Abstract Algebra I

Randall R. Holmes

Auburn University

Last revision: November 11, 2016

Notation

- $\mathbf{N} = \{1, 2, 3 \dots\}$, natural numbers
- $\mathbf{Z} = \{\dots, -2, -1, 0, 1, 2, \dots\}$, integers
- $\mathbf{Q} = \left\{ \frac{m}{n} \,|\, m, n \in \mathbf{Z}, n \neq 0 \right\}$, rational numbers (fractions)
- $\mathbf{R}$, real numbers
- $\mathbf{C} = \{a + bi \,|\, a, b \in \mathbf{R}\}$ $(i = \sqrt{-1})$, complex numbers
- $\mathbf{Q}^\times$, $\mathbf{R}^\times$, $\mathbf{C}^\times$, nonzero elements of $\mathbf{Q}$, $\mathbf{R}$, $\mathbf{C}$, respectively
- $\mathbf{Q}^+$, $\mathbf{R}^+$, positive elements of $\mathbf{Q}$, $\mathbf{R}$, respectively
- $\mathrm{Mat}_{m\times n}(\mathbf{R})$, $m \times n$ matrices over $\mathbf{R}$
- $\mathrm{Mat}_n(\mathbf{R})$, $n \times n$ matrices over $\mathbf{R}$
- $\mathrm{GL}_n(\mathbf{R})$, invertible $n \times n$ matrices over $\mathbf{R}$
- $\mathrm{SL}_n(\mathbf{R})$, $n \times n$ matrices over $\mathbf{R}$ having determinant 1
- $\mathbf{F}_\mathbf{R}$, functions from $\mathbf{R}$ to $\mathbf{R}$

0 Introduction

There are many familiar ways in mathematics to combine two things to get another. Examples are

- addition of numbers,
- multiplication of numbers,
- addition of matrices,
- multiplication of matrices,
- addition of vectors,
- composition of functions.

There is some commonality among these operations. For instance, each is associative ($(x + y) + z = x + (y + z)$, $(xy)z = x(yz)$, etc.).

We could define an "abstract associative structure" to be a set with an associative operation. Then we could study that abstract associative structure on its own knowing that anything we discovered would automatically apply to all of the examples above.

This is the idea behind abstract algebra.

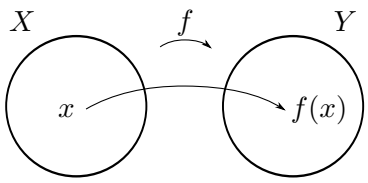
The present course is the study of a "group," which is a set with an associative operation, having an identity element, and such that each element has an inverse (see Section 4). With some restrictions, each of the examples above gives rise to a group.

Groups arise naturally in many areas of mathematics and in other areas as well (e.g., chemistry, physics, and electronic circuit theory).

1 Function

1.1 Notation

Let X and Y be sets. A **function** f from X to Y (written $f : X \to Y$) is a rule that assigns to each element x of X a unique element $f(x)$ of Y, depicted using a Venn diagram like this:



We think of x as an input to the function f and $f(x)$ as the corresponding output. The set X is the **domain** of f and the set Y is the **codomain** of f.

A function is sometimes described by giving a formula for the output in terms of the input. For instance, one writes $f(x) = x^2$ to refer to the function $f : \mathbf{R} \to \mathbf{R}$ that takes an input x and returns the output x^2. So the equation $f(x) = x^2$ says that for an input x "the output $f(x)$ *is* x^2."

1.2 Well-defined function

For a proposed function to be **well defined** (and hence actually be a function) it must assign to each element of its domain a unique element of its codomain. The following example shows various ways a proposed function can fail to be well defined.

1.2.1 Example The following proposed functions are not well defined (and are therefore not actually functions):

(a) $f : \mathbf{R} \to \mathbf{R}$ given by $f(x) = 1/x$. (The number 0 is in the domain $\mathbf{R}$, but $f(0) = 1/0$ is undefined, so f does not assign an element to each element of its domain.)

(b) $g : [0, \infty) \to \mathbf{R}$ given by $g(x) = y$ where $y^2 = x$. (We have $g(4) = 2$

(since $2^2 = 4$), but also $g(4) = -2$ (since $(-2)^2 = 4$), so g does not assign a *unique* element to each element of its domain.)

