

5.3 Binary Operations

Sections 5.1 and 5.2 built new functions from old ones by cutting, gluing and factoring. This section looks at functions of a special shape: functions that take two elements of a set and return a third element of the same set, such as $+$ on $\mathbb{Z}$, $\cup$ on $\mathcal{P}(X)$ and $\circ$ on the functions from a set to itself. We name the properties such an operation may have, one at a time, and ask what each property buys on its own. The central answers, uniqueness of identities and of inverses, are short proofs by one method, computing a single expression in two ways; the rest are proved by checking candidates. All of them work at once for numbers, for sets, for functions and for the hours of the clock.

5.3.1 Brackets

Nobody writes brackets in $2 + 3 + 4$: whether we add $2 + 3$ first or $3 + 4$ first, the answer is 9. Subtraction is different. Reading $2 - 3 - 4$ from the left gives $(2 - 3) - 4 = -5$, and from the right gives $2 - (3 - 4) = 3$. Powers behave like subtraction: $2^{(3^2)} = 2^9 = 512$, while $(2^3)^2 = 8^2 = 64$. School arithmetic settles this by convention (subtraction from the left, towers of powers from the top), and a convention is needed exactly because the bracketing changes the answer.

The same questions arise far from numbers. For subsets of a set X , is $(A \cup B) \cup C$ the same set as $A \cup (B \cup C)$? For functions from X to itself, is $h \circ (g \circ f)$ the same function as $(h \circ g) \circ f$? On the clock $\mathbb{Z}/12$ of Section 4.2, is there an hour that changes nothing when added, as 0 does for integers, and can every hour be undone?

Each of these questions asks whether some rule of arithmetic holds for some way of combining two things into a third. The aim of this section is to separate the rules and to find out what each rule gives on its own. Here is a test question to keep in mind: can a set with an operation have two different elements that both behave like 0? For $+$ on $\mathbb{Z}$ the answer seems obvious, but the reason is not; the answer comes in the subsection “One identity, one inverse”.

5.3.2 Operations

The first thing to fix is what counts as a way of combining two things. Two natural candidates fail. Subtraction on $\mathbb{N}$ takes the pair $(2, 3) \in \mathbb{N} \times \mathbb{N}$ to -1 , which is not in $\mathbb{N}$. Division on $\mathbb{R}$ has no value at all at the pair $(1, 0)$. The first fails because a value leaves the set; the second fails because a pair has no value. A way of combining must give **every** pair a value, and the value must lie **in the set**. Those are the two halves of being a function with domain $X \times X$ and codomain X (Definition 1.5.1).

An operation on a set combines any two of its elements into a third element of the same set.

Definition 5.3.1. Binary Operation

Let X be a set. A **binary operation** on X , or an **operation** on X , is a function

$$*: X \times X \rightarrow X.$$

Its value at (x, y) is written $x * y$ rather than $*(x, y)$.

A subset $A \subseteq X$ is **closed** under $*$ if $a * b \in A$ **for all** $a, b \in A$.

In words: the definition asks for a function, so each pair (x, y) of elements of X , in this order,

has **exactly one** value, and that value lies in X . The order matters, since (x, y) and (y, x) are different pairs and may have different values; $2 - 3 \neq 3 - 2$. The letter $*$ is a name for the operation, like f for a function. In examples it is replaced by a familiar symbol, $+$, $\cdot$, $\cup$, $\circ$.

If A is closed under $*$, then the restriction of $*$ to $A \times A$, with codomain A , is an operation on A : restriction to a subset of the domain (Definition 5.1.1) gives a function $A \times A \rightarrow X$, and closure says its values lie in A , so A may serve as the codomain. We keep the symbol $*$ for the restricted operation.

Example. Operations

Decide which of the following are operations on the set named, and which subsets named are closed.

- (a) $+$, $\cdot$ and $-$ on $\mathbb{Z}$; the average $x * y := (x + y)/2$ and $\max$ on $\mathbb{R}$.
- (b) $\cup$, $\cap$ and the symmetric difference $\triangle$ of Section 5.1 on $\mathcal{P}(X)$.
- (c) Composition $\circ$ on X^X , the set of all functions $X \rightarrow X$.
- (d) $[a] + [b] := [a + b]$ and $[a][b] := [ab]$ on $\mathbb{Z}/n$, for $n \in \mathbb{Z}_{>0}$.
- (e) Division $(x, y) \mapsto x/y$ on $\mathbb{R} \setminus \{0\}$; and the subset $\mathbb{Z}_{>0}$ of $\mathbb{Z}$, under $+$ and under $-$.

Solution.

- (a) Each rule gives every pair of integers one integer, and every pair of reals one real, so each is an operation. The average is an operation on $\mathbb{R}$ but not on $\mathbb{Z}$: $(0 + 1)/2 \notin \mathbb{Z}$.
- (b) For $A, B \subseteq X$, the sets $A \cup B$, $A \cap B$ and $A \triangle B$ are again subsets of X (Definition 1.3.1), so each is an operation on $\mathcal{P}(X)$.
- (c) For $f, g \in X^X$, the composite $g \circ f$ is a function $X \rightarrow X$ (Definition 1.5.2), so $(g, f) \mapsto g \circ f$ is an operation on X^X .
- (d) Both rules read representatives of classes; Proposition 4.2.5 proved that they are well defined, that is, that each pair of classes gets exactly one class. So both are operations on $\mathbb{Z}/n$.
- (e) If $x, y \neq 0$, then x/y is defined and $x/y \neq 0$, so division is an operation on $\mathbb{R} \setminus \{0\}$. The positive integers are closed under $+$, since a sum of positive integers is positive. They are not closed under $-$: $1, 2 \in \mathbb{Z}_{>0}$, and $1 - 2 = -1 \notin \mathbb{Z}_{>0}$.

