# Chapter 10

# Group Axioms

In the five early, introductory, examples of groups the respective groups themselves were not really *defined* rigorously but were rather *described* loosely and the diligent students of mathematics have already spent a good amount of ink and paper working on the relevant and thought-provoking exercises.

There was a method to the madness. On the one hand, using the material that does not require a long and dedicated mathematical training, we wanted to involve the readers into *doing* the group-theoretic work right away because doing mathematics is learning mathematics.

By working with the concrete and, perhaps, tangible, in some sense, examples of groups and by thinking about the specific details of that work we develop an intuitive feel for the texture of the fabric from which the given discipline is stitched.

On the other hand, in parallel, we wanted to demonstrate how the phenomenon of abstract symbolism emerges gradually and naturally in the course of the above work.

Namely, the concrete and specific examples of groups are supposed to also be the fodder for the inevitable transition to and the comprehension of the looming abstract narrative.

We specifically did not want to hit our readers with a perfect squall of abstract symbolism on day one because doing so in this text serves no purpose at best and is downright harmful at worst.

However, after a reasonable amount of preparatory work, sooner or later, there must come the time when the kiddie gloves are taken off.

Now is that time. Starting with this discussion we will be switching the style of our exposition toward more formal, more rigorous and more grown-up.

## Axiomatic Systems

As such, we observe right away that the upcoming axiomatic definitions of a group is just one of several ways of defining what a group is.

Eventually we will learn that a group can also be defined via a construct known as *a multiplication table*, which we already met informally, via a construct known as *a graph of a group* and via the so-called *generators and relations* to name a few but not all possible ways to define a mathematical group.

However, as we shall discover momentarily, in the realm of axiomatic definitions of a group alone there is a fair amount of interesting, relevant and technically worthy variation of its own.

Axioms in general, in so many words of a crash course, are small, in some sense, and simple, in some sense, statements that are taken to be true without proof.

Combined with the primitive notions, that are not defined, relevant definitions and the rules of inference, axioms form the foundation of a given, vaguely defined, mathematical discipline from which the hierarchy of theorems is then developed.

Multiple distinct collections or sets of axioms may delineate a given, vaguely defined, mathematical discipline.

For example, there exist several axiomatizations of what we refer to as the *Euclidean geometry*:

- the Euclid's five postulates, which are considered to be too lax by the modern standards or rigor
- the Tarski's axioms
- the Birkhoff's axioms and
- the Hilbert's axioms

of geometry to name a few.

Such a collection of axioms that pertains to a given, vaguely defined, discipline is commonly referred to as *an axiomatic system*, which itself has a number of properties - an axiomatic system can be *complete*, *minimal* and so on.

Across two axiomatic systems A and B, an axiom in the system A may be a theorem in the system B and conversely, and an axiom in a system B may be a theorem in the system A and conversely.

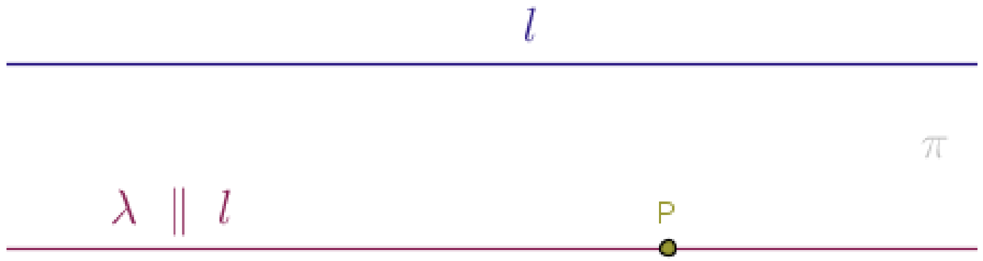
In addition to developing the actual corpus of knowledge of a vaguely defined mathematical discipline, the purpose of the axioms is to:

- explicitly spell out the boundaries of the applicability of the said corpus and of the relevant apparatus
- ensure that all the participants speak the same language and operate with the same entities, which, in turn, facilitates the communication between the participants from different countries and ensures the consistency of the respective results
- deduce the neither obvious nor intuitive but true facts that are completely detached from time and from human *opinions* and *emotions*

In order to elaborate on the last point above, it should be understood well that the perceived *trueness* of the *true mathematical facts* is *bounded to this specific set of axioms*.

For example, it may seem that given a straight line $l$ and a point $P$ distinct from $l$ there can ever be *one and only one* other coplanar straight line, name that other coplanar straight line $\lambda$, that will satisfy the following three requirements at once:

- the straight line $\lambda$ must be in the plane $\pi$ defined by $l$ and $P$
- the straight line $\lambda$ must pass through the point $P$
- the straight line $\lambda$ must be parallel to the straight line $l$ (Figure 10.1):



Right?

This observation just makes perfect sense that does not betray our everyday experience.

Well.

This observation is both right *and* wrong - and that is the heart of the matter.

We now know that nothing can prevent us from experimenting with the seemingly absurd idea that probes two other extremes of the above setup when there may be exactly zero $\lambda$-like straight lines or there may be infinitely many $\lambda$-like straight lines.

Indeed, in the early nineteenth century, overcoming the sad and myopic resistance of and the non-acceptance by the contemporaries, such mathematicians as J. Bolyai (1802–1860), Carl F. Gauss (1777–1855), N. Lobachevsky (1792–1856) and B. Riemann (1826 -1866) discovered that there exist perfectly *internally consistent*, or *also true* if you will, geometries if the above Euclid's fifth postulate is *complemented* with the above two cases:

- in the so-called *elliptic* geometry there are exactly *zero* $\lambda$-like straight lines that:
    - pass through the point $P$ and
    - are parallel to the given straight line $l$ and
- in the so-called *hyperbolic* geometry there are *infinitely many* $\lambda$-like straight lines that:
    - pass through the point $P$ and
    - are parallel to the given straight line $l$

and what we refer to as the *Euclidean* geometry, then, should really be called the *parabolic* geometry.

Moreover, the elliptic, hyperbolic and Euclidean geometries not only do not contradict each other, but it was later discovered by the early twentieth century theoretical physicists and mathematicians that non-Euclidean geometries provide a more accurate *mathematical model* of the physical reality, which is a very deep and an absolutely fascinating subject in its own right.

However, we cannot deep dive into it on a tangent, since we have to stay focused on the theory of groups.

From a purely technical perspective, then, *the correctness* of a set of axioms has a very precise and a very hard requirement: at its very minimum, all the axioms in a given set should be *independent of each other* and not a single axiom can *contradict* the remaining axioms.

In other words, from a technically sound set of axioms it should be impossible to derive both a statement and its negation and no single axiom of a given set should follow from the other axioms.

If an axiom does follow from the rest of the axioms then that axiom is not really an axiom and it should be unbuckled from the given set of axioms and branched out into *a theorem* with a corresponding proof.

From a purely philosophical perspective it makes no sense in contemplating *the correctness* of a given set of axioms inasmuch as it makes no sense in contemplating the correctness of the rules of the game of hockey or the correctness of the rules of the game of chess and *the validity* or *the correctness* of the chess pieces themselves, for that matter.

We should also not care at all about what *a knight* or *a bishop* in chess *are* - the only thing that should matter to us as the mathematicians is what a chess knight and a chess bishop can *do* and how these pieces of the game of chess *interact* with the other like pieces on the chessboard.

In general, a chess knight is *an idea* and so is a chess bishop.

The rules of hockey and the rules of chess are neither correct nor incorrect - they just are and they delineate a certain game.

It is perfectly fine to change the rules of a given game but then the result of such a change will be *a different* game.

Whether a proposed change leads to an interesting different game that others will be willing to participate in is a valid technical concern but is a different matter.

Lastly, there is this concept of *optimality* that can be attached to a given set of axioms.

That is.

On the one end of the optimality spectrum, if the axioms in a given set are too loose in quality and are, perhaps, too large in number then just about anything can be proven with these axioms and such a game is considered to be not interesting.

On the one end of the optimality spectrum, if the axioms in a given set are too restrictive in quality and are, perhaps, too few in number then just about nothing can be proven with these axioms beyond a trivial and mostly non-consequential fact and such a game is considered to be not interesting also.

Somewhere in between the above two extremes there is this fuzzy sweet spot, the proverbial Goldilocks Zone, in which the prohibitive quality of the axioms and their number are dialed in, in concert, just perfectly so that it is quite challenging and difficult but not impossible to generate the relevant proofs and not a single axiom can be taken away, as the discipline at hand will crumble like a house of cards, and not single independent and non-contradictory axiom can be added.

Having said that, there is no hard and fast requirement in the grown-up mathematics that such a perfectly balanced set of axioms is penned every time - intuitively speaking, there is *some* very, very technical leeway in the Goldilocks Zone.

Indeed.

In the upcoming five discussions of families of group-theoretic axioms we will explore the *heavy* or the *strong*, in some sense, set of group axioms and the *light* or the *weak*, in some sense, set of group axioms.

Namely.

In the direction from heavier and stronger toward lighter and weaker, in the **Take 1** discussion we will study, perhaps, the most demanding set of group axioms which bakes the uniqueness and the existence of the double-sided identity element and of the double-sided inverse elements of a group right in.

In the **Take 2** discussion we will loosen the screws a bit by considering a set of group axioms in which the above uniqueness of the identity element and of the inverse elements is *not* demanded but the existence of a double-sided identity and of a double-sided inverse element of each element of a group is preserved.

However, as a formal, straightforward but important and fun, pair of exercises, our readers will then generate the relevant proofs of the two theorems that state that the identity element of a group and that the respective inverse elements of a group are, in fact, unique.

The mechanics of these proofs will dovetail or percolate into the set of the group axioms covered in the **Take 1** discussion.

Whether it is axiomatically demanded or proven that the inverse of a given group element is unique, does not really matter much at this point - either way, that uniqueness of the inverse of a group element $a$ gives us the ability to introduce a standard and a non-ambiguous designation of such an element as $a^{-1}$.

Such a notation for an inverse element of a given element of a group is consistent with the manipulative mechanics of the integral powers in the arithmetic of exponentiation of *numbers*:

$$a^{-1} \cdot a^{1} = a^{-1+1} = a^{0} = 1 = e$$

and, say:

$$a^{-1} \cdot a^{-1} \cdot a^{-1} = a^{-1+(-1)+(-1)} = a^{-1 \cdot 3} = a^{-3}$$

and so on.

Here, the symbol $e$ is, of course, *not* the popular transcendental *number*, but, rather, is a short-hand notation for *the identity element of a group*, since such an element is unique thanks to either the gift of the respective axioms or a series of proofs that follow from the respective looser demands.

We walk away from the traditional middle and high school curricula knowing that for all natural numbers, integers, rational numbers, real numbers and complex numbers $a$ and $b$ it is the case that:

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

where this time by the symbol $\cdot$ above we mean the good old multiplication of *numbers* and not a group product.

Well.

It turns out that in the grown-up mathematics, such as Linear Algebra, for an example, there exist objects, such as *matrices*, for an example, for which the above commutative property does not hold in general.

As such, it is a common practice in grown-up mathematics to cast the net as wide as possible and not automatically assume that the above commutativity property applies to the matter at hand in a wholesale fashion.

Thus, in the **Take 3** discussion we will loosen the things down even more by explicitly splitting a uniform identity element of a group into *a left identity* $e_l$ and *a right identity* $e_r$ and by explicitly splitting a uniform inverse element into *a left inverse* $x_l$ and a *right inverse* $x_r$ of a given element of a group.

Specifically, in the **Take 3** group axioms we will only demand that in a proposed set $G$ *at least one* right identity element $e_r$ exists and that *at least one* right inverse element $x_r$ of a given group element exists, for all the elements of the proposed set.

The weakening of the requirements baked into that variance of the group axioms will come at the expense of more delicate proofs.

We will see that the above splitting maneuver is entirely possible and that in one set of group axioms it is sufficient to simply demand only the existence of a right identity and of a right inverse for each element of a group.

However, as an exercise, we shall prove that these *lightened* group axioms still have plenty of juice in the tank in order to prove that under these axioms a right identity of a group is also a left identity of that group and that a right inverse of a given element of a group is also a left inverse of the same element of that group.

In other words, we shall show that even under the **right**-weakened system of axioms a right identity of a group and a left identity of a group are actually one and the same element $e = e_r = e_l$$ which is still *an* identity element of a group and not *the* identity element of a group, and we shall also show that a right inverse of a given element and a left inverse of the same element of a group are actually one and the same element $x = x_r = x_l$, which is still *an* inverse and not *the* inverse.

We will then prove the uniqueness of both the identity element of a group and of the respective inverse elements.

Such a proof will, again, dovetail into the set of group axioms discussed in **Take 1**.

In the **Take 4** discussion we will take a look at a **left**-only twin set of the group axioms that demands only the existence of *at least one left identity* and of *at least one left inverse* for each element of a group.