(c) $h : [2, \infty) \to (4, \infty)$ given by $h(x) = x^2$. (The number 2 is in the domain $[2, \infty)$, but $h(2) = 4$, which is not in the codomain, so h does not assign to each element of its domain an element of its codomain.)

□

1.3 Equal functions

Two functions f and g are **equal** (written $f = g$) if they have the same domain and the same codomain and if $f(x) = g(x)$ for each element x in their common domain.

1.3.1 Example Let $f : (-\infty, 0] \to \mathbf{R}$ be given by $f(x) = -x$ and let $g : (-\infty, 0] \to \mathbf{R}$ be given by $g(x) = \sqrt{x^2}$. Prove that $f = g$.

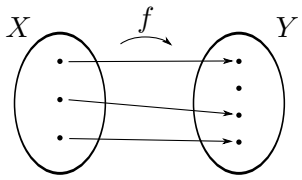
Solution For every $x \in (-\infty, 0]$, we have

$$f(x) = -x = |x| = \sqrt{x^2} = g(x).$$

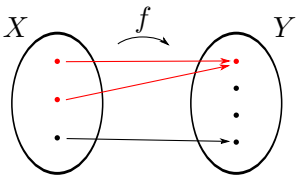
Therefore, $f = g$. □

1.4 Injective function

Let $f : X \to Y$ be a function. Informally, f is "injective" if it never sends two inputs to the same output:



f injective



f *not* injective

Here is the formal definition:

The function $f : X \to Y$ is **injective** if it satisfies the following:

For every $x, x' \in X$, if $f(x) = f(x')$, then $x = x'$.

In words, f is injective if whenever two inputs x and x' have the same output, it must be the case that x and x' are just two names for the same input.

An injective function is called an **injection**.

1.4.1 Example Prove that the function $f : \mathbf{R} \to \mathbf{R}$ given by $f(x) = 2x + 3$ is injective.

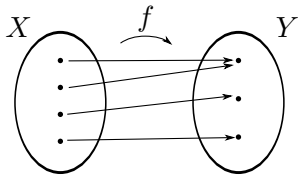
Solution Let $x, x' \in \mathbf{R}$ and assume that $f(x) = f(x')$. Then $2x+3 = 2x'+3$ and we can subtract 3 from both sides and divide both sides by 2 to get $x = x'$. Therefore, f is injective. □

1.4.2 Example Prove that the function $f : \mathbf{R} \to \mathbf{R}$ given by $f(x) = x^2$ is not injective.

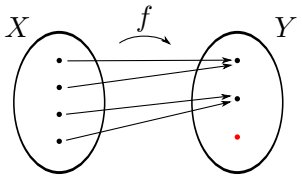
Solution We have $1, -1 \in \mathbf{R}$ and $f(1) = 1^2 = 1 = (-1)^2 = f(-1)$, but $1 \neq -1$. Therefore, f is not injective. □

1.5 Surjective function

Let $f : X \to Y$ be a function. Informally, f is "surjective" if every element of the codomain Y is an actual output:



f surjective



f *not* surjective

Here is the formal definition:

The function $f : X \to Y$ is **surjective** if it satisfies the following:

For every $y \in Y$ there exists $x \in X$ such that $f(x) = y$.

A surjective function is called a **surjection**.

1.5.1 Example Prove that the function $f : (-\infty, 0] \to [2, \infty)$ given by $f(x) = 2 - 3x$ is surjective.

Solution Let $y \in [2, \infty)$. Put $x = \frac{1}{3}(2 - y)$. Since $y \geq 2$, we have $x \leq 0$, so that $x \in (-\infty, 0]$. Also,

$$f(x) = 2 - 3x = 2 - 3\left(\tfrac{1}{3}(2 - y)\right) = y.$$

Therefore, f is surjective.

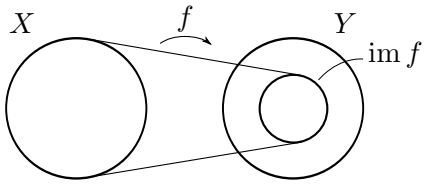
(Since we were seeking an x in the domain for which $f(x) = y$, that is, for which $2 - 3x = y$, we just solved this equation for x. When you prove surjectivity, there is no obligation to show how you came up with an x that works. In fact, it confuses the reader if you include this scratch work since the reader does not expect it.) □

1.5.2 Example Prove that the function $f : [1, \infty) \to (2, \infty)$ given by $f(x) = x + 2$ is not surjective.

Solution The number $5/2$ is in the codomain $(2, \infty)$. But this number is not an output, for if $f(x) = 5/2$ for some $x \in [1, \infty)$, then $x + 2 = 5/2$, implying $x = 1/2 \notin [1, \infty)$, a contradiction. Therefore, there is no $x \in [1, \infty)$ for which $f(x) = 5/2$ and we conclude that f is not surjective.