Part (d) is the reason this section returns to quotients at its end: an operation on classes is a rule on representatives together with a proof of well-definedness. Part (e) shows that a rule that fails on one set may succeed on a smaller one; the pairs that caused trouble for division, those with second entry 0, have been removed.

Quick check. Is $(A, B) \mapsto A \setminus B$ an operation on $\mathcal{P}(X)$? Are the even integers closed under $+$? The odd integers?

Solution. Yes: for $A, B \subseteq X$, $A \setminus B \subseteq A \subseteq X$, so the value lies in $\mathcal{P}(X)$. Yes: $2k + 2l = 2(k + l)$. No: 1 is odd and $1 + 1 = 2$ is not.

5.3.3 Properties

The questions of the hook are now questions about an operation $*$ on a set X . Each asks whether an equation holds for every choice of elements, or whether some element has a special behavior.

Definition 5.3.2. Associative, Commutative, Identity, Inverse

Let $*$ be an operation on a set X .

- (a) $*$ is **associative** if $(x * y) * z = x * (y * z)$ **for all** $x, y, z \in X$.
- (b) $*$ is **commutative** if $x * y = y * x$ **for all** $x, y \in X$.
- (c) An element $e \in X$ is a **left identity** of $*$ if $e * x = x$ **for every** $x \in X$; a **right identity** if $x * e = x$ **for every** $x \in X$; and an **identity** if it is both.
- (d) Suppose $*$ has an identity e , and let $x \in X$. An element $y \in X$ is an **inverse** of x if $x * y = e$ **and** $y * x = e$. The element x is **invertible** if it has an inverse.

In words: associativity says brackets may be moved; commutativity says the two inputs may be swapped. A left or right identity is an element that changes nothing, from the side named; an identity must change nothing from **both** sides and must do so for **every** element. An inverse of x undoes x , again from both sides, and it is defined only relative to an identity. Clause (d) says “an inverse”, not “the inverse”: nothing in the definition says there is only one.

For $+$ on $\mathbb{Z}$, all four hold: $+$ is associative and commutative, 0 is an identity, and $-x$ is an inverse of x . For $\cdot$ on $\mathbb{Z}$, 1 is an identity, and only 1 and -1 are invertible. For $\cup$ on $\mathcal{P}(X)$, $\emptyset$ is an identity, since $\emptyset \cup A = A = A \cup \emptyset$.

Deciding whether an operation has a property is the work of Section 4.1’s method for relations (Example (Method: proving or disproving a property of a relation)): a property that says “for all” is proved by taking arbitrary elements, and a failure needs one witness, checked. For an identity the quantifiers are the other way round, “there is an e such that for every x ”, so a proof names one e and checks it against every x , and a refutation must show that **every** candidate e fails at some x .

Example. A right identity that is not an identity

Decide whether subtraction on $\mathbb{Z}$ is associative, and find its left and right identities.

Solution. Not associative. The triple $2, 3, 4$ of the hook is a witness: $(2 - 3) - 4 = -5$ and $2 - (3 - 4) = 3$.

A right identity. For every $x \in \mathbb{Z}$, $x - 0 = x$, so 0 is a right identity.

Not a left identity. $0 - 1 = -1 \neq 1$, so 0 fails at $x = 1$.

No left identity at all. Suppose e is a left identity, so $e - x = x$ for every $x \in \mathbb{Z}$. At $x = 0$ this gives $e = 0$; at $x = 1$ it gives $e - 1 = 1$, so $e = 2$. Then $0 = 2$, which is false. So no integer is a left identity, and subtraction has no identity.

The refutation of “there is a left identity” did not test candidates one by one. It assumed a left identity e , used the hypothesis “for every x ” at two well-chosen values of x , and reached two incompatible values for e .

Quick check. Is the average $x * y := (x + y)/2$ on $\mathbb{R}$ associative? Is it commutative? Has it an identity?

Solution. Not associative: $(0 * 0) * 4 = 0 * 4 = 2$, while $0 * (0 * 4) = 0 * 2 = 1$. Commutative: $(x + y)/2 = (y + x)/2$. No identity: if $(e + x)/2 = x$ for every x , then $e = x$ for every $x \in \mathbb{R}$, so $e = 0$ and $e = 1$, which is false.

Quick check. Consider $\max$ on $\mathbb{N}$ and $\max$ on $\mathbb{Z}$. Is each associative? Commutative? Has it an identity?

Solution. Both are associative, since $\max(\max(x, y), z)$ and $\max(x, \max(y, z))$ are both the largest of x, y, z , and both are commutative. On $\mathbb{N}$, 0 is an identity: $\max(0, x) = x = \max(x, 0)$ since $x \geq 0$. On $\mathbb{Z}$ there is none: an identity e would need $\max(e, e - 1) = e - 1$, but $\max(e, e - 1) = e$. The same rule, on a larger set, loses its identity.

