} \cdot 16$? Well, you know that $\frac{1}{2}=\frac{1}{2}$. (This is called the reflexive property of equality.) You are given $2x = 16$. Therefore, the second line in the above series of equations is a direct consequence of the fact that real number multiplication is well defined.

There are numerous properties that can be used to describe the behavior of a binary operation. We will consider a few of these now.

<u>Commutivity</u>

A binary operator $\bigstar$ is said to be commutative iff $a \bigstar b = b \bigstar a$ for every a and b in S. Real number addition and multiplication are commutative operations. Subtraction and division in the real number system are not commutative. Addition of 2×2 matrices is a commutative operation, but multiplication of 2×2 matrices is not commutative. Specifically,

$$\begin{pmatrix} 2 & -1 \\ 3 & 0 \end{pmatrix} \cdot \begin{pmatrix} 1 & 1 \\ 0 & 0 \end{pmatrix} = \begin{pmatrix} 2 & 2 \\ 3 & 3 \end{pmatrix}$$

but

$$\begin{pmatrix} 1 & 1 \\ 0 & 0 \end{pmatrix} \cdot \begin{pmatrix} 2 & -1 \\ 3 & 0 \end{pmatrix} = \begin{pmatrix} 5 & -1 \\ 0 & 0 \end{pmatrix}$$

Please notice that one counter example is sufficient to prove that a proposition is not true. Later, we will stress that examples are not sufficient to prove that a proposition is true unless the examples are exhaustive.

Associativity

A binary operation $\bigstar$ is said to be associative on the set S iff $(x \bigstar y) \bigstar z = x \bigstar (y \bigstar z)$ for every x, y and z in S. We will refer at times to the above equation as the Associativity Test Equation (ATE). Both addition and multiplication in the real number system as usually defined are associative operations. However, subtraction is not. Consider the ATE:

$$(x - y) - z = x - (y - z)\,?$$

Let $x = 8$, $y = 5$ and $z = 1$.

$(x - y) - z$ can be thought of as $3 - 1$ which equals 2. $x - (y - z)$ can be thought of as $8 - 4$ which equals 4. This demonstrates that subtraction is not associative. Notice how we have used the parentheses to give priority to operations. This is consistent with the use of parentheses in high school algebra. Also, it highlights the fact that subtraction is a binary operation. We have the right at any time to think of the symbol $(a \bigstar b)$ as a single element of the set S by the very definition of a binary operation.

It is natural to think of associativity as a three element property. However, associativity (once established) for an operation $\bigstar$ can be easily extended to prove equality of expressions with four elements or more such as: $(a \bigstar b) \bigstar (c \bigstar d) = a \bigstar \big(b \bigstar (c \bigstar d)\big)$. This equation is a direct consequence of our original associative property if we think of the expression $(c \bigstar d)$ as a single element of S (which it has to be by the definition of a binary operation). Further, if a binary operation is both associative and commutative, we can become quite lax in our use of parentheses. For example, if we write $a \bigstar b \bigstar c \bigstar d$ it does not matter if one student computes $a \bigstar \big(b \bigstar (c \bigstar d)\big)$ and another computes $(a \bigstar d) \bigstar (c \bigstar b)$ or any of a number of other possibilities. Let's see why. If we assume $\bigstar$ is both associative and commutative then:

$$\begin{aligned} & a \bigstar \big(b \bigstar (c \bigstar d)\big) \\ &= a \bigstar \big(b \bigstar (d \bigstar c)\big) && \text{commutative property} \\ &= a \bigstar \big((b \bigstar d) \bigstar c\big) && \text{associative property} \\ &= a \bigstar \big((d \bigstar b) \bigstar c\big) && \text{commutative property} \\ &= a \bigstar \big(d \bigstar (b \bigstar c)\big) && \text{associative property} \\ &= (a \bigstar d) \bigstar (b \bigstar c) && \text{associative property} \\ &= (a \bigstar d) \bigstar (c \bigstar b) && \text{commutative property} \end{aligned}$$

Therefore, where appropriate, we will drop parentheses altogether. We must, however, be very careful that we differentiate where we can and where we can not do this.

Let's practice the Associativity Test Equation in a more difficult setting.

Theorem: Prove that multiplication of 2×2 matrices over the real number system is associative.