(Since an input x is ≥ 1 and the corresponding output is $x + 2$, we saw that the output would always be ≥ 3 and this is what gave the idea to consider $5/2$.) □

Let $f : X \to Y$ be a function. The "image of f" is the set of all outputs.



Here is the formal definition:

The **image** of $f : X \to Y$ (denoted $\operatorname{im} f$) is given by

$$\operatorname{im} f = \{f(x) \mid x \in X\}.$$

1.5.3 Example Let $f : [1, \infty) \to \mathbf{R}$ be given by $f(x) = 3 - x$. Prove that $\operatorname{im} f = (-\infty, 2]$.

Solution ($\subseteq$) Let $y \in \operatorname{im} f$. Then $y = f(x) = 3 - x$ for some $x \in [1, \infty)$. Since $x \geq 1$, we have $y \leq 2$ so $y \in (-\infty, 2]$. This shows that $\operatorname{im} f \subseteq (-\infty, 2]$.

($\supseteq$) Let $y \in (-\infty, 2]$. Put $x = 3 - y$. Since $y \leq 2$, we have $x \geq 1$ so $x \in [1, \infty)$. Thus, $y = 3 - x = f(x) \in \operatorname{im} f$. This shows that $(-\infty, 2] \subseteq \operatorname{im} f$.

Therefore, $\operatorname{im} f = (-\infty, 2]$.

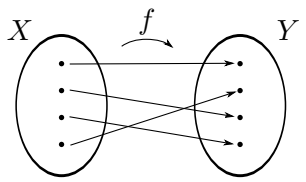
(The claim is that the two sets $\operatorname{im} f$ and $(-\infty, 2]$ are equal. To show two sets are equal, one shows that each is a subset of the other. We use ($\subseteq$) to introduce the proof that $\operatorname{im} f \subseteq (-\infty, 2]$ and ($\supseteq$) to introduce the proof that $\operatorname{im} f \supseteq (-\infty, 2]$.) □

Let $f : X \to Y$ be a function. Saying $\operatorname{im} f = Y$ is the same as saying every element of Y is in the image of f, that is, every element of Y is an output. Therefore, saying $\operatorname{im} f = Y$ is the same as saying that f is surjective.

1.6 Bijective function

A **bijective function** is a function that is both injective and surjective. In the Venn diagram of a bijective function, each element of the codomain has

precisely one arrow pointing to it (it has at least one such arrow since the function is surjective and at most one since the function is injective).



f bijective

A bijective function is called a **bijection**. It is said to set up a **one-to-one correspondence** between the elements of its domain and the elements of its codomain.

Let X and Y be sets. We write $|X| = |Y|$ and say that X and Y have the same **cardinality** if there exists a bijection from X to Y.

If X is finite (i.e., has finitely many elements), we denote by $|X|$ the number of elements in X. If X and Y are both finite sets, then they have the same number of elements if and only if there exists a bijection from X to Y. In this case, the statement $|X| = |Y|$ causes no confusion since it is true whether it is interpreted as saying X and Y have the same number of elements or as saying there exists a bijection from X to Y.

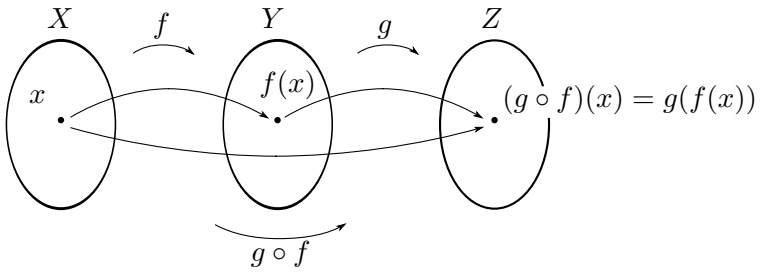
Even if X is not finite, we think of $|X|$ as a measure of the size of X. (Technically, $|X|$ is the equivalence class of X under the equivalence relation $\sim$ defined on sets by putting $X \sim Y$ if there exists a bijection from X to Y.) However, when the set is infinite, some counterintuitive things can happen. For instance, Exercise 1–6 shows that it is possible to have $|X| = |Y|$ with Y a proper subset of X, which certainly cannot happen if X is finite.