5.3.4 One identity, one inverse

Back to the test question of the hook. An operation may have several left identities: for $x * y := y$ on a set with two elements, every element is a left identity (Exercise A1 (c)). But an element that is an identity from both sides is never shared.

Proposition 5.3.1. An Identity Is Unique

Let $*$ be an operation on a set X . If e is a left identity and e' is a right identity of $*$, then $e = e'$. In particular, $*$ has at most one identity.

Idea (Scratch work). Two candidates, so this is the uniqueness half of Example (Method: existence and uniqueness): two names, about which we know only the defining equations, to be shown equal. The givens are equations about products; the goal mentions no product at all. The gap is to find one product that both givens can simplify.

Givens	Goal
$e * x = x$ for every $x \in X$; $x * e' = x$ for every $x \in X$	$e = e'$
the givens speak about products; the goal about two elements	one product that each given simplifies
the product $e * e'$: the first given at $x = e'$ makes it e' ; the second at $x = e$ makes it e	$e = e * e' = e'$

The last row closes the gap: the product $e * e'$, with one candidate on each side, is the expression both givens can reach.

Proof. Since e' is a right identity, the case $x = e$ of its defining equation gives $e * e' = e$. Since e is a left identity, the case $x = e'$ gives $e * e' = e'$. Hence $e = e * e' = e'$.

If e and e' are both identities, then e is a left identity and e' a right identity, so $e = e'$. This proves the proposition. ■

Neither associativity nor commutativity was used: the proof applies two hypotheses once each, to the single product $e * e'$. So the answer to the test question is no, for every operation whatsoever. Because of the proposition, we may speak of **the** identity of $*$ when there is one.

The proof is an instance of a move that runs through this section and the next.

Example. Method: compute one expression in two ways

Template. To prove $a = b$ when a and b are known only through equations: (1) find one expression m that the equations about a reduce to a , and the equations about b reduce to b ; (2) write the chain $a = \dots = m = \dots = b$, citing a hypothesis at each “=”.

When to use it. Uniqueness of identities and of inverses, cancellation, and any goal equating two objects given by equations.

The usual failure. Assuming $a = b$ somewhere in the chain (entry (N9) of Logic and Proof, Example (What is not allowed)); using associativity or commutativity that was not given; a bracket moved silently.

Inverses are the second test of the method. Here associativity is needed, and the proof shows exactly where.

Proposition 5.3.2. Inverses Are Unique for an Associative Operation

Let $*$ be an associative operation on a set X with identity e , and let $x \in X$. If $y * x = e$ and $x * z = e$, then $y = z$. In particular, x has at most one inverse.

Idea. As in [Example \(Method: compute one expression in two ways\)](#). The expression is $m = (y * x) * z$, which is also $y * (x * z)$ by associativity: bracketed as written it is $e * z = z$, and regrouped it is $y * e = y$. Associativity is exactly the license to read it both ways.

Proof. Using that e is an identity, then $x * z = e$, then associativity, then $y * x = e$, and finally that e is an identity again:

$$y = y * e = y * (x * z) = (y * x) * z = e * z = z.$$

If y and z are both inverses of x , then in particular $y * x = e$ and $x * z = e$, so $y = z$. This proves the proposition. ■

For an associative operation with identity, the inverse of an invertible x is therefore unique, and we write it x^{-1} . For an operation written $+$, the inverse is written $-x$ instead. The proposition is a little stronger than uniqueness: an element x with some y such that $y * x = e$ and some z such that $x * z = e$ has $y = z$, and then y is an inverse of x , so x is invertible. This is the same computation as Proposition 1.6.3 for functions, now done for any associative operation.

Without associativity the conclusion can fail, and a three-element table shows it.

Example. Without associativity, two inverses

Let $X = \{e, a, b\}$ with three different elements, and define $*$ by the table below: the entry in row u and column v is $u * v$.

$*$	e	a	b
e	e	a	b
a	a	e	e
b	b	e	e

Show that $*$ is a commutative operation with identity e , that a has two different inverses, and that $*$ is not associative.

Solution. The table gives each of the nine pairs exactly one value in X , so $*$ is an operation on X . The table is symmetric about its diagonal, which says $u * v = v * u$ for all u, v : $*$ is commutative. The row and the column of e repeat the headings, so $e * u = u = u * e$ for every u : e is the identity.

Since $a * a = e$, the element a is an inverse of itself; since $a * b = e = b * a$, the element b is another inverse of a , and $a \neq b$.

Finally, $(a * a) * b = e * b = b$, while $a * (a * b) = a * e = a$. These differ, so $*$ is not associative.

The last line is Proposition 5.3.2's chain, run on $y = a$, $x = a$, $z = b$, breaking at the one step that used associativity.

With uniqueness in hand, the rules that school algebra uses for inverses of numbers can be proved for any associative operation. The method for each is the same: name a candidate, check it on both sides, and let uniqueness do the rest.

Proposition 5.3.3. Inverses of Products

Let $*$ be an associative operation on a set X with identity e .

- (a) e is invertible, and $e^{-1} = e$.
- (b) If x is invertible, then so is x^{-1} , and $(x^{-1})^{-1} = x$.
- (c) If x and y are invertible, then so is $x * y$, and $(x * y)^{-1} = y^{-1} * x^{-1}$.