Likewise, we shall *prove* that these *lightened* or *weakened* group axioms still have plenty of juice in the tank in order to prove that under these axioms a left identity of a group is also a right identity of that group and that a left inverse of a given element of a group is also a right inverse of the same element of a group.

In other words, we shall show that even under the **left**-weakened system of axioms a left identity of a group and a right identity of a group are actually one and the same element $e = e_l = e_r$, which is still *an* identity element of a group and not *the* identity element of a group, and we shall also show that a left inverse of a given element and a right inverse of the same element of a group are actually one and the same element $x = x_l = x_r$, which is still *an* inverse and not *the* inverse.

We will then prove the uniqueness of both the identity element of a group and of the respective inverse elements.

Such a proof will, again, dovetail into the set of group axioms discussed in **Take 1**.

In the **Take 5** discussion, for completeness, we shall consider the single, so-called *unrestricted group division*, axiom that can replace the two, traditional by now, existence of the identity and of the inverse elements axioms.

Technically, in the **Take 5** discussion we will present only *two* group axioms - the axiom of the associativity of the proposed binary operation and the axiom of the unrestricted group division.

Each Take $n > 1$ chapter is a complete and a stand-alone unit of the group-theoretic knowledge that starts with the relevant, weaker, axioms and runs them up, via a set of the respective theorems, to the doorstep of the **Take 1** group axioms.

Thus, by the end of the **Take 5** discussion we will understand why we see what we see in the modern textbooks on the subject - most such texts simply roll up and omit all of the above nuanced (and fun) work into a single set of (boring) group axioms and run with it.

## A Technical Look at The Base of The Mountain

So why bother?

Why bother with all these details when most modern textbooks on the subject flash the strongest group axioms discussed in **Take 1** at worst or the slightly weaker group axioms discussed in **Take 2** at best and then ask the students to throw together a one-liner for the proof of the uniqueness of the relevant elements of a group?

We bother with these technical details that swim in the primordial group-theoretic soup because we remember *why* are we reading this text and *why* are we working through the material presented in this text in the first place.

We do this not because we care about the grades - we do not.

We do this not because we care about the titles - we do not.

We do this not because we care about the money - we do not.

Now, it *may* so happen that by working through the material presented in this text, later in life, as a side effect of a proper attitude and approach to studying mathematics, you will get high grades, higher academic titles and you may come into some money or even some fame.

Things happen.

Best of luck and more power to you - if I, the author of this work, is still alive, drop me a note.

But *we* do this for the sole and share intellectual beauty of the idea and of the pursuit, we do this because we want to *know* and *understand* the subject matter (which is quite different from getting good grades), we do this purely for the sake of developing our overall mathematical culture, we do this just for the sake of the craft and we do this in order to participate in the development of abstract cognition in general.

As a bonus, from the early age we get to run with the grown-ups, since we get to see how the realistic mathematics is done.

Make no mistake, the material presented in this chapter *will be difficult*.

As such, it is entirely possible to read only the **Take 1** discussion and move on, skipping the rest of the group axiomatic variations.

However, doing so will result in the loss of some precious mathematical gemstones - starting with the **Take 2** discussion we will begin developing the care that goes into crafting the sound grown-up mathematical arguments, that, accidentally and as a side effect, *will* stand up to the scrutiny of a real-time face-to-face verbal examination.

To that end, we observe that in the first four discussions of this chapter we will present *three* popular group axioms and in the fifth discussion we will present just *two* group axioms.

But grown-up mathematics is not a sculpture that is frozen in ice once and for all - the grown-up mathematics breathes, lives a full life of its own, moves around and is being saturated with technical details of varying scope and caliber at all times.

The after-the-fact investigative work into the very foundation of the theory of groups was rather active well into the twentieth century - one of the most complete and conclusive such papers are due to the mathematicians Baer R. and Levi F. who analyzed the properties of optimality and minimalism of an axiomatic system which we touched upon briefly earlier:

*Abelsche Gruppen mit abzahlbaren Elementen, Dissertation, Leipzig, 1917*

In particular, Baer R. and Levi F. showed that what we actually have here technically is *seven* (!), yes, *seven group axioms*.

In order to motivate the later group axiomatic discussions, we will just *list*, but not dwell on, the seven group axioms due to Baer R. and Levi F. at the end of the **Take 1** discussion.

An alternative approach to the foundations of the theory of groups can be found in the papers by Lorenzen P:

*Ein Beitrag zur Gruppenaxiomatik, Math. Z. 49. (1944), 313—327*

A word of caution.

To the eager young minds who are interested in a deeper study of the foundations of the theory of groups right way and who, perhaps are in a great hurry to do so, at this point there is, unfortunately or not, there is only *one* sound algorithm to proceed - *skip* the technical study of the Baer R. and Levi F. axioms initially and revisit them some time later.

In addition to the, seemingly, theoretical-only interest in the various types of sets of group axioms, such variations have a purely practical application.

Namely.

As we already mentioned earlier, in the course of grown-up research in hard sciences there often arises a need to deterministically answer the following question:

*does this candidate set $S$ coupled with this candidate operation $\circ$ form a group?*

In certain situations it is very easy to answer such a question and in other situations answering such a question may be too daunting of a task.

It stands to reason, then, that it would be really nice to have *a smallest possible* number of or the *weakest* possible conditions, the verification of which would guarantee a deterministic answer to the above question.

Intuitively speaking, finding as low of an axiomatic barrier to entry as possible is a good thing.

Thus, the weaker the set of group axioms, the less work we have to do trawling the usual suspects through the sieve of the said axioms.

We will illustrate this idea in the **Take 5** discussion but in order for that illustration to, intellectually, *stick*, we have to crawl through all four takes first.

# 10.1 Take 1

## Existence, Uniqueness of Double-Sided Identity and Inverses Assumed

Let a set $G$, finite or otherwise, with a single binary operation $\circ$ defined on the elements of that set be given.

Suppose further that the said binary operation coupled with the said set in an order-insensitive fashion satisfies the following three axioms.

**Axiom 1** (Associativity): for any three elements $a, b, c$ of the set $G$ the following relationship holds:

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

**Axiom 2** (Identity Element): among the elements of the set $G$ there exists a unique element $e$, called *the identity element*, such that for any element $a$ of $G$ it is the case that:

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

**Axiom 3** (Inverse Elements): for every element $a$ of the set $G$ there exists a unique element $b$ of the same set $G$, called *the inverse element of the element* $a$, such that:

$$a \circ b = b \circ a = e \tag{3}$$

Note that in the **Axiom 3** we used the same identity element, $e$, that we carefully defined in the previous axiom, the **Axiom 2**.

As a technical aside, the construct *for any three elements* $a, b, c$ in the **Axiom 1** does not impose any additional or implied restrictions on the distinctness of the said elements.

In other words, the phrase *for any three elements* $a, b, c$ does not exclude the possibility that the three symbols $a, b, c$ actually denote *one and the same* element, or that these symbols denote three *truly distinct* elements or that these three symbols denote some other mix of elements where, say, the symbols $a, b$ denote *one and the same* element but the symbol $c$ denotes *a different* element and so on.

We briefly remind our readers that in real time the above *three* popular group axioms were not birthed by a single mathematician in one sitting in one day in their final instance.

Rather, it took a collective effort, smudged over about one hundred years, give or take, of a number of mathematicians for these axioms to, gradually, crystallize into a crisp textbook-ready shape shown above.

One of the reasons why we keep making such historical references is to show the younger audience that none of the successful grown-up definitions and axioms in mathematics are a manna from heaven - all such successes, and failures, are written by us, certain people.

**Definition 13:** the given set $G$ with the defined on it, single, binary operation $\circ$ that satisfies the above three axioms is called *a group* and the axioms themselves are called *the group axioms*.

The said binary operation, as we already know from **A Difficult, Giant, Leap Forward** chapter, is also called *the group multiplication* and (the result of) an individual such multiplication, as in $a \circ b = a \cdot b = ab$, is called *the group product*.

**Definition 14:** the elements of the above set $G$ are called *the group elements*.

**Definition 15:** a group is called *finite* if it is comprised of a finite number of elements; otherwise a group is called *infinite*.

All the first five sample groups that we studied officially so far are *finite*:

- the duplex light switch group
- the tire rotations group

- the group of rigid symmetries of a non-square rectangle
- the contra dance group and
- the group of rigid symmetries of a square

In contrast, the additive group of integers is *infinite*, as is sometimes reflected in its name.

**Definition 16:** the number of elements of a finite group is called *the order* of that group.

Thus, the order of the first three groups, that of the light switch group, that of the tire rotations group and that of the group of rigid symmetries of a non-square rectangle, is equal to $4$.

The order of the contra dance group and the order of the group of rigid symmetries of a square is equal to $8$.

Using the result of the **Exercise 5.1.1**, we can now state officially that:

*the number of group products of a finite group of order $n$ is equal to $n^2$*

In one of the upcoming exercises, the readers who are familiar with complex numbers, will already, and effortlessly, prove that:

*for any positive integer $n > 0$ a group of order $n$ exists!*

How cool is that?

(it can also be shown that for *infinite* groups a group of any *cardinality* exists. This is even more cool)

**Definition 17:** a group is called *commutative* if and only if *for each* pair of its elements $a$ and $b$ it is the case that:

$$a \circ b = b \circ a \tag{4}$$

In other words, a group is *commutative* if and only if every pair of its elements *commutes*.

Hence, *all* these groups that we have studied officially so far:

- the duplex light switch group
- the tire rotations group
- the group of rigid symmetries of a non-square rectangle and
- the additive group of integers

are *commutative* and some of these groups are finite, while some of these groups are infinite.

The group of rigid symmetries of a square and the contra dance group are *not* commutative.

A commutative group is also called *an Abelian group*, after the Norwegian mathematician Niels Henrik Abel (1802–1829) and we now understand the punch line of the joke:

- *What is purple and commutes? An Abelian grape.*

From this version of the group axioms we can right away deduce the following two *properties* of the identity element of a group:

- the identity element of a group is its own inverse and
- the identity element of a group does commute with every element of that group

and we can also deduce the following *property* of the inverse element of a given element of a group:

- every element of a group commutes with its inverse

Whether the remaining, non-identity, elements of a given group commute with each other or not in a wholesale fashion is, as per **Definition 17**, a different story.

We also see that **Theorem 1** can be ported directly into the context of a group because the premise of that theorem requires only that the binary operation at hand *is associative*.

But now, if we do have *a group* then we do have a defined on a certain set binary operation that *is* associative by the, associativity, **Axiom 1**.

As such, we now have on the books:

**Theorem 2:** let $n$ be any natural number greater than zero. Then, for any positive natural number $m$ such that $m \leqslant n$ the following relationship for the elements, $a$, of a group holds:

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

Tentatively, the above theorem can be thought of as *the first rule* of the removal of parentheses in group products.

*The second* such rule will address the group products that deal with the inverse elements of a group:

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

where we carefully note 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.

Closing the circle of the early examples, we state officially that the respective operations in all of these examples are *binary* and *associative* and that *the identity element* of the:

- duplex light switch group is the *no flips* element
- tire rotations group is the *no tire rotations* element
- group of rigid symmetries of a non-square rectangle is the *no motions* element
- contra dance group is the *no partners' swaps* element
- group of rigid symmetries of a square is the *no motions* element
- additive group of integers is the $0$ element

For any specifically named or chosen element $a$ of the following groups:

- the duplex light switch group
- the tire rotations group and
- the group of rigid symmetries of a rectangle

its inverse element is $a$ itself.

Put differently, every element of each of the respective three groups listed above is *its own inverse*.

Later on, in a separate exercise, we will prove that a group whose elements possess such a property *must* be commutative.

The inverse elements of the contra dance group and of the group of rigid symmetries of a square were generated by our readers and, in general, such inverses no longer share the universal property that the inverses of the above three groups have.

Formally, that is, in the contra dance group and in the group of rigid symmetries of a square there exists an element that is its own inverse - the dance figure number 3 in the contra dance group, *circle right twice* or *left and right through*, and the rigid congruence motion number 3 in the group of symmetries of a square, any rotation about the square's center from the infinite set
$B = \{\pi + 2\pi k,\ k = 0, \pm 1, \pm 2, \pm 3, \ldots\}$.

But in each of the above two groups there also exists an element that is *not* its own inverse - the dance figure number 2 in the contra dance group, *circle right once*, and the rigid congruence motion number 2 in the group of symmetries of a square, any rotation about the square's center from the infinite set
$A = \{\pi/2 + 2\pi k,\ k = 0, \pm 1, \pm 2, \pm 3, \ldots\}$.

Given an integer $k$ from the additive group of integers, its inverse is the element of the same underlying set $\mathbb{Z}$ named $(-k)$.