It has been shown that $|\mathbf{Q}| = |\mathbf{Z}|$, but $|\mathbf{R}| \neq |\mathbf{Z}|$.

1.7 Composition

Let $f : X \to Y$ and $g : Y \to Z$ be functions. The **composition** of f and g is the function $g \circ f : X \to Z$ given by

$$(g \circ f)(x) = g\big(f(x)\big).$$



The following theorem says that composition of functions is associative.

1.7.1 Theorem. *If $f : X \to Y$, $g : Y \to Z$, and $h : Z \to W$ are functions, then $(h \circ g) \circ f = h \circ (g \circ f)$.*

Proof. Let f, g, and h be functions as indicated. For every $x \in X$ we have

$$\begin{aligned}\big[(h \circ g) \circ f\big](x) &= (h \circ g)\big(f(x)\big) \\ &= h\big(g(f(x))\big) \\ &= h\big((g \circ f)(x)\big) \\ &= \big[h \circ (g \circ f)\big](x).\end{aligned}$$

Therefore, $(h \circ g) \circ f = h \circ (g \circ f)$. □

Because of this theorem, we can write $h \circ g \circ f$ (without parentheses) and no confusion can arise.

The following example shows that a composition of injective functions is injective.

1.7.2 Example Let $f : X \to Y$ and $g : Y \to Z$ be functions. Prove that if f and g are injective, then so is $g \circ f$.

Solution Assume that f and g are injective. Let $x, x' \in X$ and assume that $(g \circ f)(x) = (g \circ f)(x')$. Then $g(f(x)) = g(f(x'))$ and, since g is injective, we get $f(x) = f(x')$. But since f is injective, this last equation implies $x = x'$. Therefore $g \circ f$ is injective. □

Exercise 1–7 shows that a composition of surjective functions is surjective.

1.8 Identity function

Let X be a set. The **identity function** on X is the function $1_X : X \to X$ given by $1_X(x) = x$.

1.8.1 Theorem. *Let $f : X \to Y$ be a function from the set X to the set Y. We have $f \circ 1_X = f$ and $1_Y \circ f = f$.*

Proof. For every $x \in X$, we have

$$(f \circ 1_X)(x) = f\big(1_X(x)\big) = f(x),$$

where the last equality uses the definition of 1_X. Therefore $f \circ 1_X = f$.

The proof of the second equality is Exercise 1–8. □

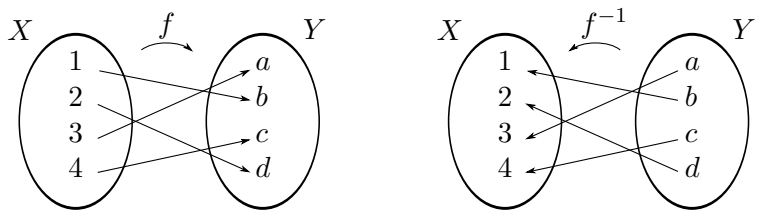
1.9 Inverse function

Let X and Y be sets and let $f : X \to Y$ be a function. An **inverse** of f is a function $f^{-1} : Y \to X$ such that for all $x \in X$ and $y \in Y$,

$$f^{-1}\big(f(x)\big) = x \quad \text{and} \quad f\big(f^{-1}(y)\big) = y.$$

The first equation says that if you apply f first and then apply f^{-1}, you get back the original input x. So, in a sense, f^{-1} undoes what f does. Similarly, the second equation says that f undoes what f^{-1} does.

In terms of the Venn diagram, f^{-1} is just like f except with the direction of the arrows reversed:



Another way to say that $f^{-1} : Y \to X$ is an inverse of f is to say that

$$f^{-1} \circ f = 1_X \quad \text{and} \quad f \circ f^{-1} = 1_Y.$$

The first equation here says that for every $x \in X$, $(f^{-1} \circ f)(x) = 1_X(x)$, that is, $f^{-1}\big(f(x)\big) = x$, which is the first equation above. Similarly, the second equation here says the same thing as the second equation above.