Idea. Each part names a candidate and checks it, which is the existence half of Example (Method: existence and uniqueness); uniqueness was proved once and for all in Proposi-

tion 5.3.2. For (c) the candidate is found by asking what undoes $x * y$: first remove y , then x .

Proof. In each part we show that the candidate is an inverse by checking both equations of Definition 5.3.2 (d); then it is **the** inverse by Proposition 5.3.2.

(a) $e * e = e$, since e is an identity, and this one equation is both required equations.

(b) The two equations $x * x^{-1} = e$ and $x^{-1} * x = e$, which say that x^{-1} is an inverse of x , also say that x is an inverse of x^{-1} .

(c) Using associativity twice to regroup, then the defining equation of y^{-1} , the identity, and the defining equation of x^{-1} :

$$\begin{aligned} (x * y) * (y^{-1} * x^{-1}) &= x * (y * (y^{-1} * x^{-1})) = x * ((y * y^{-1}) * x^{-1}) \\ &= x * (e * x^{-1}) = x * x^{-1} = e. \end{aligned}$$

In the same way, $(y^{-1} * x^{-1}) * (x * y) = y^{-1} * (x^{-1} * (x * y)) = y^{-1} * ((x^{-1} * x) * y) = y^{-1} * (e * y) = y^{-1} * y = e$. This proves the proposition. ■

In (c) the order reverses: to undo “first x , then y ”, one undoes y first. The display moved brackets one step at a time; Exercise C1 shows that for four factors every bracketing gives the same element.

Quick check. Which elements of $\mathcal{P}(X)$ are invertible under $\cup$? Which are invertible under Δ ?

Solution. Both operations have identity $\emptyset$: $A \cup \emptyset = A$, and $A \Delta \emptyset = (A \setminus \emptyset) \cup (\emptyset \setminus A) = A$ and $\emptyset \Delta A = (\emptyset \setminus A) \cup (A \setminus \emptyset) = A$. Under $\cup$, if $A \cup B = \emptyset$, then $A \subseteq A \cup B = \emptyset$, so $A = \emptyset$: only $\emptyset$ is invertible. Under Δ , $A \Delta A = (A \setminus A) \cup (A \setminus A) = \emptyset$, so every A is invertible and is its own inverse.

5.3.5 Operations on functions

An operation on a set Y gives an operation on every set of functions into Y , by combining values point by point. This is how $f + g$ and $f \cdot g$ are defined for real functions, and it carries each property of the operation on Y over to the functions.

Proposition 5.3.4. Pointwise Operations

Let $*$ be an operation on a set Y , and let X be a set. For $f, g \in Y^X$, define $f * g: X \rightarrow Y$ by

$$(f * g)(x) := f(x) * g(x) \quad (x \in X).$$

This is an operation on Y^X , the **pointwise** operation, and:

- (a) if $*$ is associative, or commutative, on Y , then so is the pointwise operation on Y^X ;
- (b) if e is an identity of $*$, then the constant function $c_e: X \rightarrow Y, x \mapsto e$, is an identity of the pointwise operation;
- (c) if $*$ is associative with identity e , then $f \in Y^X$ is invertible if and only if every value $f(x)$ is invertible in Y , and then the inverse of f is $x \mapsto f(x)^{-1}$.

Idea. An equation between functions is checked value by value (Proposition 1.5.1), and at the point x each law for the pointwise operation is the same law for $*$, applied to the values $f(x), g(x), h(x)$.

Proof. For $x \in X$, the value $f(x) * g(x)$ is one element of Y , so $f * g$ is a function $X \rightarrow Y$, and $(f, g) \mapsto f * g$ is an operation on Y^X . Each equation below is between functions $X \rightarrow Y$, so by Proposition 1.5.1 it suffices to compare values at an arbitrary $x \in X$.

(a) By the definition, used twice on each side, and associativity in Y ,

$$((f * g) * h)(x) = (f(x) * g(x)) * h(x) = f(x) * (g(x) * h(x)) = (f * (g * h))(x).$$

Likewise $(f * g)(x) = f(x) * g(x) = g(x) * f(x) = (g * f)(x)$ when $*$ is commutative.

(b) $(c_e * f)(x) = e * f(x) = f(x)$ and $(f * c_e)(x) = f(x) * e = f(x)$.

(c) $(\Rightarrow)$ Let g be an inverse of f , so $f * g = c_e = g * f$, the identity being c_e by (b) and Proposition 5.3.1. Evaluating at x gives $f(x) * g(x) = e = g(x) * f(x)$, so $g(x)$ is an inverse of $f(x)$. $(\Leftarrow)$ If every $f(x)$ is invertible, its inverse $f(x)^{-1}$ is unique (Proposition 5.3.2), so $g(x) := f(x)^{-1}$ defines a function $g: X \rightarrow Y$. Then $(f * g)(x) = f(x) * f(x)^{-1} = e = c_e(x)$, and likewise $(g * f)(x) = e$, so g is an inverse of f . The pointwise operation is associative by (a), so this inverse is the only one, by Proposition 5.3.2. This proves the proposition. ■

Part (c) needs every value to be invertible, not just most of them. On $\mathbb{R}^{\mathbb{R}}$ with pointwise $\cdot$, the identity is the constant c_1 ; the function $x \mapsto x$ is not invertible, because its value at 0 has no multiplicative inverse, although every other value has one.

