Chapter 9

Associativity

In the **Binary Operations** chapter we learned that *a binary operation on a set* is one of the central characters of a group. One of the other defining characters of a group is the property of *associativity* of a binary operation. For a brief moment in time mathematicians toyed around with the idea of including the property of *commutativity* of a binary operation into the definition of a group as well.

However, historically, this way or that way, it was shaken out that across these two popular properties of a binary operation on a set, that of *associativity* and that of *commutativity*, it is the property of the said operation of being *associative* is the defining one, while the property of the said operation of being *commutative* is not, even though the theory of commutative or *Abelian* groups is a sizable one.

Putting the cart before the horse somewhat, in the upcoming **Group Axioms** chapter, it is this property of *associativity* of a binary operation on a set that is baked into the heart and soul of the axiomatic definition of a group, while the property of commutativity is left out of it.

Thus, it pays to become reasonably well familiar with exactly what does the associativity of a binary operation defined on a certain set is, exactly what does it entail, which, as we are about to discover, is quite a bit, and how it differs from the commutativity property of the said operation.

In this chapter we will give an official definition of the associativity of a binary operation and we will prove our first, and a very important, group-theoretic theorem.

For a motivating example consider the operation of exponentiation defined on the set of positive integers.

Such an operation is certainly binary because any positive integer raised to a positive integral power is, again, a positive integer.

We now wonder if a string of two consecutive exponentiations will or will not produce the same result regardless of the order in which the individual exponentiations of that string are carried out, *while the order of the positive integers themselves remains fixed*?

Well. We quickly see that, on the one hand, it is the case that:

$$\left(3^2\right)^4 = 9^4$$

and, on the other hand, it is the case that:

$$3^{\left(2^4\right)} = 3^{16} = 3^{2 \cdot 8} = 9^8 \neq 9^4$$

We, thus, conclude that the binary operation of exponentiation defined on the set of positive integers is very sensitive to the order in which the individual exponentiations are carried out in a string of two consecutive such operations.

Formally, if for any two positive integers a and b we define:

$$a \circ b \equiv a^b$$

then, in general, there exist positive integers a, b, c such that:

$$\left(a^b\right)^c \neq a^{\left(b^c\right)}$$

or:

$$(a \circ b) \circ c \neq a \circ (b \circ c)$$

In other words, it is *not* the case that for all positive integers a, b, c the following equality:

$$(a \circ b) \circ c = a \circ (b \circ c)$$

holds.

Hence, in vacuum and without the special agreements and conventions, in this particular case the following symbolic expression:

$$a \circ b \circ c = a^{b^c}$$

is meaningless because in general it is impossible to assign one specific and non-ambiguous result to such an expression.

The existence of the right-associative convention that attempts to assign a unique value to a tower of powers or *tetration* expressions does not change the fact that the binary operation at hand is not associative.

Our readers are encouraged to convince themselves, as a separate informal exercise, that the binary operation of *division* defined on the set of *positive rational* numbers:

$$a \circ b \equiv a \div b$$

in general, is also highly sensitive to the order in which the individual divisions are carried out in a string of two consecutive such operations and is, thus, not associative.

Again, the existence of the left-associative convention that attempts to assign a unique value to the above expressions does not change the fact that the binary operation at hand is not associative.

On the other hand, in the additive group of integers we already came across a binary operation of *addition* defined on the set of *integers*:

$$a \circ b \equiv a + b$$

that is completely numb to the order of the individual operations in a string of two consecutive additions.

That is, for any three integers a, b, c it is the case that:

$$(a + b) + c = a + (b + c)$$

or:

$$(a \circ b) \circ c = a \circ (b \circ c)$$

In this particular case, since no matter how a string of two consecutive additions of integers is sliced one and the same particular integer always results, it becomes possible to omit the order of execution/evaluation modifiers, the parentheses $()$, and simply write:

$$(a + b) + c = a + (b + c) = a + b + c$$

or:

$$(a \circ b) \circ c = a \circ (b \circ c) = a \circ b \circ c$$

without any fear of introducing a confusing and an unwelcome ambiguity into the meaning of the $a \circ b \circ c$ expression above.

The first two sample binary operations above are said to be *not associative*, while the third sample binary operation above is said to be *associative* and we can now record an official definition of the associativity of binary operations.

Definition 11: a binary operation $\circ$ defined on a set G is *associative* if for any three elements a, b, c of the set G the following relationship:

$$(a \circ b) \circ c = a \circ (b \circ c) \tag{1}$$

holds.

It is important to keep in mind that in the defining relationship (**1**) *the order of the elements* a, b, c with respect to the operations $\circ$ remains the same on either side of the equal sign.