Proof: The ATE demands that we demonstrate:

$$\left(\begin{pmatrix} a & b \\ c & d \end{pmatrix} \cdot \begin{pmatrix} e & f \\ g & h \end{pmatrix}\right) \cdot \begin{pmatrix} i & j \\ k & l \end{pmatrix} = \begin{pmatrix} a & b \\ c & d \end{pmatrix} \cdot \left(\begin{pmatrix} e & f \\ g & h \end{pmatrix} \cdot \begin{pmatrix} i & j \\ k & l \end{pmatrix}\right)$$

for all real numbers $a, b, \ldots, l$.

The left hand side of this equation can be computed as follows:

$$\begin{aligned}
&\left(\begin{pmatrix} a & b \\ c & d \end{pmatrix} \cdot \begin{pmatrix} e & f \\ g & h \end{pmatrix}\right) \cdot \begin{pmatrix} i & j \\ k & l \end{pmatrix} \\
&= \begin{pmatrix} ae + bg & af + bh \\ ce + dg & cf + dh \end{pmatrix} \cdot \begin{pmatrix} i & j \\ k & l \end{pmatrix} \\
&= \begin{pmatrix} aei + bgi + afk + bhk & aej + bgj + afl + bhl \\ cei + dgi + cfk + dhk & cej + dgj + cfl + dhl \end{pmatrix}
\end{aligned}$$

Now let's turn our attention to the right hand side:

$$\begin{aligned}
&\begin{pmatrix} a & b \\ c & d \end{pmatrix} \cdot \left(\begin{pmatrix} e & f \\ g & h \end{pmatrix} \cdot \begin{pmatrix} i & j \\ k & l \end{pmatrix}\right) \\
&= \begin{pmatrix} a & b \\ c & d \end{pmatrix} \cdot \begin{pmatrix} ei + fk & ej + fl \\ gi + hk & gj + hl \end{pmatrix} \\
&= \begin{pmatrix} aei + afk + bgi + bhk & aej + afl + bgj + bhl \\ cei + cfk + dgi + dhk & cej + cfl + dgj + dhl \end{pmatrix}
\end{aligned}$$

The two results might look at first quite different. Remember, however, that real number addition is associative and commutative (which already has been assumed in creating these steps). A close inspection shows that the two sides are equal and associativity has been established.

Closure

A binary operation ★ is said to be closed on a set A iff whenever $x \in A$ and $y \in A$ then $x ★ y$ is also an element of A.

Consider real number multiplication used on the set of positive odd integers. It would certainly seem to be closed. $3 \cdot 5 = 15$ which is an odd integer. $7 \cdot 9 = 63$ which is also an odd integer. However, all the examples we could come up with do not constitute a proof of closure. How could we prove that multiplication is closed on the set of positive odd integers? First, we need to remember the definition of a positive odd integer. It is an integer that can be put in the form $2q + 1$ where q is an integer and $q \geq 0$.

Let x and y both be positive odd integers. $x = 2q + 1$ and $y = 2r + 1$ where q and r are non-negative integers.

$$\begin{aligned} x \cdot y &= (2q+1) \cdot (2r+1) \\ &= 4qr + 2q + 2r + 1 \\ &= 2(2qr + q + r) + 1 \end{aligned}$$

Since q and r are non-negative integers, $2qr + q + r$ must be a non-negative integer (admittedly, this assumes we have studied some other closure considerations). Notice, $2(2qr + q + r) + 1$ is precisely of the form required to be a positive odd integer.

Let's look at some more examples:

1. Division is not closed on the real number system since 4 is a real number and 0 is a real number but $\frac{4}{0}$ is not a real number.

2. Addition is not closed on the set of positive odd integers since 3 and 5 are both positive odd integers, but $3 + 5$ is not.

3. Matrix addition is not closed on the set of non-singular matrices (those whose determinants are not 0) because both $\begin{pmatrix} 3 & 5 \\ 1 & 8 \end{pmatrix}$ and $\begin{pmatrix} -3 & -5 \\ -1 & -8 \end{pmatrix}$ are nonsingular, but $\begin{pmatrix} 3 & 5 \\ 1 & 8 \end{pmatrix} + \begin{pmatrix} -3 & -5 \\ -1 & -8 \end{pmatrix} = \begin{pmatrix} 0 & 0 \\ 0 & 0 \end{pmatrix}$ which is singular.

Possession of an Identity

A binary operation ★ defined on a set S is said to possess an identity iff $\exists$ an element e in S (e will be our generic symbol for an identity) $\ni x ★ e = x$ and $e ★ x = x$ for every x in S.