An inverse function need not exist. For instance, the function $f : \mathbf{R} \to \mathbf{R}$ given by $f(x) = x^2$ has no inverse. Indeed, if there did exist an inverse f^{-1} of f, we would get

$$\big(f^{-1}(-1)\big)^2 = f\big(f^{-1}(-1)\big) = -1,$$

contradicting that the square of a number is never negative.

However, the next theorem says that any bijection has an inverse (and also that any function that has an inverse must necessarily be bijective).

1.9.1 Theorem. *A function $f : X \to Y$ has an inverse if and only if it is bijective.*

Proof. Let $f : X \to Y$ be a function.

($\Rightarrow$) Assume that f has an inverse f^{-1}. (f injective?) Let $x, x' \in X$ and assume that $f(x) = f(x')$. Then

$$x = f^{-1}\big(f(x)\big) = f^{-1}\big(f(x')\big) = x'.$$

Therefore, f is injective. (f surjective?) Let $y \in Y$. Put $x = f^{-1}(y)$. Then $x \in X$ and

$$f(x) = f\big(f^{-1}(y)\big) = y.$$

Therefore, f is surjective. Since f is both injective and surjective, it is bijective.

($\Leftarrow$) Assume that f is bijective. Define $f^{-1} : Y \to X$ by letting $f^{-1}(y)$ be the unique x in X for which $f(x) = y$. (Since f is surjective, there is at least one such x and since f is injective, there is at most one such x.) For $x \in X$, we have $f^{-1}\big(f(x)\big) = x$ (since $f^{-1}\big(f(x)\big)$ is defined to be the element that f sends to $f(x)$). Similarly, for $y \in Y$, $f\big(f^{-1}(y)\big) = y$ (since $f^{-1}(y)$ is defined to be the element that f sends to y). Therefore, f^{-1} is an inverse of f. $\square$

1 – Exercises

1–1 Determine whether each proposed function is well defined. If the proposed function is not well defined, explain why not.

(a) $f : \mathbf{R} \to \mathbf{R}$ given by $f(x) = \ln x$.

(b) $g : \mathbf{Z} \to \mathbf{Z}$ given by $g(n) = n/2$.

(c) $h : \mathbf{Z} \to \mathbf{Z}$ given by $h(n) = \begin{cases} n/2, & \text{if } n \text{ is a multiple of 2,} \\ n/3, & \text{if } n \text{ is a multiple of 3,} \\ n, & \text{otherwise.} \end{cases}$

1–2 Prove that the function $f : (-\infty, 1] \to \mathbf{R}$ given by $f(x) = (x-1)^2$ is injective.

1–3 Let $\mathrm{Mat}_2(\mathbf{R})$ be the set of all 2×2 matrices having entries in the set $\mathbf{R}$ of real numbers. Let $f : \mathrm{Mat}_2(\mathbf{R}) \to \mathbf{R}$ be the "determinant function" given by

$$f\left(\begin{bmatrix} a & b \\ c & d \end{bmatrix}\right) = ad - bc.$$

(a) Prove or disprove: f is injective.

(b) Prove or disprove: f is surjective.

1–4 Let $f : \mathbf{R} \to [1, 4)$ be given by $f(x) = 2 - \sin x$. Prove that f is *not* surjective.

1–5 Let $f : [0, \infty) \to \mathbf{R}$ be given by $f(x) = 1 - (x+1)^2$. Prove that $\operatorname{im} f = (-\infty, 0]$.

1–6 Let $2\mathbf{Z}$ denote the set $\{2n \mid n \in \mathbf{Z}\}$ (even integers). Prove that the function $f : \mathbf{Z} \to 2\mathbf{Z}$ given by $f(n) = 2n$ is a bijection. (This shows that $|\mathbf{Z}| = |2\mathbf{Z}|$ even though $2\mathbf{Z}$ is a proper subset of $\mathbf{Z}$.)

1–7 Let $f : X \to Y$ and $g : Y \to Z$ be functions. Prove that if f and g are surjective, then so is $g \circ f$.

1–8 Let $f : X \to Y$ be a function from the set X to the set Y. Prove that $1_Y \circ f = f$.