We also would like to remind our readers about *the strength* of the universal requirement imposed on the elements of a set in the **Definition 11**. From the **All, Every, Each, Any, Exists, If P Then Q** chapter we remember that in some intuitive sense it is laughably easy to invalidate such universal requirements or claims.

Namely, if in a given set G there exist just one measly triplet of elements x, y, z for which the relationship shown in (**1**) does *not* hold then the game is over - the binary operation defined on such a set is *not* associative, regardless of how many other triplets of that set do honor the relationship (**1**).

Commutativity

Using the same set of positive integers, we also notice that it is always possible to find two positive integers, say, 2 and 3, for which their order in a single operation of exponentiation produces different results:

$$2^3 = 8 \neq 9 = 3^2$$

which is to say that there exist positive integers a and b such that:

$$a^b \neq b^a$$

or:

$$a \circ b \neq b \circ a$$

In other words, over the set of positive integers it is *not* the case that for any two positive integers a and b the following relationship:

$$a^b = b^a$$

or:

$$a \circ b = b \circ a$$

holds.

Likewise, our readers are encouraged to convince themselves, as a separate informal exercise, that over the set of positive rational numbers it is *not* the case that for any two positive rational numbers a and b the following relationship holds:

$$a \div b = b \div a$$

Put, say, $a = 1/2$ and $b = 2/3$ for a counterexample:

$$\frac{1}{2} \div \frac{2}{3} = \frac{3}{4} \neq \frac{4}{3} = \frac{2}{3} \div \frac{1}{2}$$

But over the set of integers it *is* the case that for any two integers a and b the following relationship:

$$a + b = b + a$$

holds.

The first two sample binary operations above are said to be *not commutative*, while the third sample binary operation above is said to be *commutative* and we can now record an official definition of a commutativity of binary operations.

Definition 12: a binary operation $\circ$ defined on a set G is *commutative* if for any two elements a, b of the set G the following relationship:

$$a \circ b = b \circ a \tag{2}$$

holds.

If the relationship shown in (**2**) holds for some two elements p and q of a given set under a given binary operation then mathematicians simply say that:

$$\textit{the elements } p \textit{ and } q \textit{ commute (under } \circ\textit{):} \; p \circ q = q \circ p$$

Such a jargonish shorthand way of interpreting the relationship in (**2**) in the English language gives birth to a famous joke:

- What is purple and commutes? An Abelian grape.

In our first **Group Axioms** discussion we will understand the punchline of that joke.

If the relations shown in (**2**) does *not* hold for some two elements r and s of a given set under a given operation then mathematicians simply say that:

$$\textit{the elements } r \textit{ and } s \textit{ do not commute (over } \circ\textit{):} \; r \circ s \neq s \circ r$$

Here, again, we pay a close attention to the fact that **Definition 12** is built around *a universal* requirement - if there exists just one measly pair of elements x, y of the set G that does not commute under a certain operation $\circ$, meaning that $x \circ y \neq y \circ x$, then the proposed binary operation is *not* commutative, regardless of how many other pairs of elements of the given set do commute under the given operation.

Do feel the difference between the above two properties of a binary operation: if the order of the operands in the definition of the associativity property remains strictly fixed, the order of the operands in the definition of the commutativity property gets necessarily shuffled.

In other words, the property of associativity of a binary operation defined on a set is *independent* from the property of commutativity of a binary operation defined on the same set. That is, there exist binary operations defined over the corresponding sets that are:

- associative and commutative
- neither associative nor commutative
- associative but not commutative and
- not associative but commutative

Below we illustrate the above statements with specific examples.

Associative and Commutative

The binary operation of addition of integers is both associative:

$$a + (b + c) = (a + b) + c$$

and commutative:

$$a + b = b + a$$

since the above equalities hold for any three integers a, b, c.

The binary operation of multiplication of integers is also both associative:

$$a \cdot (b \cdot c) = (a \cdot b) \cdot c$$

and commutative:

$$a \cdot b = b \cdot a$$

since the above equalities also hold for any three integers a, b, c.

Neither Associative Nor Commutative

The binary operation of exponentiation of positive natural numbers is neither associative:

$$(4^3)^2 = 4096 \neq 262144 = 4^{(3^2)}$$

nor commutative:

$$4^3 = 64 \neq 81 = 3^4$$

The binary operation of division of positive rational numbers is neither associative:

$$\left(\frac{3}{2} \div \frac{7}{4}\right) \div \frac{5}{9} = \frac{54}{35} \neq \frac{10}{21} = \frac{3}{2} \div \left(\frac{7}{4} \div \frac{5}{9}\right)$$

nor commutative:

$$\frac{3}{2} \div \frac{7}{4} = \frac{6}{7} \neq \frac{7}{6} = \frac{7}{4} \div \frac{3}{2}$$

also.