The uniqueness of the double-sided inverse element of a given group element $a$ gives us the ability to agree on an unambiguous designation of such an inverse with $a^{-1}$, which, further, paves the way for the following natural *definition*:

$$a^0 = e$$

where the symbol $e$ stands for the unique, and also double-sided, identity element of a group.

The above definition aligns well with our intuitive extension of the arithmetic of the exponentiation of *numbers*:

$$a^{-1} \cdot a^1 = a^{-1+1} = a^0 = 1$$

in which we further abstract and generalize the meaning of the numeric symbol 1 into the group-theoretic symbol $e$ that now stands for *the identity element of a group*, which itself is unique and double-sided.

As we mentioned this already, the above set of the group axioms is, in some vague sense, *the heaviest* or *the strongest* one because not only it assumes or demands both the existence and the uniqueness of the identity element and the existence and the uniqueness of the inverse elements for each element of a set under a single associative binary operation, but it also extends that assumption onto the **double**-sideness of these elements.

In other words, this particular variety of the group axioms assumes that the given set $G$ does possess such a unique element, $e$, the group multiplication of any element $a$ of $G$ by which from *either* (!) side, *left* or *right*, produces that original element $a$ nonetheless:

$$e \circ a = a \circ e = a$$

In the upcoming takes on the group axioms, however, we will see that it is possible to split such a uniform, double-sided, identity into a so-called *left identity* $e_l$ and a so-called *right identity* $e_r$, where the said left identity $e_l$ has the natural definition of:

$$e_l \circ a = a$$

and where the said right identity $e_r$ has the natural definition of:

$$a \circ e_r = a$$

for all the elements $a$ of the set under consideration.

We, thus, understand that in *this set* of the group axioms the above left identity $e_l$ and the above right identity $e_r$ are welded or glued together into a monolithic whole e:

$$e_l \circ a = a \circ e_r = a, \ e_l = e_r = e$$

Likewise, this particular variety of the group axioms assumes that for each element $a$ of the given set $G$ there exists such a unique element, $b$, of $G$ the group multiplication of that element $a$ by which from *either* (!) side, *left* or *right*, produces the defined earlier, unique, identity element $e$:

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

In the upcoming takes on the group axioms, however, we will see that it is also possible to split such a uniform, double-sided, inverse element into a so-called *left inverse* $b_l$ and a so-called *right inverse* $b_r$, where the said left inverse $b_l$ has the natural definition of:

$$b_l \circ a = e_l$$

and where the said right inverse $b_r$ has the natural definition of:

$$a \circ b_r = e_r$$

As more and more technical nuances pile up, we observe in passing that in the upcoming alternative sets of the group axioms we will not be assuming the uniqueness of the left and right identities and we will not be assuming the uniqueness of the left and right inverses. Thus, in the actual formulations of the said group axioms, out of the potential multitude of the identity elements we will have to settle on this specific one:

$$b_l \circ a = e_{l0} \quad \text{or} \quad a \circ b_r = e_{r0}$$

and so on.

In any case, we now understand that in *this set* of the group axioms the left $b_l$ and the right $b_r$ inverses of a given element of a group are welded or glued together into a monolithic whole $b$:

$$b_l \circ a = a \circ b_r = e = e_l = e_r, \; b_l = b_r = b$$

In order to approach such delicate group-theoretic details gradually, we will pace ourselves and we will take these things slowly, developing the ideas that go into the respective proofs one small step a time.

Namely.

In the next discussion we will see that it is possible to remove the uniqueness of the identity element of a group and the uniqueness of the inverse elements requirement from the above set of the group axioms.

In other words, in the next set of the group axioms we will see that when a proposed set and a proposed single (associative, of course) binary operation defined on that set decide to hang together for the group formation purposes, it is sufficient to assume *only the existence*, and not the uniqueness, of *an* identity element of a set and of *an* inverse element for each element of the proposed set.

Even after such a removal of the respective uniqueness requirements, the left over axioms will still have enough juice in the tank in order to prove that the uniqueness of the corresponding elements must necessarily follow from them nonetheless.

## Advanced and Optional

In order to motivate the upcoming technical discussions of the various sets of group axioms, below we list without any further discussions and proofs, the seven group axioms as per Baer R. and Levi F.

Assume that we are given a set $G$ whose certain ordered triplets of elements $a, b, c$ honor the following relationship:

$$a = bc \tag{5}$$

in which $\circ$, not shown, is the respective *operation* and:

- $a$ is *the product of* $b$ by $c$
- $b$ is *the left quotient of the elements* $a$ and $c$
- $c$ is *the right quotient of the elements* $a$ and $b$

The set $G$ with the respective operation defined on it is *a group* if the following seven conditions (on the elements of $G$ and the implied operation $\circ$, of course) are satisfied.

$E_a$. For the given elements $b$ and $c$ there exists at least one element $a$ such that (**5**) holds.

E_b. For the given elements $a$ and $c$ there exists at least one element $b$ such that (**5**) holds.

E_c. For the given elements $a$ and $b$ there exists at least one element $c$ such that (**5**) holds.

U_a. For the given elements $b$ and $c$ there exists no more than one element $a$ such that (**5**) holds.

U_b. For the given elements $a$ and $c$ there exists no more than one element $b$ such that (**5**) holds.

U_c. For the given elements $a$ and $b$ there exists no more than one element $c$ such that (**5**) holds.

$A$. If in $G$ there exist the elements of the shape $(a_1a_2)a_3$ and the elements of the shape $a_1(a_2a_3)$ then both such products define one and the same set of elements.

Do note the following technical wrinkle in the above Baer/Levi axiom of associativity $A$: it does not contain any *statements* of existence or uniqueness and it allows for a situation when one of the products $(a_1a_2)a_3, a_1(a_2a_3)$ is defined in $G$, while the other is not.

# 10.2 Take 2

## Only the Existence of Double-Sided Identity and Inverses Assumed

In this version of the group axioms we will remove *the uniqueness* requirements on the identity element and on the inverse elements of a group but we will leave the demand for the existence of a **double**-sided identity and of a **double**-sided inverse element of each element of a group intact.

As an exercise, our readers will be invited to *prove* that the uniqueness of the said, double-sided, elements of a group necessarily follows from the upcoming set of group axioms nonetheless.

Before we jump into the proofs proper, however, let us agree that for the sake of brevity, instead of the phrase

*an inverse element of each element of a group*

we will use the following shortcut:

*the inverses of a group*

that should be understood as the equivalent of its lengthy and descriptive parent.

Let a set $G$, finite or otherwise, with a single binary operation $\circ$ defined on the elements of that set be given.

Suppose further that the said binary operation coupled with the said set in an order-insensitive fashion satisfies the following three axioms.

**Axiom 1** (Associativity): for any three elements $a, b, c$ of the set $G$ the following relationship holds:

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

**Axiom 2** (Identity Element): among the elements of the set $G$ there exists a particular element $e$, called *an identity element*, such that for any element $a$ of $G$ it is the case that:

$$a \circ e = e \circ a = a$$

**Axiom 3** (Inverse Elements): for every element $a$ of the set $G$ there exists an element $b$ of the same set $G$, called *an inverse element of the element* $a$, such that:

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

Note, again, that in the **Axiom 3** we used the same identity element, $e$, one of potentially many such elements, that we carefully defined in the previous axiom, the **Axiom 2**.

In the next discussion of the group axioms, where we will assume only the existence of at least one right identity and of at least one right inverse, we will present a slightly more pedantic formulation of the group axioms.

As a technical aside, the construct *for any three elements* $a, b, c$ in the **Axiom 1** does not impose any additional or implied restrictions on the distinctness of the said elements.

In other words, the phrase *for any three elements* $a, b, c$ does not exclude the possibility that the three symbols $a, b, c$ actually denote *the same* element, or that these symbols denote three $truly distinct$ elements or that these three symbols denote some other mix of elements where, say, the symbols $a, b$ denote *the same* element but the symbol $c$ denotes *a different* element and so on.

**Definition 13** (duplicated for completeness): the given set $G$ with the, single, defined on it binary operation $\circ$ that satisfies the above three axioms is called *a group* and the axioms themselves are called *the group axioms*.

In the *English* language we express the facts that in the above axioms the uniqueness requirement for an identity element and for the inverses of a group is absent by using the indefinite article *an* when referring to these types of elements – *an* identity and *an* inverse.

However, in the upcoming exercises we will be asked to show that under the above set of axioms the uniqueness of an identity element and of the inverses of a group must necessarily follow from that set of group axioms.

As such and soon after, in the English language we will replace the indefinite article *an* with the definite article *the* when referring to these elements – *the* identity element of a group and *the* inverse element of a given element of a group.

The readers who are new to the concept of *a proof* in mathematics will have a very hard time doing this exercise on their own - that is understood and that is expected.

Here, not only we are on the hook to generate the respective *proof* on our own, which is a task that entails a good understanding of what a mathematical proof *is* to begin with, but we have to do so in a *generic*, *reusable* and *templetizable* way, which is a task that, additionally, entails a good understanding of certain *properties* of a proof, which themselves amount to somewhat of a high wire balancing act.

Since this is not a text in which we specifically teach how to construct mathematical proofs, the best advice that we can give to the newcomers is to operate in the *monkey-see-monkey-do* fashion coupled with the ideas described in the **What Makes It Perfect** chapter (peek-and-go).

Having said that, in an incredibly compressed and *descriptive* way, a mathematical proof is a convincing enough argument that:

- starts with a given premise
- stitches together a finite number of *steps* or *inferences*, each of which is correct and has zero mistakes, and each of which uses only the given primitive notions, definitions, axioms and previously proven results and
- terminates with a given conclusion

The above *description* of a mathematical proof is recursive because it is a very important property of a mathematical proof that, in negative terms, *the current* proof cannot possibly use any *future results* that have not been proven yet - intuitively speaking, no future knowledge can be the foundation for a rigorous establishment of the current knowledge.

In positive terms, *the current* proof can use only *the previously proven* results coupled with the primitive notions, definitions and axioms.

Since a mathematically sound recursive definition must terminate (in a finite number of iterations), it follows that once a collection of primitive notions, definitions, axioms and the rules of inference are inked, there will be such a thing as *a first theorem* in that system of axioms.

Well, consider **Theorem 2** to be our fist group-theoretic theorem or consider the next exercise to be our fist group-theoretic theorem.

Either way, we now understand that in the upcoming exercise we have *an extremely limited budget* of mathematical entities that we *are allowed to* manipulate.

That is what makes this whole business of generating proofs fun and that is what makes makes this whole business of generating proofs difficult, in general.

The game is on.

Even if many of our readers are familiar with the concept of a mathematical proof and even if many of our readers did generate their own correct and valid proofs in other, vaguely defined, mathematical disciplines, we, still, would like to stress one more time that here and now we are starting at the very bottom of the hierarchy of the relevant theorems and we do not really have much to go on except (!) for the three stated above group axioms.

That is, we, as this proof generators, are not allowed to bring into the upcoming proofs much external knowledge.

In practice, it will become evident very quickly that many readers are simply not ready to exhibit the required level of *mathematical care* in their reasoning.

The symbolic manipulations in the theory of groups may look dry and abstract but they do demand the not-middle-school-usual and not-high-school-usual depth of understanding of both *what* are we doing and *why* are we allowed to do that.

Intuitively speaking, in such manipulations as newcomers we have to *slow down a lot*.

How much is *a lot*?

The amount of the proposed *slowing down* will become evident once we crawl, one baby step at a time, through the first proof.

To that end, not only we know that generating the proofs in these discussions *will be* difficult to many readers, but we know exactly *where* these difficulties will be encountered.

That is why we will be doing these exercises together. In order for the *monkey-see-monkey-do* paradigm to have a chance at succeeding, initially, we will keep sprinkling the relevant commentary in the upcoming proofs to highlight these fine points.

Eventually, though, we will be supplying less and less of such commentary and eventually, our mind will zip through all the commentary and more almost instantly. Getting to that state of affairs, however, requires an effort.

As a gentle hint, the main bright *tactical* idea in the early group-theoretic proofs is to avoid the work with the *monolithic* objects, such as $a$, or $x$, or $e$, and, instead, try to find an advantageous *compound* object, such as a group product $a^{-1} \circ a$ or some such, and so on.

**Theorem 3:** (show that) if for a certain element $a$ of a group $G$ there exists an element $e_a$ of $G$ that satisfies either the relationship:

$$e_a = a \tag{6}$$

or, separately, the relationship:

$$e_a a = a \tag{7}$$

then it necessarily must be the case that:

$$e_a = e \tag{8}$$

where $e$ is an identity element of the group $G$ (from *this* **Axiom 2**).

**Proof:** begins with the assumption that just and only the relationship shown in (**6**) holds: $e_a = e$.

Commentary: note that in order to avoid the necessity of dragging the cumbersome $\circ$ and $\cdot$ symbols in many symbolic manipulations, we omit these symbols altogether but we understand that these symbols, that denote *the group operation*, are always there nonetheless and they can be reproduced at will and on the moment's notice on demand.