Warning (Iterate or product?). On $\mathbb{R}^{\mathbb{R}}$ the symbol f^2 could mean two different functions: the pointwise product $x \mapsto f(x) \cdot f(x)$, or the composite $f \circ f$. For $f(x) = x + 1$ the first is $x \mapsto (x + 1)^2$ and the second is $x \mapsto x + 2$. In this book f^n always means the n -th iterate, f composed with itself n times, defined in Section 5.4. A pointwise product is written $f \cdot g$, and a pointwise power is written out, $x \mapsto f(x)^n$. For the same reason f^{-1} standing alone always means the inverse function, while $f^{-1}(B)$ for a set B is still the preimage of Definition 1.7.2, defined for every f ; the inverse of f under pointwise $\cdot$, when it exists, is written $x \mapsto 1/f(x)$.

Indicators are a first instance. The set $\{0, 1\}$ is closed under multiplication of numbers, so $\cdot$ is an operation on $\{0, 1\}$, and pointwise multiplication is an operation on $\{0, 1\}^X$. By Proposition 5.1.3 (a), $\mathbf{1}_A \cdot \mathbf{1}_B = \mathbf{1}_{A \cap B}$: on indicators, the pointwise product is intersection. The identity of pointwise $\cdot$ is the constant function c_1 , which is $\mathbf{1}_X$, matching $X \cap A = A$ for $A \subseteq X$.

The second instance is composition. On X^X , any two functions can be composed in either order, and composition is an operation (Example (Operations) (c)).

Proposition 5.3.5. Composition on X^X

Let X be a set. Composition $(g, f) \mapsto g \circ f$ is an associative operation on X^X with identity id_X . An element $f \in X^X$ is invertible under $\circ$ if and only if f is bijective, and then its inverse under $\circ$ is the inverse function f^{-1} . If X has two different elements, then $\circ$ is not commutative on X^X .

Proof. Associativity and $f \circ \text{id}_X = f = \text{id}_X \circ f$ are Proposition 1.5.3, with all four sets equal to X . Under $\circ$, an inverse of f in the sense of Definition 5.3.2 (d) is a $g \in X^X$ with $f \circ g = \text{id}_X = g \circ f$, which is exactly a two-sided inverse of f in the sense of Definition 1.6.2. By Theorem 1.6.4, f has one if and only if f is bijective, and it is then the inverse function f^{-1} , which is unique by Proposition 1.6.3.

Now let $a, b \in X$ with $a \neq b$, and let $c_a, c_b \in X^X$ be the constant functions with values a and b . For every $x \in X$, $(c_a \circ c_b)(x) = c_a(b) = a$ and $(c_b \circ c_a)(x) = c_b(a) = b$. So $c_a \circ c_b = c_a$ and $c_b \circ c_a = c_b$, and these differ, since their values at a differ (Proposition 1.5.1). This proves the proposition. ■

So the invertible elements of X^X under composition are exactly the bijections from X to itself, the subject of Section 5.4. For them, Proposition 5.3.3 (c) says $(g \circ f)^{-1} = f^{-1} \circ g^{-1}$. That rule appeared as Exercise B2 of Section 1.6 (Exercise (B2: The inverse of a composite)); here it is proved once, for every associative operation, and the rule for bijections of a set to itself is one case of it (Exercise B2 of Section 1.6 allows three different sets).

Quick check. In $\mathbb{R}^{\mathbb{R}}$, find the inverse of $f(x) = 2x + 1$ under composition, and its inverse under pointwise $+$.

Solution. Under $\circ$: $g(x) = (x - 1)/2$, since $f(g(x)) = (x - 1) + 1 = x$ and $g(f(x)) = (2x + 1 - 1)/2 = x$. Under pointwise $+$, whose identity is the constant c_0 : $x \mapsto -2x - 1$, since $(2x + 1) + (-2x - 1) = 0$. The two inverses are different functions; “the inverse” always names its operation.

5.3.6 Operations on a quotient

The clock adds hours, and Section 4.2 checked that the addition is well defined (Proposition 4.2.5). Every operation that respects an equivalence relation passes to the quotient in the same way, and it takes its properties with it.

Proposition 5.3.6. Operations on a Quotient

Let $*$ be an operation on a set X , and let $\sim$ be an equivalence relation on X such that, for

all $x, x', y, y' \in X$,

$$x \sim x' \text{ and } y \sim y' \implies x * y \sim x' * y'.$$

Then $[x] * [y] := [x * y]$ is a well-defined operation on $X/\sim$, and the quotient map satisfies $q(x * y) = q(x) * q(y)$. Moreover:

- (a) if $*$ is associative, or commutative, then so is the operation on $X/\sim$;
- (b) if e is an identity of $*$, then $[e]$ is an identity of the operation on $X/\sim$;
- (c) if y is an inverse of x , then $[y]$ is an inverse of $[x]$.

Idea. As in Example (Method: define a function on a quotient), the rule computes a value from representatives, so the one thing to check is that the value does not depend on them (Example (Method: checking that a definition on classes is well defined)); here there are two representatives to change, and the hypothesis on $\sim$ handles both at once. Each law then holds for classes because it holds for representatives, and every class has one.