Associative But Not Commutative

One of the most important examples of a binary operation that is associative but not commutative is *composition*.

In the respective branch of mathematics it is proven that for any three single-variable real-to-real appropriately defined functions $f(x), g(x)$ and $h(x)$ it is the case that:

$$(f \circ g) \circ h = f \circ (g \circ h)$$

As a concrete example, let the following functions:

$$f(x) = \frac{1}{x},\ g(x) = \sin x,\ h(x) = x^2$$

be defined over their natural domains.

Then, if we first compose the functions g and f, we shall have as per **Definition 9.1**:

$$f \circ g = \frac{1}{\sin x}$$

and by composing $h(x)$ with the above result we arrive at:

$$(f \circ g) \circ h = \frac{1}{\sin\left(x^2\right)}$$

If we, next, compose the functions h and g first, then, as per the same Definition 9.1, we shall have:

$$g \circ h = \sin\left(x^2\right)$$

and by composing the last result with $f(x)$ we will arrive at:

$$f \circ (g \circ h) = \frac{1}{\sin\left(x^2\right)}$$

the same result.

However, the composition of two functions, say, the function f and the function g in this example, is, in general, *not* commutative.

Indeed.

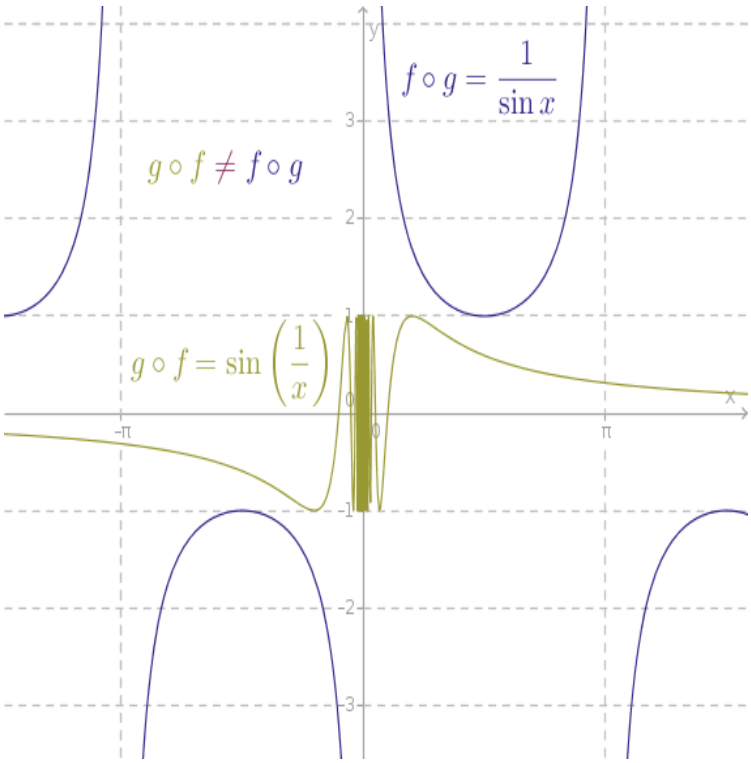
We already know the shape of the composition $f \circ g$:

$$f \circ g = \frac{1}{\sin x}$$

and we see that the composition $g \circ f$:

$$g \circ f = \sin\left(\frac{1}{x}\right)$$

is a totally different function (Figure 9.1):



In the *doing-the-grown-up-mathematics-the-grown-up-way* spirit of this space, our readers are encouraged to generate more such examples on their own.

As a highly advanced example, the binary operation of multiplication defined on the set of numbers known as *quaternions* is also associative but is not commutative.

Not Associative But Commutative

Let us define the following operation over the set of positive integers:

$$a \circ b \equiv a \cdot b + 1$$

where the symbols $\cdot$ and $+$ stand for the traditional multiplication and addition of integers respectively.

Is such an operation binary?

It surely is - prove it on your own.

Then, clearly, such an operation *is* commutative because for any two positive integers a and b it is the case that $a\cdot = b \cdot a$ and, hence:

$$a \circ b = a \cdot b + 1 = b \cdot a + 1 = b \circ a$$

However. In general, such an operation is *not* associative. Let a, b, c be any three positive integers. Then, on the one hand, we have it that:

$$(a \circ b) \circ c = (ab + 1)c + 1 = abc + c + 1$$

and, on the other hand, we have it that:

$$a \circ (b \circ c) = a(bc + 1) + 1 = abc + a + 1$$

Thus, as long as $a \neq c$, it is not the case that the equality:

$$(a \circ b) \circ c = a \circ (b \circ c)$$

holds for any three positive integers a, b, c.