Thus, we, first, assume that in a group $G$ there exists an element $e_a$ such that upon the group multiplication of a certain element $a$ of $G$ by that element $e_a$ *from the right*:

$$ae_a = a$$

we get back the original element $a$.

Commentary: this portion of the proof can operate only in terms of what we have across the three group axioms *listed in this discussion* and the assumption (**6**), which is, seemingly, not much.

What *are* we allowed to manipulate?

Ah.

Actually quite a lot: we have all three group axioms shown above, we have an identity element $e$ of $G$, we have all the relevant inverses of $G$ and we have the equation in (**6**).

The motivating question now is: how can we legally shuffle this material into submission?

Since $G$ is *a group* and $e$ is an identity element of $G$, we know that for *any* element $b$ of $G$, as per the **Axiom 2**, it must be the case that:

$$be = b \tag{9}$$

Commentary: thus, this transition is legal and valid because, as per the **Axiom 2**, the group multiplication by the element $e$ *from both sides* (!) is allowed.

Thus, we *are allowed* to choose and use the group multiplication by $e$ *from the right* and that is exactly what we do.

But we are told that in the group $G$ *there exists* an element named $e_a$ with the property captured in (**6**).

Hence, the next expression constructed by hand is also legal and valid because in such an expression all we are doing is multiplying an arbitrary group element $b$ by the said element $e_a$ from the right in order to investigate what will happen next.

For such an element $b$, we, thus, have as per (**9**):

$$be_a = (be)e_a$$

and, by the **Axiom 1**, since the group operation is associative, we have:

$$be_a = (be)e_a = b(ee_a) \tag{10}$$

Commentary: note how we already came through with the earlier hint - instead of working with the monolithic object, $b$, in (**10**), we manufactured what is supposed to be an advantageous *compound* object, a group product $be = b \cdot e = b \circ e$.

Will that maneuver bear any fruit?

Let us see.

By the **Axiom 3**, we also have for the group element $a$:

$$e = a^{-1}a \tag{11}$$

where $a^{-1}$ designates a double-sided inverse element of $a$.

Commentary: **the Axiom 3** assures us that for a given element $a$ of the group $G$ among the elements of that group we can always find *an* element $x$ such that $ax = xa = e$, meaning that the group multiplication by the element $x$ *from both sides* is allowed and meaning that for the said element $e$ we pick an identity element whose existence is gifted to us by the **Axiom 1**.

Hence, we *are allowed* to choose and use an inverse element that sits *to the left* of its original - and that is exactly what we do.

Here we simply named that inverse element $x$ of $a$ as $a^{-1}$.

Note that we are not concerned at all about the fact that this is *an* element of $G$, since nowhere will we demand that it must be *the* element $x$.

Injecting the RHS of (**11**) into the RHS of (**10**), we find:

$$be_a = (be)e_a = b(ee_a) = b(a^{-1}ae_a) \tag{12}$$

Commentary: aha, we did it again!

Onto the monolithic object $e$ we poured the **Axiom 3** and, like mushrooms after the rain, out popped what is supposed to be yet another advantageous compound object $a^{-1}a$.

Moreover, here, on the RHS of (**12**), we again have a 3-element product that we already met in the **Associativity** chapter.

Precisely *because* the group operation is associative, we can choose the order in which the individual group multiplications in such a product are to be executed on the RHS of (**12**) at will - and, clearly, we want to choose the *rightmost* group product to be evaluated first.

By the, associativity, **Axiom 1**, we have for the 3-element product on the RHS of (**12**):

$$a^{-1}ae_a = a^{-1}(ae_a) \tag{13}$$

But by the given assumption (**6**), we are told that:

$$ae_a = a$$

Commentary: note well that the relation shown in (6) is the only specimen that we are allowed to bring into this proof - explicitly, we are not allowed to use the relation shown in (**7**).

Hence, the RHS of (**12**), via (**13**), collapses into:

$$be_a = \ldots = b(a^{-1}(ae_a)) = b(a^{-1}a) \tag{14}$$

Commentary: thus far, the result obtained on the far right in (**14**) is legal and valid.

By the **Axiom 3**, we have for the last two elements on the RHS of (**14**):

$$a^{-1}a = e$$

Hence, the expression in (**14**) becomes:

$$be_a = \ldots = b(a^{-1}a) = b(e) = be \tag{15}$$

But by the **Axiom 2**, we have for the last two elements on the RHS of (**15**):

$$be = b$$

Therefore, the expression in (**15**) becomes:

$$be_a = \ldots = be = b \tag{16}$$

Omitting all the intermediate results in (**16**), via *a finite sequence of legal inferences that have exactly zero mistakes*, we have shown that:

$$be_a = b \tag{17}$$

Next, we want to analyze the result of the group multiplication of the element $b$ of $G$ by the impostor $e_a$ *from the left*:

$$e_a b = ?$$

Commentary: note well that the proposed existence of the impostor $e_a$ does not really cancel the fact that a ruling king of the hill $e$ can still eat *any* element of $G$ for breakfast.

In other words, we now realize that the **Axiom 2** is actually very powerful precisely because it revolves around a universal requirement *any* - and the element $e_a$ is *any* element of $G$.

Moreover, as per the **Axiom 2**, the group multiplication by the element $e$ *from both sides* is allowed.

Thus, we *are allowed* to choose and use the group multiplication by $e$ *from the left* and that is exactly what we do.

By the **Axiom 2**, we have for the element $e_a$:

$$ee_a = e_a$$

Therefore, the above expression becomes:

$$e_a b = (ee_a)b \tag{18}$$

>Commentary: can we spell *monolithic-to-compound* again?

By the **Axiom 3**, however, we have for the element $e$ in (**18**):

$$e = a^{-1}a$$

implying that:

$$e_a b = (ee_a)b = (a^{-1}ae_a)b \tag{19}$$

By the **Axiom 1**, we have for the 3-element product on the RHS of (**19**):

$$a^{-1}ae_a = a^{-1}(ae_a)$$

and by the working assumption (**6**), we have it that $ae_a = a$.

As such, the expression in (**19**) becomes:

$$e_a b = \ldots = (a^{-1}(ae_a))b = (a^{-1}a)b \tag{20}$$

By the **Axiom 3**, we have for the two elements on the far right side of (**20**):

$$a^{-1}a = e$$

Then, the expression in (**20**) morphs into:

$$e_a b = \ldots = (a^{-1}a)b = (e)b = eb \tag{21}$$

By the (double-sided) **Axiom 2**, we have for the two rightmost elements in (**21**):

$$eb = b$$

and, thus:

$$e_a b = \ldots = eb = b \tag{22}$$

Omitting all the intermediate results in (22), via *a finite sequence of legal inferences that have exactly zero mistakes*, we have shown that:

$$e_a b = b \tag{23}$$

In other words, we have shown that for any element $b$ of $G$, under the standing assumption in (**6**), we have:

$$be_a = e_a b = b \tag{24}$$

But the element $e$ of $G$ is *any* such element $b$.

In other words, in the result (**24**) we simply put $b = e$:

$$ee_a = e \tag{25}$$

On the other hand, by *the definition* of the element $e$, we also have (**Axiom 2**):

$$ee_a = e_a \tag{26}$$

As such, the equations (**25**) and (**26**) do show that, since the group product $e \circ e_a$ names *a particular* or *a uniquely defined* element of the group $G$, under the assumption (**6**) it necessarily must be the case that:

$$e_a = e$$

which is what was required to prove. □

The line of reasoning that we showed here does not only constitute a correct proof of the theorem formulated for the assumption (**6**) but it is also a proof that is *reusable* enough so as to be a template for the next proof that is based on the assumption (**7**).

Namely, we now assume that just and only the relation shown in (**7**):

$$e_a a = a$$

holds and our objective is to weave a convincing enough argument that even in that case the element $e_a$ is actually the element $e$.

To that end, we will be less wordy now and as a useful exercise, hoping that our readers will do the needful and fill in the gaps, we will only show the two legal strings that constitute a correct proof:

$$be_a = b(e_a e) = be_a aa^{-1} = baa^{-1} = be = b \tag{27}$$

and:

$$e_a b = (e_a e)b = e_a aa^{-1}b = aa^{-1}b = eb = b \tag{28}$$

Our readers should nonetheless explain all things group-theoretic that are unfolding in these two strings of abstract manipulations and boast their understanding of the *monolithic-to-compound* tactical maneuver.

Since we managed to show that $be_a = b$ and that $e_a b = b$ for any element $b$ of a group, it follows, via the templetizable argument shown in the first part of this proof above, that even when $e_a a = a$ it is still the case that $e_a = e$. □

The theorem that we just proved tells us that there is one and only one identity element in a group - there are no other contenders for that role and, thus, we refer to it as *the* identity element of a group and we designate the well-defined identity element of a group unambiguously with $e$.

Moreover, that unique identity element of a group is double-sided and it commutes with every element of its group.

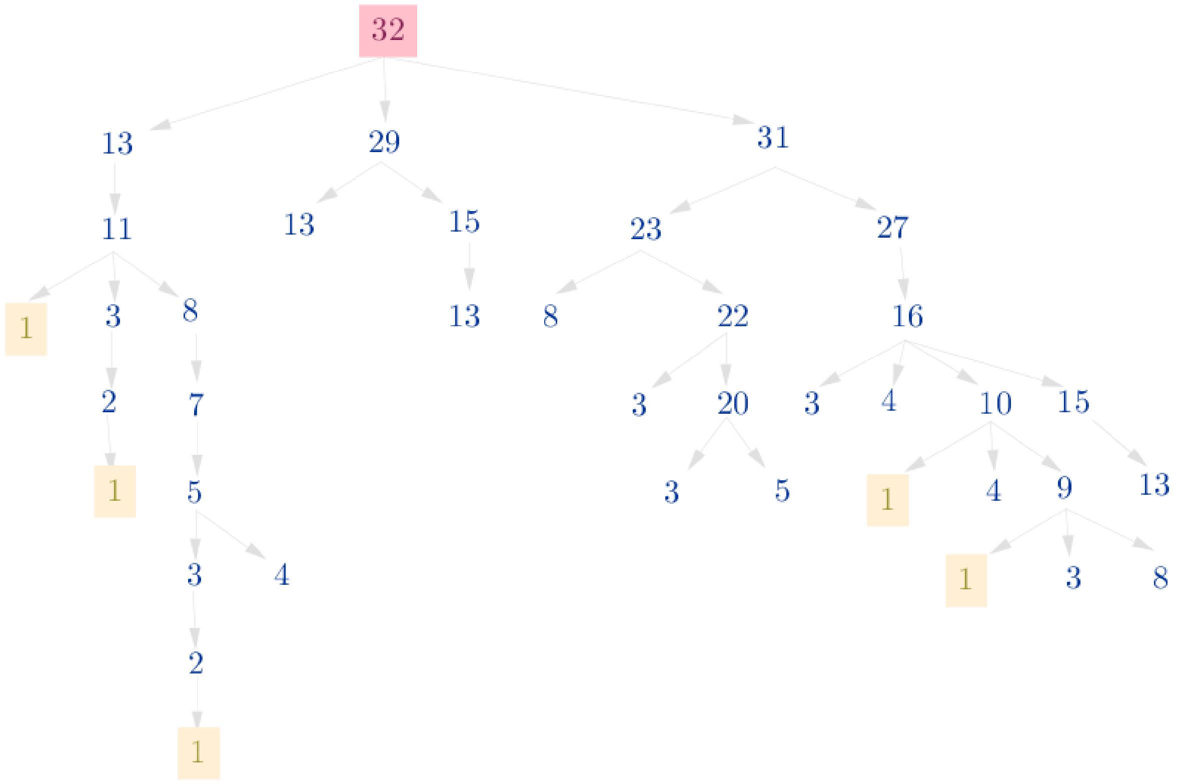
## Proof Post-Processing and Analysis

We are still not done with the proof of the uniqueness of the identity element of a group - we still have to digest it by constructing its so-called *dependency tree* and by making useful technical observations about it.

A dependency tree of a given theorem is a construct that lists all the previous theorems that the proof of this theorem depends on, all the way down to the discipline-specific axioms.

Normally, inhaling a healthy dose of a reality-check into it, constructing such dependency trees for all but the simplest, in some sense, theorems amounts to a monumental task that may be not very practical for a human or even a group of humans, pun intended.