Proof. Well defined. Every class is $[x]$ for some $x \in X$ (Definition 4.2.4), so the rule gives every pair of classes a value, and the value $[x * y]$ lies in $X/\sim$. Let $[x] = [x']$ and $[y] = [y']$. By Theorem 4.2.1 (b), $x \sim x'$ and $y \sim y'$, so $x * y \sim x' * y'$ by hypothesis, and $[x * y] = [x' * y']$ by Theorem 4.2.1 (b) again. So the value does not depend on the representatives, and $*$ is an operation on $X/\sim$. The equation $q(x * y) = [x * y] = [x] * [y] = q(x) * q(y)$ is the definition.

(a) Let three classes be given, with representatives x, y, z . Applying the definition twice on each side and associativity in X ,

$$([x] * [y]) * [z] = [(x * y) * z] = [x * (y * z)] = [x] * ([y] * [z]).$$

Likewise $[x] * [y] = [x * y] = [y * x] = [y] * [x]$ when $*$ is commutative.

(b) $[e] * [x] = [e * x] = [x]$ and $[x] * [e] = [x * e] = [x]$, for every class $[x]$.

(c) $[x] * [y] = [x * y] = [e]$ and $[y] * [x] = [y * x] = [e]$, and $[e]$ is the identity by (b). This proves the proposition. ■

The hypothesis on $\sim$ is the whole content: it says that $*$ does not see the difference between equivalent elements. For $\mathbb{Z}$ with congruence modulo n , it is exactly Proposition 4.2.5, for $+$ and for $\cdot$. So $\mathbb{Z}/n$ inherits from $\mathbb{Z}$: addition is associative and commutative with identity $[0]$, every class $[a]$ has the inverse $[-a]$ and we write $-[a] = [-a]$, and multiplication is associative and commutative with identity $[1]$. On the clock, $[9] + [3] = [12] = [0]$, so $-[9] = [3]$: the hour that undoes nine hours is three hours.

Part (c) goes one way only. The quotient can have inverses that X lacks: in $\mathbb{Z}/3$, $[2][2] = [4] = [1]$, so $[2]$ is invertible under multiplication, while no integer y has $2y = 1$, since 1 is odd.

5.3.7 Exercises

5.3.7.1 A. Check your understanding

Exercise. A1

- (a) Which of the following are operations: subtraction on $\mathbb{N}$; subtraction on $\mathbb{Z}$; $(x, y) \mapsto x/y$ on $\mathbb{R} \setminus \{0\}$; $(x, y) \mapsto x/y$ on $\mathbb{Z} \setminus \{0\}$?
- (b) Write the table of $+$ on $\mathbb{Z}/3 = \{[0], [1], [2]\}$. Find the identity and the inverse of each class.
- (c) Let X be a set with at least two elements, and let $x * y := y$. Find all left identities and all right identities of $*$.
- (d) State the template of the method of computing one expression in two ways, and say which expression it computes in the proof of [Proposition 5.3.2](#).

Solution.

- (a) Subtraction on $\mathbb{N}$: no, $2 - 3 = -1 \notin \mathbb{N}$. Subtraction on $\mathbb{Z}$: yes. Division on $\mathbb{R} \setminus \{0\}$: yes, since x/y is defined and non-zero for $x, y \neq 0$. Division on $\mathbb{Z} \setminus \{0\}$: no, $1/2 \notin \mathbb{Z}$.
- (b) By the rule $[a] + [b] = [a + b]$, reducing with Proposition 4.2.4 ($[3] = [0]$, $[4] = [1]$):

$+$	$[0]$	$[1]$	$[2]$
$[0]$	$[0]$	$[1]$	$[2]$
$[1]$	$[1]$	$[2]$	$[0]$
$[2]$	$[2]$	$[0]$	$[1]$

The row and column of $[0]$ repeat the headings, so $[0]$ is the identity. Reading off the entries $[0]$: $-[0] = [0]$, $-[1] = [2]$, $-[2] = [1]$.

- (c) Every $e \in X$ is a left identity, since $e * y = y$ for every y . No element is a right identity: for $e \in X$, pick $x \in X$ with $x \neq e$ (there is one, since X has at least two elements); then $x * e = e \neq x$. So left identities need not be unique when there is no right identity; [Proposition 5.3.1](#) needs one of each.
- (d) To prove $a = b$ for objects known only through equations, find one expression that the equations about a reduce to a and those about b reduce to b , and write $a = \dots = m = \dots = b$ with a reason at each step ([Example \(Method: compute one expression in two ways\)](#)). In [Proposition 5.3.2](#) the expression is $(y * x) * z$, which equals z as written and, regrouped as $y * (x * z)$, equals y .

5.3.7.2 B. Practice**Exercise. B1: Deciding properties**

On $\mathbb{R}$, let $x * y := x + y - xy$. Determine whether $*$ is associative and whether it is commutative, find its identity, and find which elements are invertible, with their inverses. Justify your answer.

Solution. Associative. Expanding both sides,

$$\begin{aligned}(x * y) * z &= (x + y - xy) + z - (x + y - xy)z \\ &= x + y + z - xy - xz - yz + xyz, \\ x * (y * z) &= x + (y + z - yz) - x(y + z - yz) \\ &= x + y + z - xy - xz - yz + xyz.\end{aligned}$$

The two results agree, so $*$ is associative. (Both are unchanged by any rearrangement of x, y, z .)