As another example of a binary operation that is not associative but is commutative consider the absolute value of the difference of two real numbers a and b:

$$a \circ b \equiv |a - b|$$

Such an unsigned difference of any two real numbers is a real number. Hence, the said operation is binary.

Clearly, for any two real numbers a and b we have:

$$a \circ b = |a - b| = |b - a| = b \circ a$$

Therefore, such an operation *is* commutative.

However, for any three real numbers a, b, c we have:

$$(a \circ b) \circ c = ||a - b| - c|$$

while:

$$a \circ (b \circ c) = |a - |b - c||$$

and it is very straightforward to choose three real numbers for which it is not the case that:

$$||a-b|-c| = |a-|b-c||$$

Consider $a = 1, b = 2$ and $c = 3$:

$$||1-2|-3| = 2 \neq 0 = |1-|2-3||$$

which shows that the said $|a-b|$ operation is not associative.

Returning to **Definition 11** in general and its workhorse symbolic embodiment:

$$(a \circ b) \circ c = a \circ (b \circ c)$$

in particular, what does such an expression really say and how should we interpret it?

On the one hand, we know that the operation $\circ$ is binary and, therefore and by definition, for any *two* elements a, b of the underlying set G the expression $a \circ b$ is just an alternative name for a certain element, let us name that element x, that also belongs to the same set G:

$$a \circ b = x \in G$$

In other words, in a properly established context the expression $a \circ b$ is always well-defined and there can never be any confusion about its meaning, which we just described.

Likewise, the expression $b \circ c$ also names a certain element of G, let us name that element y, for any two elements b and c of G:

$$b \circ c = y \in G$$

We, thus, see that the relationship in (**1**) actually insists or requires that:

$$x \circ c = a \circ y \tag{3}$$

if the operation $\circ$ wants be *associative*.

In other words, the expression (**3**) involves only *two* elements per one side of the equal sign and not *three* elements per side as we have it in (**1**).

For example, in the additive group of integers we have:

$$(2+3)+5 = 2+(3+5)$$

and, by the above logic, the expression $2 \circ 3 = 2 + 3$ corresponds to the particular element, the element 5, of $\mathbb{Z}$ and the expression $3 \circ 5 = 3 + 5$ corresponds to the particular element, the element 8, of $\mathbb{Z}$ and:

$$5 + 5 = 10 = 2 + 8$$

implying that in this case it is possible to attach a unique and a non ambiguous meaning to the expression at hand:

$$(2 + 3) + 5 = 2 + (3 + 5) = 2 + 3 + 5 = 10$$

in particular and to all such expressions over the set of integers in general.

We, thus, see that the binary operation of addition on the set of integers *is* associative.

However, can we say the same about the binary operation of division defined on the set of positive rational numbers?

Let us see. Can we attach a unique and a non ambiguous meaning to, say, the following expression:

$$\frac{2}{3} \div 2 \div \frac{4}{3}$$

?

Well, the intermediate expression $2/3 \div 2$ names the positive rational number $1/3$, while the intermediate expression $2 \div 4/3$ names the positive rational number $3/2$ and clearly:

$$\frac{1}{3} \div \frac{4}{3} = \frac{1}{4} \neq \frac{4}{9} = \frac{2}{3} \div \frac{3}{2}$$

Thus, it is not at all clear which particular value should we attach to the above expression: should it be $1/4$ or should it be $4/9$? Regardless of the choice that can be made here, the next question is: *why* would we choose once rational number over another?

The binary operation of division on the set of positive rational numbers, therefore, is *not* associative.

In general, if the binary operation $\circ$ is not associative then the element $x \circ c$ is distinct from the element $a \circ y$ and for such operations it is impossible to assign a unique meaning to the expression $a \circ b \circ c$. Such an impossibility, in turn, invites ambiguity and ambiguity in mathematics is an unwanted guest.

For a slightly different angle, the property of associativity of a binary operation on a set reveals how the shifting allegiance of the monkey in the middle affects the result of two consecutive operations.

So far we were anchoring our discussion of the associativity of binary operations to the order of the said *operations*. But it is also possible to switch gears somewhat and anchor such a discussion to *the binding of the middle operand* or the middle *argument* in a string of two consecutive actions.

In our lingo the role of the monkey in the middle is played by the element named b (Figure 9.2):

For the binary operations that *are* associative the result of the above expression will be the same if we *bind* or *combine* the middle operand b with its *left* operation first or if we *bind* or *combine* the middle operand b with its *right* operation first for all the respective elements a, b and c.