Here, for an example, is *an incomplete* dependency tree for the Euclid's *"Elements"* Book 1 Proposition 32 that states, among other things, that the sum of the magnitudes of the interior angles of a planar triangle is equal to two right angles (Figure 10.1):



In the tree above *the root* node, shown on the pink background, is the Book 1 Proposition 32 itself and the nodes *below* the root show the numbers of the Book 1 theorems that the current proof *depends on.*

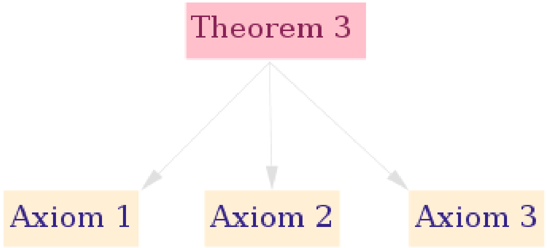
The *terminal* nodes in that tree, shown on the yellow background, are marked with the theorem number 1 and we did not show *all* such terminal nodes - in certain cases we did not show anything below the theorems numbered 13, 8 and 5 in order to avoid the clutter, but the dependency tree for these theorems is spelled out completely on the diagram's left side.

Constructing such dependency trees is an addictive fun exercise that gives us a sobering look at what exactly does it take to prove, in an axiomatic system that is actually not rigorous enough by the modern standards, a seemingly trivial fact that we all remember from our middle school days.

While we will not be dedicating any quality time to the task of constructing the dependency trees for our theorems, we, nonetheless, would like to make our readers aware of their existence - these dependency trees can play a useful pedagogical role and be a learning tool that keeps us honest in our proofs, enforcing the all-important *no future results in the current proof* requirement.

Since this is one of the very first group-theoretic theorems, there is not much of a dependency *tree* to speak of for it.

But we do see that in that proof we used all three axioms - the **Axiom 1**, the **Axiom 2** and the **Axiom 3** (Figure 10.2):



In the **Take 5** section below we will see that the last two axioms, namely the **Axiom 2** and the **Axiom 3**, can be replaced with a single *unrestricted group division* axiom.

By first assuming the existence of an impostor *right* identity $e_a$ in (**6**), note that in the transition (**12**), justified by (**11**), we relied heavily on the existence of a so-called *left* inverse or an element that, while sitting *to the left* of the original element, produced an identity element in the respective group product $a^{-1}a$. The existence of such a left inverse is gifted to us by the double-sided **Axiom 3**.

In the upcoming **Take 3** section, however, we will lose that **double**-sided luxury.

What should we do then?

Think about it.

We, clearly, would have to synthesize a more delicate or a more restrictive argument.

Likewise, in the transition (**27**), by assuming the existence of an impostor *left* identity $e_a$ in (**7**), we relied heavily on the existence of a so-called *right* inverse or an element that, while sitting *to the right* of the original element, produced an identity element in the respective group product $aa^{-1}$. The existence of such a right inverse is gifted to us by the double-sided **Axiom 3**.

Again, in the upcoming, weaker, group axioms we will lose that **double**-sided luxury as we shall require only the existence of a *single-sided* identity element and of a *like* single-sided inverse element for each element of a group.

**Theorem 4:** (show that) if for an element $a$ of a group $G$ there exists an element $x_a$ of $G$ that satisfies either the relationship:

$$ax_a = e \tag{29}$$

or, separately, the relationship:

$$x_a a = e \tag{30}$$

then it necessarily must be the case that:

$$x_a = a^{-1} \tag{31}$$

where $e$ is an identity element of the group $G$ from the **Axiom 2** and $a^{-1}$ is an inverse of the element $a$ from the **Axiom 3**.

**Proof:** begins with the assumption that just and only the relationship shown in (**29**) holds:

$$ax_a = e$$

In other words, we, first, assume that in a group $G$ there exists an element $x_a$ such that upon the group multiplication of an element $a$ of $G$ by that element $x_a$ *from the right*:

$$ax_a = e$$

we obtain an identity element $e$ of the group $G$ from the **Axiom 2**.

Commentary: in the **Take 3** and **Take 4** sections of this chapter we will get a bit more pedantic with the formulations of the group axioms and in them we will name one of the many possible left identities as $e_{l0}$ or one of the many possible right identities as $e_{r0}$.

On the one hand, by the same **Axiom 2**, we have for the element $a^{-1}$ of the group $G$:

$$a^{-1}e = a^{-1} \tag{32}$$

and, on the other hand, that element $e$ in (**32**) is produced by (**29**).

Thus, the LHS of (**32**) can be rewritten as follows:

$$a^{-1}ax_a = a^{-1} \tag{33}$$

Since the existence of a left inverse $a^{-1}$ of the element $a$ of the group $G$ is gifted to us by the **Axiom 3**, $a^{-1}a = e$, the LHS of (**33**), via the **Axiom 1**, becomes:

$$a^{-1}ax_a = (a^{-1}a)x_a = ex_a = a^{-1} \tag{34}$$

and, since the existence of a left identity $e$ is gifted to us by the **Axiom 2**, the LHS of (**34**) becomes:

$$ex_a = x_a = a^{-1}$$

which is what was required to prove. □

Likewise, we now assume that just and only the relationship shown in (**30**) holds:

$$x_a a = e$$

and then, by the **Axiom 2**, we have:

$$ea^{-1} = a^{-1}$$

which, by the assumption (**30**), is to say that:

$$x_a aa^{-1} = a^{-1}$$

which, by the **Axiom 1** and the **Axiom 3**, is to say that:

$$x_a aa^{-1} = x_a(aa^{-1}) = x_a e = a^{-1}$$

which, by the **Axiom 2**, is to say that:

$$x_a e = x_a = a^{-1}$$

which is what was required to prove. □

Note that, again, the tactical foundation on which this proof was erected still has the *monolithic-to-compound* motto chiseled on it.

The theorem that we just proved tells us that for a given element of a group, $a$, there is one and only one inverse - among the other elements of this group there no other contenders for that role.

Since the inverse of a given group element $a$ is unique, we can agree to designate such an inverse in an unambiguous fashion as:

$$a^{-1}$$

and *define**

$$a^0 = e$$

understanding how such a definition, intuitively speaking, *converges*, since we already proved that the identity element of a group, $e$, is unique.

We also see that the inverse element of a given group element is double-sided and that every element of a group commutes with its inverse.

We can also borrow the mechanics of the power arithmetic as it applies to numbers and import into the theory of groups:

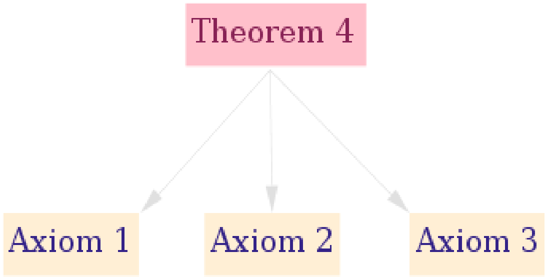
$$a^{-1} \cdot a^{-1} \cdot a^{-1} \cdot a^{-1} = a^{-1 \cdot 4} = a^{-4}$$

and so on.

### Proof Post-Processing and Analysis

Is mostly left to the reader as an exercise.

The dependency tree of **Theorem 4** is just as simple as the dependency tree of Theorem 3 (Figure 10.3):



By first assuming the existence of an impostor *right* inverse $x_a$ in (**29**), in the transition from (**33**) to (**34**) we relied heavily on the existence of *a left* inverse $a^{-1}$ gifted to us by the double-sided **Axiom 3**.

By, next, assuming the existence of an impostor *left* inverse $x_a$ in (**30**), we relied on the existence of *a right* inverse $a^{-1}$ gifted to us by the double-sided **Axiom 3**.

But in the next two takes on group axioms we will lose that double-sided luxury.

## 10.3 Take 3

### Only the Existence of Right Identity and Inverses Assumed

In the next two versions of the group axioms we will further weaken the demands imposed on the candidate set and the candidate binary operation by:

- removing the, previously taken for granted, uniformity of an identity element and of the inverse elements of a group by:
    - splitting an identity element of a group into *a left identity* $e_l$ and *a right identity* $e_r$ and by
    - splitting an inverse of a given element of a group into *a left inverse* $x_l$ and *a right inverse* $x_r$ and by
- sorting the above four *types* of elements into the following two piles:
    - a right-sided pile that contains only a right identity and only the right inverses and
    - a left-sided pile that contains only a left identity and only the left inverses

In addition to the associativity of the proposed binary operation, in this discussion we will only demand that in the candidate set there exists at least one *right* identity element and that each element of the candidate set possesses at least one *right* inverse element that yields a particular right identity of that group.

In the next discussion we will only demand that, in addition to the associativity of the proposed binary operation, of course, in the candidate set there exists at least one *left* identity element and that each element of the candidate set possesses at least one *left* inverse element that yields a particular left identity of that group.

It should also be understood that, as their names imply, the geographic location of a corresponding element in question with respect to its peer decides or locks in its *sideness*.

Namely.

A *left identity* $e_l$ is such an element of a group for which the following relationship holds for all elements $a$ of a group:

$$e_l \cdot a = a$$

A *right identity* $e_r$ is such an element of a group for which the following relationship holds for all elements $a$ of a group:

$$a \cdot e_r = a$$

A *left inverse* $x_l$ of a given group element $a$ is such an element of that group that produces *a particular* left identity of that group $e_{l0}$ when coupled with the element $a$ via the corresponding group operation:

$$x_l \cdot a = e_{l0}$$

A *right inverse* $x_r$ of a given group element $a$ is such an element of that group that produces *a particular* right identity of that group $e_{r0}$ when coupled with the element $a$ via the corresponding group operation:

$$a \cdot x_r = e_{r0}$$

Keep in mind that since we are *not* demanding the uniqueness of the single-sided identity elements of a group, we will operate under the assumption that there could be *several* left identities or *several* right identities in a group.

Thus, in the above definitions of the single-sided inverses we will settle on a particular single-sided identity element - out of the potential multitude of such identity elements we pick that one, $e_{l0}$ or $e_{r0}$, respectively.

As an exercise, in this discussion our readers will be invited to *prove* on their own that even under the much weakened, *right-sided*, group axioms *a left* identity $e_l$ and *a left* inverse $x_l$ are, in fact and nonetheless, respectively, the elements $e_r$ and $x_r$ named in that set of group axioms and that these elements are unique:

$$e_l = e_r = e, \;\; x_l = x_r = x$$

In the next discussion we will *prove* that even under the much weakened, *left-sided*, group axioms *a right* identity $e_r$ and *a right* inverse $x_r$ are, in fact and nonetheless, respectively, the elements $e_l$ and $x_l$ named in that set of group axioms and that these elements are unique:

$$e_r = e_l = e, \;\; x_r = x_l = x$$

Note carefully that, as a useful and fun exercise that our readers are invited to do on their own, crossing the beams, the Ghost Busters style, is *not* going to work for a set of group axioms:

- demanding the existence of only *a left* identity and of only *a right* inverse does not lead to a set of group axioms and, vice versa
- demanding the existence of only *a right* identity and of only *a left* inverse does not lead to a set of group axioms also

In other words, a set of group axioms can be generated only if we demand the **same**-sideness of identity and inverses *in unison* and trying to prove the opposite is a very instructive way to witness how failures come about in mathematics.

In the upcoming set of group axioms we will designate an identity element with $e_r$ and we will designate an inverse element with $x_r$ for purely pedagogical and illustrative purposes - in order to impress the hardness of the requirement that must be honored in the relevant proofs on the minds of the younger students who may not be as experienced with abstract symbolic manipulations.

Since we will quickly prove that in that case a left identity is also a right identity and that a left inverse is also a right inverse, we may have inked the upcoming axioms with just the traditional symbols $e$ and $x$. This is how these things are normally done in the grown-up literature on the subject.

To that end, let a set $G$, finite or otherwise, with a single binary operation $\circ$ defined on the elements of that set be given.

Suppose further that the said binary operation coupled with the said set in an order-insensitive fashion satisfies the following three axioms.

**Axiom 1** (Associativity): for any three elements $a, b, c$ of the set $G$ the following relationship holds:

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

**Axiom 2** (Identity Element): among the elements of the set $G$ there exists at least one element $e_r$, called *a right identity element*, such that for any element $a$ of $G$ it is the case that:

$$a \circ e_r = a$$

**Axiom 3** (Inverse Elements): among the right identity elements of $G$ there exists an element $e_{r0}$ such that for every element $a$ of the set $G$ there exists at least one element $x_r$ of the same set $G$, called *a right inverse element of* $a$, such that:

$$a \circ x_r = e_{r0}$$

**Definition 13** (duplicated for completeness): the given set $G$ with the, single, defined on it binary operation $\circ$ that satisfies the above three axioms is called *a group* and the axioms themselves are called *the group axioms*.

We now suggest that our readers try to prove, on their own, the following

**Theorem 5:** under the given set of axioms it must also be the case that for any element $a$ of a group $G$ the following, left-sided, relationship:

$$e_{r0} \cdot a = a \tag{35}$$

holds, where $e_{r0}$ is a right identity element of a group from the **Axiom 2**.