0 is the identity for addition in the real number system since $0 + x = x + 0 = x$ for every real number x. Subtraction in the real number system does not possess an identity. $4 - 0 = 4$ and it would seem that 0 is an identity. However, $0 - 4 \neq 4$.

A binary operation ★ may possess an identity whether or not the operation is commutative. Here are a few examples of identities:

1. $\left(\begin{smallmatrix}1 & 0\\ 0 & 1\end{smallmatrix}\right)$ for the 2×2 matrices under multiplication (a non-commutative operation)

2. 1 for the reals under multiplication

3. $\left(\begin{smallmatrix}0 & 0\\ 0 & 0\end{smallmatrix}\right)$ for the 2×2 matrices under addition

4. $\langle 0, 0, 0\rangle$ for 3-space vectors under addition

5. ϕ for any specific collection of sets that contains ϕ where the operation is set union.

Theorem: If a set S is endowed with a well defined binary operation ★, S can not contain two different identities with respect to ★.

Proof: Suppose not. Suppose S possesses elements e_1 and e_2 such that :

1. e_1 is an identity with respect to (wrt) ★

2. e_2 is an identity wrt ★

and 3. $e_1 \neq e_2$

$e_1 \bigstar e_2 = e_1$ because e_2 is an identity.
$e_1 \bigstar e_2 = e_2$ because e_1 is an identity.
Because ★ is well defined, $e_1 \bigstar e_2 = e_1 \bigstar e_2$.
$\therefore e_1 = e_2$
This is a contradiction (symbolized: $\rightarrow \leftarrow$)

QED

We now know that when an identity exists, it is unique.

Inverses

We can not even use the term "inverse" unless the set S is known to possess an identity e wrt the binary operation ★. If this is the case, an element x in S is said to possess an inverse (which we will denote x^{-1}) iff:

1. $x \bigstar x^{-1} = e$

and

2. $x^{-1} \bigstar x = e$.

For particular choices of S and ★, some elements could possess inverses and others not. If S is the set of all integers and ★ represents multiplication, 4 does not possess an inverse. Remembering that $e = 1$ in this example, there does not exist an integer x such that $4 \cdot x = 1$ and $x \cdot 4 = 1$ ($\frac{1}{4}$ is not an integer). However, -1 does possess an inverse. Since $(-1) \cdot (-1) = 1$, we know that $(-1)^{-1} = -1$. Such an element in a set S is said to be self invertable.

If an identity e exists for a binary operation ★ defined on a set S, e is always self invertable ($e ★ e = e$ by the definition of an identity). We call e the trivial self invertable element.

Another interesting case is the set of all 2×2 matrices over the reals using matrix multiplication. $e = \begin{pmatrix} 1 & 0 \\ 0 & 1 \end{pmatrix}$ in this case. $\begin{pmatrix} 2 & 3 \\ -1 & 4 \end{pmatrix}^{-1} = \begin{pmatrix} \frac{4}{11} & \frac{-3}{11} \\ \frac{1}{11} & \frac{2}{11} \end{pmatrix}$ which you should verify. $\begin{pmatrix} 3 & 6 \\ 1 & 2 \end{pmatrix}^{-1}$ does not exist since $\begin{pmatrix} 3 & 6 \\ 1 & 2 \end{pmatrix}$ is a singular matrix.

Let's list a few more examples:

1. For the reals under multiplication, $4^{-1} = \frac{1}{4}$.

2. For the reals under addition, $4^{-1} = -4$.

3. For the reals under multiplication, 0^{-1} does not exist.

4. For 3-space vectors under addition, $\left\langle 1, 2, -5 \right\rangle^{-1} = \left\langle -1, -2, 5 \right\rangle$.

Our notation for "inverse" may seem misleading to you (especially in examples 2 and 4 above). You have encountered a similar use of this notation previously. In calculus, $y = sin^{-1}x$ is a synonym for $y = arc\,sin\,x$. To be specific, $sin^{-1}x$ does not denote $\frac{1}{sin\,x}$ (or $csc\,x$). Interestingly, $y = sin^{-1}x$ is called the "inverse" sine function.

A Few Last Words

The symbol ★ has played an instructional role throughout this chapter. Among mathematicians, an unknown or alien binary operation is usually denoted by the dot used for multiplication in high school algebra or juxtaposition. Therefore, in future chapters $a ★ b$ will become $a \cdot b$ or ab unless some particular emphasis is intended. It is important that you not assume that the symbols $a \cdot b$ and ab represent real number multiplication. When the context is such that these symbols clearly represent real multiplication, then they can be read in the usual way.