For the binary operations that are *not* associative the result of the above expression will be different depending on whose side the middle operand b picks first.

Beyond the immediate tactical manipulations of just three elements of a given set by a given binary operation, however, there lies a much, much deeper phenomenon.

Namely.

On the other hand, the workhorse symbolic embodiment:

$$(a \circ b) \circ c = a \circ (b \circ c)$$

of the **Definition 11** can be interpreted as *a definition* of the generic product of *three* elements that plays an absolutely fundamental role not only in the theory of groups but in the rest of the modern grown-up abstract algebra.

What does the phrase *"the product of three elements"* mean?

The phrase *"the product of three elements"* is simply a concise equivalent version of the following phrase:

two consecutive applications of the binary operation $\circ$ *to three elements* a, b, c *of a set over which the said operation* $\circ$ *is defined*

where group theorists borrow the concept of *integer* multiplication and import it into the theory of groups, as we already explained in the **Difficult, Giant, Leap Forward** chapter.

By now we only begin comprehending and grasping the awesome power of the theory of groups which weaves its magic in a highly abstract universe in which any suitable operation can hide behind the generic symbol $\circ$ and any suitable object can hide behind the symbol a, or b, or c.

In our early examples of groups we saw that the light switch flips, tire rotations, contra dance figures, congruence motions of a non-square rectangle or of a square and the good old integers can hide behind the symbols a, b, c and that *a composition* of the respective entities or *the addition* of integers can hide behind the generic symbol $\circ$.

From now, then, it should be understood that whenever we say *a generic product of so many elements* then we actually mean *a consecutive application of the operation* $\circ$ t*o so many elements*, regardless of the true underlying nature of the operation $\circ$ and since earlier we agreed to replace the symbol $\circ$ with the symbol $\cdot$, which may be omitted, it *may* so happen that the elements of a set are integers and that the operation at hand is multiplication but it may not be just as well.

Recall that in **Definition 10** of a binary operation $\circ$ we demanded that, among the other requirements, such an operation must act on exactly *two* elements - no more and no less.

Thus, as we already noted, the meaning of a generic product $a \circ b = a \cdot b = ab$ of *two* elements or the meaning of the application of a given binary operation $\circ$ to its two constituents a and b is well-understood and well-defined, as, by its very definition, it is simply a particular element from the same underlying set.

Sitting at the very root of the inductive process, such a meaning can be interpreted as *a definition of a 2-element product*.

Note how we gradually begin getting accustomed to the grown-up mathematical terminology - we should now understand all the depth of the phrase *a 2-element product*.

In that light, the parenthesis around a stand-alone 2-element product are redundant and can be omitted without ill effects:

$$(ab) = ab = x$$

where, as we now fully understand, the invisible symbol $\cdot$, which seals the happy marriage of the elements a and b and which is also the symbol $\circ$, is there all along and it designates a generic binary operation.

However, it is still not at all obvious how are we to generically multiply *three* (or more) elements together or how do we obtain a non-ambiguous and a particular result of *two* consecutive applications of the same binary operation $\circ$ to its three elements a, b, c:

$$a \circ b \circ c = ?$$

In vacuum, which is our starting point, such a generic product of *three* elements is not even defined!

Ah.

This is exactly where the relationship in (**1**) comes in because such a rule actually *defines* the result of the generic product of *three* elements or, to be more precise, such a rule defines how the parentheses in a generic product of *three* elements can be eliminated in a non ambiguous fashion.

That is, the associativity rule in (**1**) tells us that when, on the one hand, we multiply the element a by the element $b \circ c$ and when, on the other hand, we multiply the element $a \circ b$ by the element c then as a result of such a multiplication we obtain *one and the same element*.

It is *that same element*, which is the result of the generic product of a and $b \circ c$ and which is the result of the generic product of $a \circ b$ and c, that is natural to assign to the result of the generic product of the elements a, b, c, in that particular order, and simply designate it as follows:

$$(a \circ b) \circ c = a \circ (b \circ c) = a \circ b \circ c$$

Because the younger students of mathematics are very good at finding some amusing ways to confuse themselves in the situations that warrant no confusion, we would like to iterate one more time that in all of the above purely associative manipulations the order of the operands a, b, c remains fixed at all times - to be harsh and blunt for pedagogical purposes, in such purely associative manipulations, in vacuum, we are not even allowed to change the order of the a, b, c constituents.