Commutative. $x + y - xy = y + x - yx$.

Identity. $0 * x = 0 + x - 0 = x$, and $x * 0 = x$ by commutativity; so 0 is the identity, unique by [Proposition 5.3.1](#).

Inverses. We need y with $x + y - xy = 0$ (the other side follows by commutativity), that is, $y(1 - x) = -x$. If $x \neq 1$, this has the solution $y = x/(x - 1)$: indeed $x + \frac{x}{x-1} - \frac{x^2}{x-1} = \frac{x(x-1)+x-x^2}{x-1} = 0$. If $x = 1$, then $1 * y = 1 + y - y = 1 \neq 0$ for every y , so 1 has no inverse. So every $x \neq 1$ is invertible, with inverse $x/(x - 1)$ under $*$, and 1 is not.

A remark. $1 - x * y = (1 - x)(1 - y)$. For $u, v \in \{0, 1\}$, $u * v = u + v - uv$ is the indicator rule for a union, [Proposition 5.1.3 \(c\)](#): $\mathbf{1}_{A \cup B}(x) = \mathbf{1}_A(x) * \mathbf{1}_B(x)$.

Exercise. B2: Every square is the identity

Let $*$ be an associative operation on a set X with identity e , such that $x * x = e$ for every $x \in X$. Prove that $*$ is commutative. Check the hypothesis for Δ on $\mathcal{P}(X)$.

Solution. Let $x \in X$. The equation $x * x = e$ says that x is an inverse of itself, from both sides; by [Proposition 5.3.2](#), $x^{-1} = x$. Now let $x, y \in X$. By the hypothesis applied to $x * y$, and by [Proposition 5.3.3 \(c\)](#),

$$x * y = (x * y)^{-1} = y^{-1} * x^{-1} = y * x.$$

For Δ : it is associative (Example (Symmetric difference is associative)) with identity $\emptyset$, and $A \Delta A = \emptyset$ for every $A \subseteq X$ (the Quick check after [Proposition 5.3.3](#)). So Δ is commutative, which can also be read off its definition, since $(A \setminus B) \cup (B \setminus A)$ is symmetric in A and B .

Exercise. B3: Two kinds of inverse

In $\mathbb{R}^{\mathbb{R}}$, find, if they exist, the inverses of $f(x) = x^3 + 1$ under composition and under pointwise $+$, and the inverses of $g(x) = x^2$ under composition and under pointwise $\cdot$. Justify each answer.

Solution. f under $\circ$. Let $h(x) := \sqrt[3]{x - 1}$, the real cube root. Then $f(h(x)) = (x - 1) + 1 = x$ and $h(f(x)) = \sqrt[3]{x^3} = x$, so h is the inverse ([Proposition 5.3.5](#)).

f under $+$. The identity is c_0 , and $x \mapsto -x^3 - 1$ is the inverse: $(x^3 + 1) + (-x^3 - 1) = 0$ at

every x (Proposition 5.3.4 (c)).

g under $\circ$. None: $g(1) = 1 = g(-1)$, so g is not injective, hence not bijective, hence not invertible under $\circ$ by Proposition 5.3.5.

g under $\cdot$. None: the value $g(0) = 0$ has no inverse under multiplication of reals ($0 \cdot y = 0 \neq 1$), so by Proposition 5.3.4 (c) g is not invertible.

Exercise. B4: Prove or disprove

Prove or disprove each statement. Throughout, $*$ is an operation on a set X .

- (a) Every left identity of $*$ equals every right identity of $*$.
- (b) $*$ has at most one left identity.
- (c) If $*$ is associative with identity, x is invertible and $x * y = x * z$, then $y = z$.
- (d) If $*$ is associative with identity e and $x * y = e$, then $y * x = e$.
- (e) A commutative operation with an identity is associative.

Solution.

- (a) True. This is Proposition 5.3.1.
- (b) False. For $x * y := y$ on $X = \{1, 2\}$, both 1 and 2 are left identities, as in Exercise A1 (c).
- (c) True, by computing $(x^{-1} * x) * y$, regrouped as $x^{-1} * (x * y)$, in two ways (Example (Method: compute one expression in two ways)), with associativity at the second and fourth steps:

$$y = (x^{-1} * x) * y = x^{-1} * (x * y) = x^{-1} * (x * z) = (x^{-1} * x) * z = z.$$

- (d) False. Take $X = \mathbb{N}^{\mathbb{N}}$ under composition, associative with identity $\text{id}_{\mathbb{N}}$ (Proposition 5.3.5). Let $s(n) := n + 1$, and $p(n) := n - 1$ for $n \geq 1$, $p(0) := 0$: the successor map of Section 1.6 and a left inverse of it. Then $p \circ s = \text{id}_{\mathbb{N}}$, since $p(n + 1) = n$. But $(s \circ p)(0) = s(0) = 1 \neq 0$, so $s \circ p \neq \text{id}_{\mathbb{N}}$. With $x = p$ and $y = s$, $x \circ y = e$ and $y \circ x \neq e$.
- (e) False. The operation of Example (Without associativity, two inverses) is commutative with identity e , and not associative.