**Proof:** after analyzing the proofs of **Theorems 3** and **Theorem 4**, our readers should presently catch on to the mathematical program, according to which in this proof the only *given* units of knowledge that we are allowed to use are a right inverse from *this* **Axiom 3** and a particular right identity from *this* **Axiom 2**.

To that end, this **Axiom 3** gives us a universal gift in the shape of the existence of a right inverse for *any* element of a given group $G$.

Thus, let $a$ be any element of a group and let $x_r$ be one of its right inverses.

Then, by the current **Axiom 3**, we have:

$$ax_r = e_{r0} \tag{36}$$

Multiplying both sides of the equation (**36**) by the element $e_{r0}$ from *the left*, we find:

$$e_{r0}ax_r = e_{r0}e_{r0} \tag{37}$$

But, since the element $e_{r0}$ is a right identity, by the **Axiom 2**, we have for the RHS of (**37**):

$$e_{r0}ax_r = e_{r0}e_{r0} = e_{r0} \tag{38}$$

Thus, we can substitute the LHS image of the element $e_{r0}$ from (**36**) back into the RHS of (**38**):

$$e_{r0}ax_r = ax_r \tag{39}$$

Now comes the *monolithic-to-compound* maneuver.

By the same **Axiom 3**, the element of a group $x_r$ has at least one of its own right inverses - let $y_r$ be one such right inverse:

$$x_r \cdot y_r = e_{r0}$$

Therefore, when we multiply both sides of (**39**) by the element $y_r$ from *the right*, we shall find:

$$e_{r0}ax_ry_r = ax_ry_r$$

which, by **Theorem 2** applied to the 4-element product on the LHS of the above equation:

$$e_{r0}ax_ry_r = (e_{r0}a)(x_ry_r) = (e_{r0}a)e_{r0} = e_{r0}ae_{r0}$$

is to say that:

$$e_{r0}ae_{r0} = ax_ry_r = ae_{r0} \tag{40}$$

Keeping the RHS of (**40**) as is, we can rewrite the LHS of (**40**), by the **Axiom 1**, as follows:

$$e_{r0}ae_{r0} = (e_{r0}a)e_{r0} = ae_{r0} \tag{41}$$

But by the **Axiom 2**, the element $e_{r0}$ is a right identity and, hence, we have for each side of the equal sign in (**41**):

$$(e_{r0}a)e_{r0} = (e_{r0}a) = e_{r0}a$$

which is the LHS of (**41**), and:

$$ae_{r0} = a$$

which is the RHS of (**41**).

Therefore:

$$e_{r0}a = a$$

which is what was required to prove. □

In other words, we have shown that if the group element $e_{r0}$ happens to be a right identity of a group then that element is also a left identity of the same group.

However, we still have not demonstrated that the identity element of a group must be *unique* - we shall do exactly that in the next theorem in which we will use the above fact.

**Theorem 6:** under the given set of axioms the identity element of a group is unique.

**Proof:** in **Theorem 5** we proved that a right identity of a group $e_{r0}$ is also a left identity of the same group.

Thus, let $e_r$ be an arbitrary right identity of a group and let $e_l$ be an arbitrary left identity of the same group.

By the **Axiom 2**, we have for the element $e_r$:

$$e_l \cdot e_r = e_l \tag{42}$$

and, by **Theorem 5**, we have for the element $e_l$:

$$e_l \cdot e_r = e_r \tag{43}$$

Intuitively speaking, the element $e_r$ does not move whatever sits to its left anywhere and the element $e_l$ does not move whatever sits to its right anywhere. Thus:

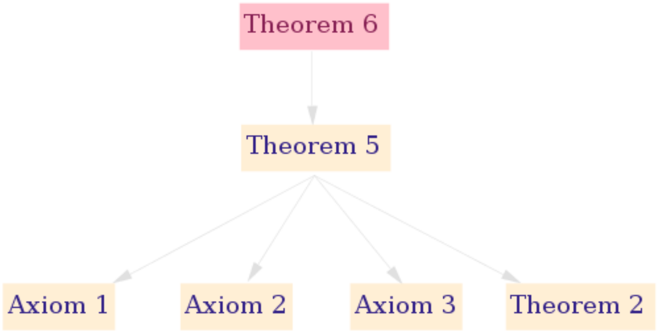
$$e_l \cdot e_r = e_l = e_r = e_l \cdot e_r$$

which means that the identity element of a group is unique and we can unambiguously designate it with $e$:

$$e_r = e_l = e$$

which is what was required to prove. □

Note that the dependency tree of **Theorem 6** will now contain **Theorem 5**, which itself depends on **Theorem 2** (Figure 10.4):



Now that we have the above two theorems on the books, the proof of the next theorem now becomes a child's play.

**Theorem 7:** under the given set of axioms it must also be the case that for any element $a$ of a group $G$ the following, left-sided, relationship:

$$x_r \cdot a = e \tag{44}$$

holds, where $x_r$ is a right inverse element of the element $a$ from the **Axiom 3** and $e$ is the, now unique, identity element of the group $G$.

**Proof:** by the just proven **Theorem 6**, since the identity element of a group $e$ is unique, we have for the elements $a$ and one of its right inverses $x_r$:

$$a \cdot x_r = e \tag{45}$$

Multiplying the relationship in (**45**) through by the right inverse $x_r$ from *the left*, we have:

$$x_r \cdot a \cdot x_r = x_r \cdot e \tag{46}$$

By **Theorem 6**, we have for the RHS of (**46**):

$$x_r \cdot e = x_r$$

and by the **Axiom 1**, we have for the LHS of (**46**):

$$x_r \cdot a \cdot x_r = (x_r \cdot a) \cdot x_r$$

Thus, equating the RHSs of the above two intermediate results:

$$(x_r \cdot a) \cdot x_r = x_r \tag{47}$$

Commentary: *monolithic-to-compound* ...

But by the **Axiom 3**, the element $x_r$ has at least one right inverse of its own - let $y_r$ be such a right inverse:

$$x_r \cdot y_r = e$$

Multiplying (**47**) through by $y_r$ from *the right*, we find:

$$(x_r \cdot a) \cdot x_r \cdot y_r = x_r \cdot y_r$$

which, by **Theorem 2** applied to the 4-element product on the LHS of the above equation, is to say that:

$$(x_r \cdot a) \cdot e = e$$

But by **Theorem 6**, we have for the LHS in the above relationship:

$$(x_r \cdot a) \cdot e = x_r \cdot a$$

Hence:

$$x_r \cdot a = e$$

which is what was required to prove. □

In other words, we have shown that if $x_r$ happens to be a right inverse of a given element of a group then $x_r$ is also a left inverse of the same element.

However, we still have not demonstrated that a given element of a group has *a unique* inverse - we shall do exactly that in the next theorem in which we will use the above fact.

**Theorem 8:** under the given set of axioms the inverse element of a given element of a group is unique.

**Proof:** in **Theorem 7** we proved that a right inverse of a given element of a group $x_r$ is also a left inverse of the same element.

Thus, let $x_r$ be an arbitrary right inverse of a given group element $a$:

$$a \cdot x_r = e \tag{48}$$

and let $x_l$ be an arbitrary left inverse of the same element $a$:

$$x_l \cdot a = e \tag{49}$$

But then, by **Theorem 6** and (**49**), we have for the element $x_r$:

$$x_r = e \cdot x_r = x_l \cdot a \cdot x_r$$

and, likewise, we have for the element $x_l$ via (**48**):

$$x_l = x_l \cdot e = x_l \cdot a \cdot x_r$$

But the associativity of the group operation captured by the **Axiom 1**, as we already explained this idea in the **Associativity** chapter, assigns an unambiguous meaning to each of the 3-element products shown on the RHSs of the last two results - such a 3-element group product designates a uniquely defined element of the underlying group.

Thus, indeed:

$$x_r = x_l = x$$

which is what was required to prove. □

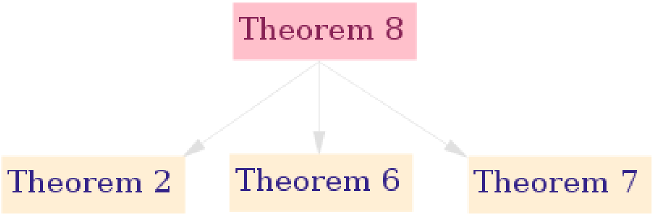
In other words, we have shown that the inverse element of a given group element $a$ is unique.

Thus, we can all agree on an unambiguous designation of such an inverse as:

$$a^{-1}$$

since for a given element of a group there are no other contenders for that role.

Note that the dependency tree of **Theorem 8** becomes (Figure 10.5):



and, overall, the proofs shown in this discussion dovetail this set of group axioms into the set of group axioms shown in the above **Take 1** section and we see that in this set of group axioms we might have called the above *right identity* as just *an identity* and we might have called the above *right inverse* as *an inverse* and so on.

# 10.4 Take 4

## Only the Existence of Left Identity and Inverses Assumed

In this versions of the group axioms we will weaken the demands imposed on the candidate set and the candidate binary operation by:

- removing the, previously taken for granted, uniformity of an identity element and of the inverse elements of a group by:
    - splitting an identity element of a group into *a left identity* $e_l$ and *a right identity* $e_r$ and by
    - splitting an inverse of a given element of a group into *a left inverse* $x_l$ and *a right inverse* $x_r$ and by
- sorting the above four *types* of elements into the following two piles:
    - a right-sided pile that contains only a right identity and only the right inverses and
    - a left-sided pile that contains only a left identity and only the left inverses

In addition to the associativity of the proposed binary operation, in this discussion we will only demand that in the candidate set there exists at least one *left* identity element and that each element of the candidate set possesses at least one *left* inverse element that yields a particular left identity of that group.

In the previous discussion we will only demand that, in addition to the associativity of the proposed binary operation, of course, in the candidate set there exists at least one *right* identity element and that each element of the candidate set possesses at least one *right* inverse element that yields a particular right identity of that group.

It should also be understood that, as their names imply, the geographic location of a corresponding element in question with respect to its peer decides or locks in its *sideness*.

Namely.

A *left identity* $e_l$ is such an element of a group for which the following relationship holds for all elements $a$ of a group:

$$e_l \cdot a = a$$

A *right identity* $e_r$ is such an element of a group for which the following relationship holds for all elements $a$ of a group:

$$a \cdot e_r = a$$

A *left inverse* $x_l$ of a given group element $a$ is such an element of that group that produces *a particular* left identity of that group $e_{l0}$ when coupled with the element $a$ via the corresponding group operation:

$$x_l \cdot a = e_{l0}$$

A *right inverse* $x_r$ of a given group element $a$ is such an element of that group that produces *a particular* right identity of that group $e_{r0}$ when coupled with the element $a$ via the corresponding group operation:

$$a \cdot x_r = e_{r0}$$

Keep in mind that since we are *not* demanding the uniqueness of the single-sided identity elements of a group, we will operate under the assumption that there could be *several* left identities or *several* right identities in a group.

Thus, in the above definitions of the single-sided inverses we will settle on a particular single-sided identity element - out of the potential multitude of such identity elements we pick that one, $e_{l0}$ or $e_{r0}$, respectively.

As an exercise, in this discussion our readers will be invited to *prove* on their own that even under the much weakened, *left-sided*, group axioms *a right* identity $e_r$ and *a right* inverse $x_r$ are, in fact and nonetheless, respectively, the elements $e_l$ and $x_l$ named in that set of group axioms and that these elements are unique:

$$e_r = e_l = e, \;\; x_r = x_l = x$$

In the previous section we *proved* that even under the much weakened, *right-sided*, group axioms *a left* identity $e_l$ and *a left* inverse $x_l$ are, in fact and nonetheless, respectively, the elements $e_r$ and $x_r$ named in that set of group axioms and that these elements are unique:

$$e_l = e_r = e, \;\; x_l = x_r = x$$

Note carefully that, as a useful and fun exercise that our readers are invited to do on their own, crossing the beams, the Ghost Busters style, is *not* going to work for a set of group axioms:

- demanding the existence of only *a left* identity and of only *a right* inverse does not lead to a set of group axioms and, vice versa
- demanding the existence of only *a right* identity and of only *a left* inverse does not lead to a set of group axioms also

In other words, a set of group axioms can be generated only if we demand the **same**-sideness of identity and inverses *in unison* and trying to prove the opposite is a very instructive way to witness how failures come about in mathematics.

In the upcoming set of group axioms we will designate an identity element with $e_l$ and we will designate an inverse element with $x_l$ for purely pedagogical and illustrative purposes - in order to impress the hardness of the requirement that must be honored in the relevant proofs on the minds of the younger students who may not be as experienced with abstract symbolic manipulations.

Since we will quickly prove that in that case a right identity is also a left identity and that a right inverse is also a left inverse, we may have inked the upcoming axioms with just the traditional symbols $e$ and $x$. This is how these things are normally done in the grown-up literature on the subject.