Now, before we deep dive into even more symbolic shuffling, we recall that we already agreed that the generic and abstract symbol $\circ$ can be replaced with the multiplication symbol $\cdot$ which, in turn, can be omitted altogether:

$$a \circ b \circ c = a \cdot b \cdot c = abc$$

As such, the above definition of the generic product of three elements tells us that:

$$(ab)c = a(bc) = abc \tag{4}$$

That is, the above equality should be interpreted as *a definition* abc of the product of three elements a, b, c.

Great.

But now we realize that the saga that starts with *two* elements and is now defined for *three* elements can be unambiguously extended into the saga of four elements a, b, c, d as in $a(bcd)$, for example.

Let us show that along the way it must be the case that:

$$a(bcd) = (ab)(cd) = (abc)d \tag{5}$$

In other words, we are about to show that a product of four elements a, b, c, d, whose relative order remains fixed at all times, can be partitioned with the order of evaluation modifiers $()$ any which legal way *without affecting the result*.

First of all, by the definition in (**4**), for the *three* elements b, c, d we have:

$$bcd = b(cd)$$

Therefore, the LHS of (**5**) can be manipulated as follows:

$$a(bcd) = a[b(cd)] \tag{6}$$

where we used the square *parentheses* $[]$ in order to make the work easier on our eyes but these square parenthesis are the same traditional parenthesis $()$ that are shown on the LHS of (**6**) - that is all that there is to it.

Now, on the RHS of (**6**) we, again, have *three* (!) elements named a, b and cd (explain *why* on your own).

But to such *three* elements a, b and cd we can apply the definition (**4**):

$$a[b(cd)] = (ab)(cd)$$

If the above transition is still confusing then simply designate the element named cd as x: $cd = x$. Then the expression shown on the RHS of (**6**) becomes $a(bx)$. But according to the very first transition in (**4**), we have: $a(bx) = (ab)x$. Now unwind the element x into what it actually is: $(ab)x = (ab)(cd)$.

Floss. Rinse. Repeat.

For, again, *three* elements named ab, c and d we also have:

$$(ab)(cd) = [(ab)c]d$$

Here put $ab = x$ and, using (**4**), obtain: $x(cd) = (xc)d$.

For, again, *three* elements named a, b and c we have, as per (**4**), $(ab)c = abc$ and, hence:

$$[(ab)c]d = (abc)d$$

Putting the sequence of the above intermediate results together, we find that indeed:

$$a(bcd) = a[b(cd)] = (ab)(cd) = [(ab)c]d = (abc)d$$

which is to say that:

$$a(bcd) = (ab)(cd) = (abc)d$$

which is what we set out to show in the first place. □

Since even in the above tiny deduction a great deal of technical things are going on, let us highlight some of them.

I. From a purely tactical standpoint, notice that while chewing on the meaning of a 4-element product, we operated solely in terms of 3-element products. Right? And the definition of a 3-element product was centered around only a 2-element product. What does that smell like already? Correct - it smells like an induction is in the works.

II. From a much broader, strategical, standpoint what just transpired is the following: in the **Prerequisites** chapter we observed that by switching from naked numbers to their symbolic representation we gained the ability to significantly increase the scope of application of abstract symbols manipulation to the entities that are not naked numbers - forces and vectors in physics, for example.

We also observed that such symbolic manipulations are very mechanical since they remain blissfully unaware of the underlying nature of exactly what the abstract symbols at hand represent.

Here and now, in the theory of groups, we can witness a very similar phenomenon:

- we borrowed the concrete operation of *multiplication* as it applies to *numbers*
- we repurposed that operation to be highly abstract and then
- we applied it to entities that may or may not be numbers at all

Thus, the respective symbolic manipulations that we just carried out above, on the one hand, follow the familiar rules of multiplication of numbers but, on the other hand, may be equally well applied in the contexts that are wildly different from the numerical ones and are still mechanical because they remain blissfully unaware of the underlying nature of the actual operation and the actual entities that are shuffled around.

III. Shifting back to a much narrower tactical analysis, we urge our readers to spend as much time on the above miniature deduction as it is needed in order to understand why its every transition was made and why such every transition made was legal.

Moreover, the readers who are new to the concept of constructing mathematical proofs should initially always answer the following question for each new proof that they come across:

which primitive notions, axioms, definitions and previously established results did this deduction rely on?

In this particular case we relied on:

- the definition of a binary operation, according to which a 2-element product is always defined and is equal to an element from the same set and
- the definition of a 3-element product in (**4**)

Based on the definitions of a 2-element and a 3-element product, such a deduction, thus, can now be taken to *define* a generic 4-element product as follows:

$$a(bcd) = abcd \tag{7}$$

Using the same tactical reasoning of operating only in terms of 4-element, 3-element and 2-element products, we can, next, define a generic 5-element product:

$$a(bcde) = abcde \tag{8}$$

and a 6-element product:

$$a(bcdef) = abcdef \tag{9}$$

and so on.