5.3.7.3 C. Going deeper

Exercise. C1: Four factors

Let $*$ be an associative operation on a set X , and let $a, b, c, d \in X$. Writing uv for $u * v$, show that the five bracketings

$$((ab)c)d, \quad (a(bc))d, \quad (ab)(cd), \quad a((bc)d), \quad a(b(cd))$$

are all equal.

Solution. We show that each equals $((ab)c)d$. Each step is one use of associativity, $(xy)z = x(yz)$, with x, y, z chosen as stated.

- $(a(bc))d = ((ab)c)d$: associativity with $x = a$, $y = b$, $z = c$ gives $a(bc) = (ab)c$, and then both sides are that element times d .
- $(ab)(cd) = ((ab)c)d$: associativity with $x = ab$, $y = c$, $z = d$.
- $a((bc)d) = (a(bc))d$: associativity with $x = a$, $y = bc$, $z = d$; and $(a(bc))d = ((ab)c)d$ by the first item.
- $a(b(cd)) = (ab)(cd)$: associativity with $x = a$, $y = b$, $z = cd$; and $(ab)(cd) = ((ab)c)d$ by the second item.

So all five bracketings are equal. That every bracketing of any finite number of factors gives the same element is true as well; its proof is an induction on the number of factors, not carried out here, and this chapter regroups longer composites only by repeated use of the three-factor law.

Exercise. C2: Find the error

Let $*$ be an operation on a set X with identity e . A student argues:

- (1) Let y and z be inverses of x . (2) Then $x*y = e$ and $x*z = e$, so $x*y = x*z$.
 (3) Cancelling x on the left, $y = z$. (4) Hence an element has at most one inverse.

- (a) Which line fails, and which hypothesis does it hide?
 (b) Show that without that hypothesis the step of the failing line is false.

Solution.

- (a) Line (3) fails. “Cancelling x ” is the statement of Exercise B4 (c), which holds when $*$ is associative and x is invertible; its proof regroups $x^{-1} * (x * y)$ as $(x^{-1} * x) * y$, and that is associativity. The statement here does not assume associativity, so line (3) cites a fact that is not available: entry (N9) of Logic and Proof, Example (What is not allowed). Lines (1) and (2) are correct, and with associativity added the argument becomes a correct proof of [Proposition 5.3.2](#).
- (b) In [Example \(Without associativity, two inverses\)](#), which has an identity and is not associative, $a * a = e = a * b$, so $a * a = a * b$, and yet $a \neq b$. Cancelling a on the left is false there, and so is the conclusion (4): a has the two inverses a and b .

Marking scheme. (10 points)

- 3: names line (3) as the step that fails.
- 3: names associativity as the hidden hypothesis, and says where cancellation uses it.
- 4: gives an operation with identity, not associative, and an **invertible** element x with $x * y = x * z$ and $y \neq z$ (for instance y, z two inverses of x), each equation checked.

A different counterexample to cancellation earns the 4 points if its table is given and the failure of associativity is shown. Fatal errors (0 for the step): naming line (2) or line (4); a counterexample that is associative, or that has no identity, or whose element x is not invertible.

Exercise. C3: Transport by a bijection

Let $\varphi: X \rightarrow Y$ be a bijection, and let $*$ be an operation on Y . For $x, x' \in X$, define

$$x \star x' := \varphi^{-1}(\varphi(x) * \varphi(x')).$$

- (a) Show that $\star$ is an operation on X with $\varphi(x \star x') = \varphi(x) * \varphi(x')$ for all $x, x' \in X$.
- (b) Show that $\star$ is associative if and only if $*$ is.
- (c) Compute $\star$ for $X = Y = \mathbb{R}$, $\varphi(x) = 1 - x$ and $*$ is $\cdot$.

Solution.

- (a) The inverse function $\varphi^{-1}: Y \rightarrow X$ exists by Theorem 1.6.4, so the right-hand side is one element of X for each pair, and $\star$ is an operation on X . Applying φ and using $\varphi \circ \varphi^{-1} = \text{id}_Y$ (Definition 1.6.2) gives $\varphi(x \star x') = \varphi(x) * \varphi(x')$.

- (b) ($\Leftarrow$) Let $*$ be associative and $x, y, z \in X$. By (a), applied twice on each side,

$$\varphi((x \star y) \star z) = (\varphi(x) * \varphi(y)) * \varphi(z) = \varphi(x) * (\varphi(y) * \varphi(z)) = \varphi(x \star (y \star z)),$$

and φ is injective, so $(x \star y) \star z = x \star (y \star z)$. ($\Rightarrow$) Let $\star$ be associative and $u, v, w \in Y$. Since φ is surjective, $u = \varphi(x)$, $v = \varphi(y)$, $w = \varphi(z)$ for some $x, y, z \in X$, and the same display read from the outside in gives $(u \star v) \star w = \varphi((x \star y) \star z) = \varphi(x \star (y \star z)) = u \star (v \star w)$.

- (c) $\varphi \circ \varphi = \text{id}_{\mathbb{R}}$, since $1 - (1 - x) = x$, so $\varphi^{-1} = \varphi$ (Definition 1.6.2). Hence

$$x \star x' = 1 - (1 - x)(1 - x') = x + x' - xx',$$

the operation of Exercise B1. Its identity $0 = \varphi(1)$ and its one non-invertible element $1 = \varphi(0)$ are the images of the identity 1 and of the non-invertible 0 of multiplication.