To that end, let a set $G$, finite or otherwise, with a single binary operation $\circ$ defined on the elements of that set be given.

Suppose further that the said binary operation coupled with the said set in an order-insensitive fashion satisfies the following three axioms.

**Axiom 1** (Associativity): for any three elements $a, b, c$ of the set $G$ the following relationship holds:

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

**Axiom 2** (Identity Element): among the elements of the set $G$ there exists at least one element $e_l$, called *a left identity element*, such that for any element $a$ of $G$ it is the case that:

$$e_l \circ a = a$$

**Axiom 3** (Inverse Elements): among the right identity elements of $G$ there exists an element $e_{l0}$ such that for every element $a$ of the set $G$ there exists at least one element $x_l$ of the same set $G$, called *a left inverse element of* $a$, such that:

$$x_l \circ a = e_{l0}$$

**Definition 13** (duplicated for completeness): the given set $G$ with the, single, defined on it binary operation $\circ$ that satisfies the above three axioms is called *a group* and the axioms themselves are called *the group axioms*.

We now suggest that our readers try to prove, on their own, the following

**Theorem 9:** under the given set of axioms it must also be the case that for any element $a$ of a group $G$ the following, right-sided, relationship:

$$a \cdot e_{l0} = a \tag{50}$$

holds, where $e_{l0}$ is a left identity element of a group from the **Axiom 2**.

**Proof:** after analyzing the proofs of **Theorem 3** and **Theorem 4**, our readers should now catch on to the mathematical program, according to which in this proof the only *given* units of knowledge that we are allowed to use are a left inverse from this **Axiom 3** and a particular left identity from this **Axiom 2**.

To that end, this **Axiom 3** gives us a universal gift in the shape of the existence of a left inverse for *any* element of a given group $G$.

Thus, let $a$ be any element of a group and let $x_l$ be one of its left inverses.

Then, by the **Axiom 3**, we have:

$$x_l a = e_{l0} \tag{51}$$

Multiplying both sides of the equation (**51**) by the element $e_{l0}$ from *the right*, we find:

$$x_l a e_{l0} = e_{l0} e_{l0} \tag{52}$$

But, since the element $e_{l0}$ is a left identity, by the **Axiom 2**, we have for the RHS of (**52**):

$$x_l a e_{l0} = e_{l0} e_{l0} = e_{l0} \tag{53}$$

Thus, we can substitute the LHS image of the element $e_{l0}$ from (**51**) back into the RHS of (**53**):

$$x_l a e_{l0} = x_l a \tag{54}$$

Commentary: now comes *the monolithic-to-compound maneuver* which we already discussed and employed before on multiple occasions.

By the same **Axiom 3**, the element of a group $x_l$ has at least one of its own left inverses - let $y_l$ be one such left inverse:

$$y_l \cdot x_l = e_{l0}$$

Therefore, when we multiply both sides of (**54**) by the element $y_l$ from *the left*, we shall find:

$$y_l x_l a e_{l0} = y_l x_l a$$

which, by **Theorem 2** applied to the 4-element product on the LHS of the above equation:

$$y_l x_l a e_{l0} = (y_l x_l)(a e_{l0}) = e_{l0}(a e_{l0}) = e_{l0} a e_{l0}$$

is to say that:

$$e_{l0}ae_{l0} = e_{l0}a \tag{55}$$

By the **Axiom 1**, we can rewrite the LHS of (**55**) as follows:

$$e_{l0}ae_{l0} = (e_{l0}a)e_{l0} = e_{l0}a \tag{56}$$

But by the **Axiom 2**, the element $e_{l0}$ is a left identity and, hence, we have for each side of the equal sign in (**56**):

$$(e_{l0}a)e_{l0} = (a)e_{l0} = ae_{l0}$$

which is the LHS of (**56**), and:

$$e_{l0}a = a$$

which is the RHS of (**56**).

Therefore:

$$ae_{l0} = a$$

which is what was required to prove. □

In other words, we have shown that if the element $e_{l0}$ happens to be a left identity of a group then that element is also a right identity of the same group.

However, we still have not demonstrated that the identity element of a group must be *unique* - we shall do exactly that in the next theorem in which we will use the above fact.

**Theorem 10:** under the given set of axioms the identity element of a group is unique.

**Proof:** in **Theorem 9** we proved that a left identity of a group $e_{l0}$ is also a right identity of the same group.

Thus, let $e_l$ be an arbitrary left identity of a group and let $e_r$ be an arbitrary right identity of the same group.

By the **Axiom 2**, we have for the element $e_l$:

$$e_l \cdot e_r = e_r \tag{57}$$

and, by **Theorem 9**, we have for the element $e_r$:

$$e_l \cdot e_r = e_l \tag{58}$$

Intuitively speaking, the element $e_l$ does not move whatever sits to its right anywhere and the element $e_r$ does not move whatever sits to its left anywhere.

Thus:

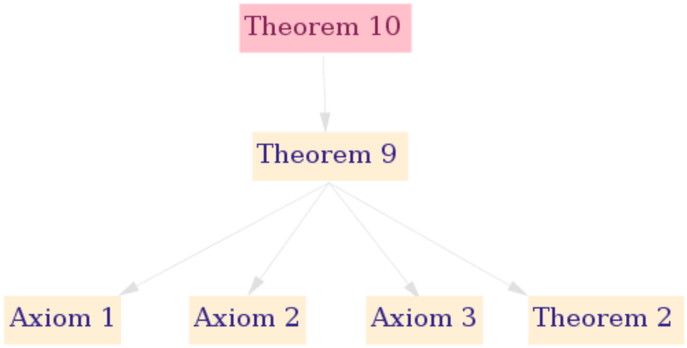
$$e_l \cdot e_r = e_r = e_l = e_l \cdot e_r$$

which means that the identity element of a group is unique and we can unambiguously designate it with $e$:

$$e_r = e_l = e$$

which is what was required to prove. □

Note that the dependency tree of **Theorem 10** will now contain **Theorem 9** (Figure 10.6):



The proof of the next theorem now becomes a child's play.

**Theorem 11:** under the given set of axioms it must also be the case that for any element $a$ of a group $G$ the following, right-sided, relationship:

$$a \cdot x_l = e \tag{59}$$

holds, where $x_l$ is a left inverse element of the element $a$ from the **Axiom 3** and $e$ is the, now unique, identity element of the group $G$.

**Proof:** by the just proven **Theorem 10**, since the identity element of a group $e$ is unique, we have for the elements $a$ and one of its left inverses $x_l$:

$$x_l \cdot a = e \tag{60}$$

Multiplying the relationship in (**60**) through by the left inverse $x_l$ from *the right*, we have:

$$x_l \cdot a \cdot x_l = e \cdot x_l \tag{61}$$

By **Theorem 10**, we have for the RHS of (**61**):

$$e \cdot x_l = x_l$$

and by the **Axiom 1**, we have for the LHS of (**61**):

$$x_l \cdot a \cdot x_l = x_l \cdot (a \cdot x_l)$$

Thus, equating the RHSs of the above two intermediate results:

$$x_l \cdot (a \cdot x_l) = x_l \tag{62}$$

Commentary: *the monolithic-to-compound maneuver* is coming up …

But by the **Axiom 3**, the element $x_l$ has at least one left inverse of its own - let $y_l$ be such a left inverse:

$$y_l \cdot x_l = e$$

Multiplying (**62**) through by $y_l$ from *the left*, we find:

$y_l \cdot x_l \cdot (a \cdot x_l) = y_l \cdot x_l$

which, by **Theorem 2** applied to the 4-element product on the LHS of the above equation, is to say that:

$$e \cdot (a \cdot x_l) = e$$

But by **Theorem 10**, we have for the LHS in the above relationship:

$$e \cdot (a \cdot x_l) = a \cdot x_l$$

Hence:

$$a \cdot x_l = e$$

which is what was required to prove. □

In other words, we have shown that if $x_l$ happens to be a left inverse of a given element of a group then $x_l$ is also a right inverse of the same element.

However, we still have not demonstrated that a given element of a group has *a unique* inverse - we shall do exactly that in the next theorem in which we will use the above fact.

**Theorem 12:** under the given set of axioms the inverse element of a given element of a group is unique.

**Proof:** in **Theorem 11** we proved that a left inverse of a given element of a group $x_l$ is also a right inverse of the same element.

Thus, let $x_l$ be an arbitrary left inverse of a given group element $a$:

$$x_l \cdot a = e \tag{63}$$

and let $x_r$ be an arbitrary right inverse of the same element $a$:

$$a \cdot x_r = e \tag{64}$$

But then, by **Theorem 10** and (**64**), we have for the element $x_l$:

$$x_l = x_l \cdot e = x_l \cdot a \cdot x_r$$

and, likewise, we have for the element $x_r$ via (**63**):

$$x_r = e \cdot x_r = x_l \cdot a \cdot x_r$$

But the associativity of the group operation captured by the **Axiom 1**, as we already explained this idea in the **Associativity** chapter, assigns an unambiguous meaning to each of the 3-element products shown on the RHSs of the last two results - such a 3-element group product designates a uniquely defined element of the underlying group.

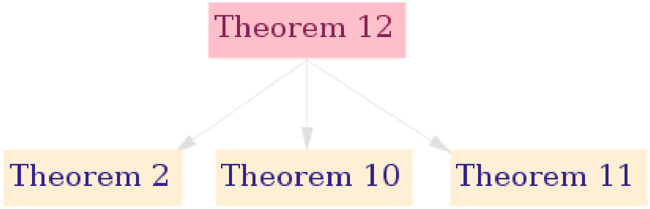
As such, indeed:

$$x_l = x_r = x$$

which is what was required to prove. □

In other words, we have shown that the inverse element of a given group element $a$ is unique. Hence, we can all agree on an unambiguous designation of such an inverse as $a^{-1}$ since for a given element of a group there are no other contenders for that role.

Note that the dependency tree of **Theorem 12** becomes (Figure 10.7):



and, overall, the proofs shown in this discussion dovetail this set of group axioms into the set of group axioms shown in the **Take 1** discussion and we see that in this set of group axioms we might have called the above *left identity* as just *an identity* and we might have called the above *left inverse* as *an inverse* and so on.

In the next discussion we will complete the brief survey of the different types of group axioms by presenting the, single, so-called *unrestricted group division* axiom that replaces the two traditional axioms of the identity element and of the inverse elements of a group.

# 10.5 Take 5

## Unrestricted Group Division

In this, final, discussion of the various types of group axioms we shall illustrate the idea spelled out at the beginning of this chapter, where we observed that it is really nice to have a minimalistic set of requirements or as low of a barrier to entry as possible in order to deterministically answer the question of whether a proposed set coupled with a proposed binary operation forms a group or not.

In the upcoming set of group axioms there will be only *two* axioms - the axiom of associativity of the binary operation at hand and the so-called axiom of *unrestricted group division*.

What does the phrase *unrestricted group division* mean?

The phrase *unrestricted group division* means that:

*in a proposed set coupled with a proposed binary associative operation it is always possible to carry out the inverse operation*

Here, once again, group theorists borrow the relevant terminology from the arithmetic of *numbers* - after importing into the theory of groups and, further, abstracting the operation of *multiplication*, what is the name of the operation that is *inverse* with respect to the said operation of multiplication?

*Division*.

Of course.

Here we go.

The phrase *group division* should, thus, be also understood in a highly abstract fashion as it is a generalization of the operation of division as it applies to *numbers*.

Thus, in the context of the theory of groups the operation of *group division* simply refers to the *inverse of the group operation* regardless of the true underlying nature of the group operation itself.

It may so happen that the group operation is the good old multiplication of (say, non zero rational) numbers and then the operation of group division will indeed correspond to the good old division of (the same non zero rational) numbers.

But, as we by now understand all too well, it may also happen that the group operation is *addition* of (say, whole) numbers and then the operation of group division will correspond to the good old *subtraction* of (the same whole) numbers and so on.

As such, the word *unrestricted* in the phrase *unrestricted group division* simply means that it is *always possible* to carry out the operation of group division or that it is *always possible* to carry out the inverse operation in that particular group - there are no limitations to doing so.

The vague English phrase *always possible* will be given a precise meaning in the wording of the respective axiom.

To that end, let a non-empty set $G$, finite or otherwise, with a single binary operation $\circ$ defined on the elements of that set be given.

Suppose further that the said binary operation coupled with the said set in an order-insensitive fashion satisfies the following *two* axioms.

**Axiom 1** (Associativity): for any three elements $a, b, c$ of the set $G$ the following relationship holds:

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

**Axiom 2** (Group Division): for any two elements $a, b$ of the set $G$ it is always possible to find the elements $x, y$ of the same set $G$ such that the following two relationships hold:

$$a \circ x = b \tag{65}$$

and

$$y \circ a = b \tag{66}$$

**Definition 13** (duplicated for completeness): the given set $G$ with the, single, defined on it binary operation $\circ$ that satisfies the above two axioms is called *a group* and the axioms themselves are called *the group axioms*.