Assuming that the product of any $(n-1)$ elements is already defined, we define the product of any n elements as follows:

$$a_1(a_2 \cdot \ldots \cdot a_n) = a_1 \cdot \ldots \cdot a_n \tag{10}$$

for a suitable positive natural number n.

As such, we can now take it that an inductive definition of the expression $a_1 \cdot \ldots \cdot a_n$ is given and valid and we can prove our first and a very important

Theorem 1: let $\circ$ be an associative binary operation defined on a set G and let n be any positive natural number. Then, for any positive natural number m such that $m \leqslant n$ the following relationship for the elements, a, of G holds:

$$(a_1 \circ \ldots \circ a_m) \circ (a_{m+1} \circ \ldots \circ a_n) = a_1 \circ \ldots \circ a_n \tag{11}$$

Proof: as we agreed earlier, in (**11**) the symbol for the binary operation $\circ$ can be safely omitted altogether:

$$(a_1 \ldots a_m)(a_{m+1} \ldots a_n) = a_1 \ldots a_n \tag{12}$$

and our plan of attack is to construct a proof by induction on n and m.

If $n = 1$ then (**11**) and (**12**) degenerate into an identity:

$$a_1 = a_1$$

We now assume that (**11**) and (**12**) hold if $n \leqslant k - 1$ for a suitable positive natural number k:

$$(a_1 \dots a_m)(a_{m+1} \dots a_{k-1}) = a_1 \dots a_{k-1}$$

Next, we need to show that (**11**) and (**12**) hold when $n = k$.

To that end, we consider the case when $m = 1$.

But then the relationship in (**12**) becomes:

$$a_1(a_2 \dots a_k) = a_1 \dots a_k$$

which is *a definition* of the expression $a_1 \dots a_k$ as it is shown in (**10**) and, hence, is valid.

Thus, for a given $n = k$ and $m = 1$ the relationship (**12**) holds.

Fixing $n = k$, assume that the relationship in (**12**) holds if $m = q - 1$ for a suitable positive natural number q:

$$(a_1 \dots a_{q-1})(a_q \dots a_k) = a_1 \dots a_k$$

We, then, want to show that the relationship in (**12**) holds if $m = q$.

To that end, because when $m = n$ the relationship in (**12**) holds:

$$(a_1 \circ \dots \circ a_n) = a_1 \circ \dots \circ a_n$$

we assume that $q < k$ since this is the only other case when partitioning a product of a, finite, number of elements with parentheses has a meaning.

As such, because we assumed that the given premise holds if $n \leqslant k - 1$, then:

$$(a_1 \dots a_q)(a_{q+1} \dots a_k) = [(a_1 \dots a_{q-1})a_q](a_{q+1} \dots a_k)$$

where we simply spelled out the definition of the expression $a_1 \dots a_q$:

$$a_1 \dots a_q = (a_1 \dots a_{q-1})a_q$$

But because the binary operation at hand $\circ$ is *associative*, for the three elements of the underlying set G named:

- $(a_1 \ldots a_{q-1})$ (make it x)
- a_q (make it y) and
- $(a_{q+1} \ldots a_k)$ (make it z)

we have $(xy)z = x(yz)$:

$$[(a_1 \ldots a_{q-1})a_q](a_{q+1} \ldots a_k) = (a_1 \ldots a_{q-1})[a_q(a_{q+1} \ldots a_k)]$$

and the above rightmost expression in square brackets:

$$[a_q(a_{q+1} \ldots a_k)]$$

is, by definition, equal to $a_q a_{q+1} \ldots a_k$ and we, thus, have:

$$(a_1 \ldots a_q)(a_{q+1} \ldots a_k) = (a_1 \ldots a_{q-1})(a_q \ldots a_k) \tag{13}$$

Hence, because we assumed that the relationship in (**12**) holds if $n = k$ and $m = q - 1$, the RHS of (**13**) is simply $a_1 \ldots a_k$.

From where it follows that:

$$(a_1 \ldots a_q)(a_{q+1} \ldots a_k) = a_1 \ldots a_k$$

which completes the proof. □

The above, very important, theorem tells us, loosely, that if a binary associative operation defined on a certain set glues together a finite number of elements of that set then such a string of consecutive operations can be partitioned with parentheses as shown in (**11**) and (**12**) in any which legal way and that these parentheses can be removed without ill effects.

In our next technical discussion of the group axioms **Theorem 1** will effortlessly become **Theorem 2** embedded into the context of an official and rigorous axiomatic definition of a group.

In that particular context the formulaic relationship shown in (**11**) can be interpreted as *the first* rule of the removal of the parentheses in group products.

A bit later but soon after we will also prove that the inverse of a finite product of n group elements is equal to the product of the n inverses of the individual factors taken in the order that is *reverse* with respect to the original:

$$c\,(a_1 \cdot a_2 \cdot \ldots \cdot a_n)^{-1} = c a_n^{-1} \cdot \ldots \cdot a_2^{-1} \cdot a_1^{-1}$$

Such a formulaic relationship can be interpreted as *the second* rule of the removal of the parentheses in group products.

As we already observed prior, in the traditional textbooks on the subject many gaps in the exposition are not explicitly filled in and many fine points of the respective ideas are not explicitly spelled out because it is assumed that the students are mathematically mature enough to fill those gaps and nail these fine points *on their own*.

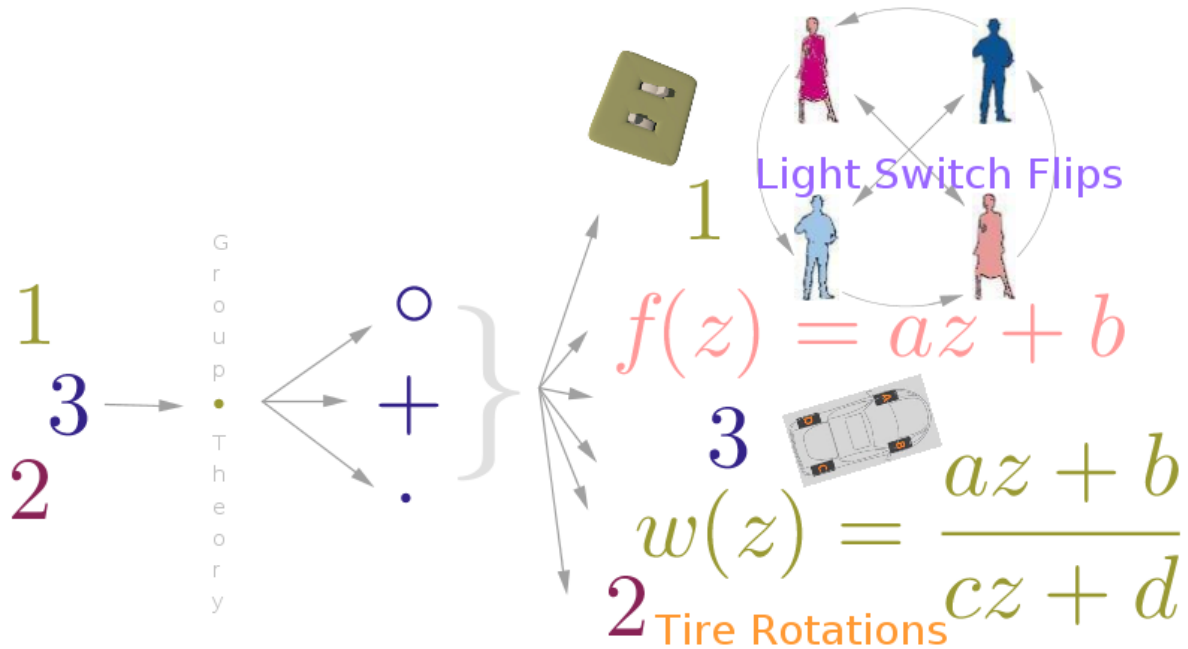
In this text, however, we make an attempt to fill the potential gaps in and highlight the important fine points explicitly. As such, do realize that we already reached the stage in our exposition that convincingly demonstrates the awesome power of abstract symbolism. Namely.

So far, we *borrowed* and *imported* the operation of multiplication of numbers. Strategically, we *repurposed* that operation in a highly abstract manner because now we claim that such a multiplication represents *any* good old binary operation as it acts on *any* good old operands or elements. Tactically we still *applied* or *used* that operation of multiplication *as if* it acts on numbers.

However.

The result of such tactical multiplicative symbolic manipulations *is still valid* even when the underlying binary operation is not multiplication and when the underlying operands or elements are not integers!

Pictorially (Figure 9.3):



As we wade into the group-theoretic waters deeper and deeper, the symbolic manipulations will get more and more abstract and the discipline-specific terminology will get more and more specialized and terse.

We hope, however, that the readers who feel that they are lost in the stormy ocean of abstract symbolism here and there and now and then will be able to reach for the flotation devices that we constructed in the early examples of groups and fall back on something tangible.