Our objective now is to cultivate the ground for a proof of the upcoming **Theorem 13**, in which we will be tasked with showing that, mainly, from the above *unrestricted group division* **Axiom 2** the existence and uniqueness of the double-sided identity element of a group and the existence and uniqueness of the double-sided inverse for each group element necessarily follows.

## Motivation

We propose to cultivate the ground for the stated purpose by working *in reverse order* with respect to the order in which the causality must flow in the upcoming **Theorem 13**.

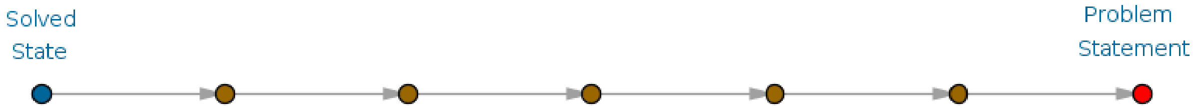
In other words, as a warm up, we would like to take the traditional group axioms of the identity and the inverse elements that we studied so far as a starting point and then we want to attempt to show that given these axioms, the unrestricted group division is always possible.

To elaborate on the idea somewhat.

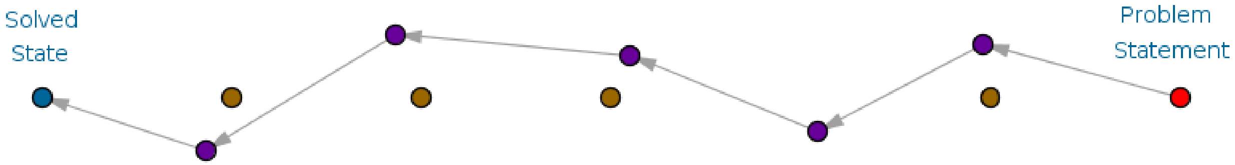
According to the *Reverse-Order* problem-solving approach, we, first and temporarily, assume that a given problem has been solved somehow, how exactly – does not matter at the moment.

After the *problem-has-been-solved* assumption is made, we try to synthesize a string of correct IF P THEN Q implications that originates at or takes the said *solved-state* as the fodder and then, chewing on the intermediate implications, moves toward and, finally, terminates at the original problem statement or the problem's *unsolved* state.

If we were to model such *implications* with *geometric points* and the *flow of causality* with *arrows* or *vectors* then a typical successful journey described above might look as follows (Figure 10.8):



Next, if, starting at the problem's solved state, through a string of correct implications, we manage to arrive at the original problem statement then, as the lightweight problem-solving theory goes, it is plausible that on the said reverse-order journey we may collect enough evidence or enough tactical material that will allow us to construct a successful proof or a computation, as the case may be, as we move in the opposite, forward-order, direction from the problem statement to the solved state (Figure 10.9):



Above, we have changed the color and the arrangement of the forward-order implications because *these* implications are *not* the same implications that we used in our reverse-order reasoning. We have left the reverse-order implications in the diagram above to show that they now play the role of *guiding landmarks* or *lighthouses*.

Note carefully that the forward-order flow of causality is now *flipped* with respect to the reverse-order flow of causality.

For the readers who are not very experienced in the art of problem-solving we would like to stress the point that the above paragraph is full of slippery *sometimes* and *maybes* for a reason - there are no guarantees of any kind here and that is why we referred to the Reverse-Order problem-solving approach as *approach*, for it is not even *a method* and by no means it is *an algorithm*.

In any case, before tackling the theorem that will demonstrate that from the above two axioms the existence of *the identity* and *the inverse* elements necessarily follows, it is a useful exercise to contemplate such a reverse-order deduction of the fact that from the *three* group axioms that we studied so far it follows that the operation of *division* in a group is always possible.

To that end, we ponder.

Hm.

If we were to actually solve the equations (**65**) and (**66**) in the variables $x$ and $y$, then what famous, by now, elements of a group will we have to necessarily deal with?

Well, we already did enough of the relevant group-theoretic manipulations to see that, using the set of group axioms from the Take 1 discussion as a starting point, in order to solve the equation (**65**) in the variable $x$ all we have to do is multiply that equation through *from the left* by the unique element $a^{-1}$, correct?

At that stage, the multiplication from the left is allowed and, by the **Axiom 3**, we know that each element of a group has a unique inverse:

$$a^{-1} \circ a \circ x = a^{-1} \circ b$$

By the **Axiom 1**, we know that the 3-element product above is always well-defined and that we can parenthesize it any which legal way we like:

$$a^{-1} \circ a \circ x = (a^{-1} \circ a) \circ x$$

We also know *the result* of such a left-sided multiplication due to the existence and uniqueness of the double-sided inverse for any group element:

$$a^{-1} \circ a = e$$

which is to say that:

$$a^{-1} \circ a \circ x = (a^{-1} \circ a) \circ x = e \circ x = a^{-1} \circ b$$

But by the **Axiom 2**, we also know *the result* of the next intermediate product due to the existence and uniqueness of the double-sided identity element of a group:

$$e \circ x = x$$

Hence, so far we have:

$$a^{-1} \circ a \circ x = (a^{-1} \circ a) \circ x = e \circ x = x = a^{-1} \circ b$$

and because there were a lot of unique elements involved in such a manipulation, our intuition tells us that the solution $x$ of the equation (**65**) *should be* unique also.

The verification of the fact that the above found $x$ is *a* solution of the equation (**65**) is straightforward:

$$a \circ (a^{-1} \circ b) = (a \circ a^{-1}) \circ b = e \circ b = b$$

Done, via the **Axiom 1**, the **Axiom 3** and the **Axiom 2** (from the **Take 1** section of this chapter).

Likewise, in order to solve the equation (**66**) in the variable $y$ we maneuver in the **right**-sided fashion, which we always can do due to the double-sideness of the group axioms shown in the Take 1 discussion:

$$y \circ a \circ a^{-1} = y \circ (a \circ a^{-1}) = y \circ e = y = b \circ a^{-1}$$

Again, the variable $y$ above can take on one and only one value - we remember that a product of any two group elements is a uniquely defined element of the same group.

Thus, we just have shown that in any group the operation of group division is *always possible*.

Moreover, if we assume for a moment that, say, the equation (**65**) had *two* distinct solutions in $x$, name these solutions as $x_1$ and $x_2$, then, clearly, on the one hand, by the definition of a solution of an equation, it must be the case that:

$$a \circ x_1 = b = a \circ x_2$$

and, on the other hand, we also have:

$$x_1 = a^{-1} \circ a \circ x_1 = a^{-1} \circ b = a^{-1} \circ a \circ x_2 = x_2$$

implying that the solution of the equation (**65**) in the variable $x$ is, indeed, unique:

$$x_1 = x_2$$

Likewise, we show that the solution of the equation (**66**) in the variable $y$ is unique as well:

$$y_1 = y_1 \circ a \circ a^{-1} = b \circ a^{-1} = y_2 \circ a \circ a^{-1} = y_2$$

Thus, we just discovered that not only the operation of division in a group is always possible, but such a division is well-defined, meaning that the solutions of the equations (**65**) and (**66**) in the variables $x$ and $y$ are, respectively, unique.

Technically, here we started with the group axioms shown in the **Take 1** discussion and, using the traditional, forward, flow of causality, we managed to show that in a group the operation of division is always possible.

Folding our find into the shape of an IF P THEN Q implication, we showed that if we are given a group as per the **Take 1** definition then the operation of division in such a group is always possible.

Switching gears, we now want to prove the converse of the above implication:

*if we are given a group as per the above, unrestricted group division, definition then in such a group there must necessarily exist the unique double-sided identity element and the unique double-sided inverses of each element of that group*

where the definitions of what an identity element of a group is and what an inverse of a given group element is is already known to us from the previous four discussions.

To that end, using the insights gained in the above deduction, we, next, change the direction of the flow of causality and treat that deduction as a reverse-order solution of our *current* problem because now we want to make the group division axiom, the **Axiom 2**, our starting point and construct a convincing argument that shows the existence and the uniqueness of the double-sided identity element of a group and of the double-sided inverse of each group element.

However, tactically we only need to show that, say, *a left* identity of a group and *a left* inverse of each group element follows from the current set of group axioms.

Why is that?

Because in the **Take 4** section on this chapter we already proved that under such conditions:

- a left identity element of a group is also its right identity element and
- that a left inverse of a given group element is also a right inverse of that element and

- that the identity and the inverse elements of a group are unique!

Game over - we, thus, can not only witness but experience first-hand how nice it is to have a minimalistic set of the group-formation requirements.

**Theorem 13:** (show that) from the above two group axioms it follows that in a group there exist the identity element and the inverse of each group element and that the said identity and inverse elements are unique and double-sided.

**Proof:** will contain a technical subtlety that we will not spell out initially, hoping that the readers will spot it on their own.

Because the given operation $\circ$ is *binary*, as per **Definition 10**, for every two elements $a, b$ of the given set $G$ there exists an element $c$ of the same set $G$ such that:

$$a \circ b = c$$

Thus, if we choose the elements of the set $G$ as follows: $a = e, b = a$ and $c = a$ then it is actually already given to us that an element $e$ of $G$ such that:

$$e \circ a = a$$

exists.

Commentary: or does it? In other words, did you notice what just transpired here?

What just transpired here is the following: we *assumed* that the set $G$ at hand *has at least one element in it*.

But is such an assumption valid?

In order to make sure that it is, we opened this discussion with the requirement that the candidate set $G$ is *not empty* and, thus, contains at least one element.

The million-dollar question now is whether the element $e$ is actually *a left identity* of a group?

This is where potentially we could run into a dead end in our proof if we were to try to work with a product like $e \cdot b$ because such a product is only useful tactically if the element $e$ is followed by the element $a$.

That is why it is advantageous to replace a monolithic object, the group element named $b$, with a compound object, a group product where the element $a$ sits to the left of anything that follows it:

$$a \circ x = b$$

and then we quickly gain the needed traction with the proof:

$$e \circ b = e \circ (a \circ x)$$

By the **Axiom 1**, we can change the order in which the factors in the above string of group multiplications are combined:

$$e \circ b = e \circ (a \circ x) = (e \circ a) \circ x = a \circ x = b$$

which is to say that $e$ is indeed *a left identity* element of a group.

We can now show that in that group there must exist *a left inverse* for each group element.

Namely, by the **Axiom 2**, since the operation of division in a group is always possible, it follows that for the elements $e$ and $a$ of a group there always exists an element $y$ such that:

$$y \circ a = e$$

and that element $y$ plays the role of *a left inverse* of the element $a$.

But, thanks to the **Take 4** discussion, we already know that under such conditions:

- a left identity element of a group is also its right identity and
- that a left inverse of a given group element is also a right inverse of that element and
- that the identity and inverse elements of a group are unique

which completes this proof. □

We now feel that the following ideas are floating in the air.

In a group, in certain equations, it is always possible to *cancel* the same element from *the left* - if, for the elements $a, p, q$ of a group, it is the case that:

$$a \circ p = a \circ q$$

then it is also the case that:

$$p = q$$

Such a possibility is known as *the left cancellation law.*

Likewise, in a group, in certain equations, it is always possible to *cancel* the same element from *the right* - if, for the elements $b, u, v$ of a group, it is the case that:

$$u \circ b = v \circ b$$

then it is also the case that:

$$u = v$$

Such a possibility is known as *the right cancellation law* and so on.

We will generate the relevant proofs of these laws in the upcoming exercises.

Admittedly, generating the correct mathematical proofs is a skill that demands care, patience, attention, creativity, ingenuity and time.

On the one hand, asking the newcomers to generate such proofs right away in a such a discipline as the theory of groups is, no doubt, a tall order.

On the other hand, one of the best ways to understand a particular fact in mathematics is either to generate your own *proof* of that fact or to simply comprehend a proof of the said fact generated by someone else. Either way, it is the proof that reveals or should reveal the essence of the local goings on.

We hope that the five different versions of the group axioms presented in this chapter and the accompanying proofs will help the readers settle the foundational matters of the theory of groups in their mind eventually - let these ideas cook, boil and simmer for a while. In addition, we hope that these discussions explain why most modern textbooks only show the version of the group axioms covered in the **Take 1** section.

We are now ready to connect the newly developed theory with practice by honing the group-detection skill.

As a fair warning, none of the upcoming exercises will be phrased as:

- *show that the candidate pair* $\langle G; \circ \rangle$ *is a group*

On the contrary, all the upcoming exercises will be phrased as:

- *you tell us whether the proposed candidate pair* $\langle G; \circ \rangle$ *is or is not a group*

By solving the exercises whose problem statements are formulated in the *you tell us* fashion, we will be reasoning from first principles and analyzing each and every problem from square one, anew.