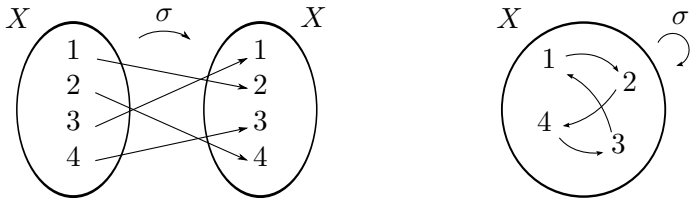
1–9 It was shown in Section 1.9 that the function $f : \mathbf{R} \to \mathbf{R}$ given by $f(x) = x^2$ does not have an inverse. Use this same formula, but change the domain and codomain of f so that it *does* have an inverse. State what the inverse function is and prove that it satisfies the definition of an inverse.

2 Permutation

2.1 Definition

Let X be a set. A **permutation** of X is a bijection from X to X. We use Greek letters, like σ and τ, to denote permutations (rather than f, g, etc.)

There are various ways to depict permutations. The figure on the left below shows a permutation σ of the set $X = \{1, 2, 3, 4\}$ using a Venn diagram with two copies of X side by side, and the figure on the right shows the same permutation using a single copy of X.



This same permutation can be represented compactly using a matrix:

$$\sigma = \begin{pmatrix} 1 & 2 & 3 & 4 \\ 2 & 4 & 1 & 3 \end{pmatrix}.$$

Each number in the top row is mapped to the number directly below it. The term "permutation," which ordinarily means rearrangement, is used here because one imagines the numbers $1, 2, 3, 4$ in the usual order (top row) being rearranged in the order $2, 4, 1, 3$ (bottom row).

The set of all permutations of the set X is denoted S_X:

$$S_X = \{\sigma : X \to X \mid \sigma \text{ is a bijection}\}.$$

When $X = \{1, 2, 3, \ldots, n\}$ we write S_X simply as S_n. For example, S_3 has the following 6 elements:

$$\begin{pmatrix} 1 & 2 & 3 \\ 1 & 2 & 3 \end{pmatrix}, \quad \begin{pmatrix} 1 & 2 & 3 \\ 2 & 1 & 3 \end{pmatrix}, \quad \begin{pmatrix} 1 & 2 & 3 \\ 3 & 2 & 1 \end{pmatrix},$$
$$\begin{pmatrix} 1 & 2 & 3 \\ 1 & 3 & 2 \end{pmatrix}, \quad \begin{pmatrix} 1 & 2 & 3 \\ 2 & 3 & 1 \end{pmatrix}, \quad \begin{pmatrix} 1 & 2 & 3 \\ 3 & 1 & 2 \end{pmatrix}.$$

Just looking at the bottom rows of these matrices, we see that all possible arrangements of the numbers 1, 2, and 3 are represented. We expect $3! = 3 \cdot 2 \cdot 1 = 6$ such arrangements and this is the case. In general,

$$|S_n| = n!.$$

2.2 Permutation composition

Let X be a set. For σ and τ in S_X, we write the composition $\sigma \circ \tau$ simply as $\sigma\tau$.

The following theorem says that the set S_X is "closed" under composition.

2.2.1 Theorem. *If $\sigma, \tau \in S_X$, then $\sigma\tau \in S_X$.*

Proof. Let $\sigma, \tau \in S_X$. Then σ and τ are both bijections from X to X. Since they are both injective, so is $\sigma\tau$ (by 1.7.2), and since they are both surjective, so is $\sigma\tau$ (by Exercise 1–7). Therefore, $\sigma\tau$ is a bijection from X to X, that is, $\sigma\tau \in S_X$. □

2.2.2 Example Let σ and τ be the elements of S_3 given by

$$\sigma = \begin{pmatrix} 1 & 2 & 3 \\ 2 & 3 & 1 \end{pmatrix}, \quad \tau = \begin{pmatrix} 1 & 2 & 3 \\ 1 & 3 & 2 \end{pmatrix}.$$

Find $\tau\sigma$.

Solution We have $(\tau\sigma)(1) = \tau\big(\sigma(1)\big) = \tau(2) = 3$, so $\tau\sigma$ sends 1 to 3. This gives the first column in the matrix representation of $\tau\sigma$. The other columns are computed similarly and we get

$$\tau\sigma = \begin{pmatrix} 1 & 2 & 3 \\ 3 & 2 & 1 \end{pmatrix}.$$

(Note that $\tau\sigma$ is a bijection and is therefore in S_3 in accordance with the theorem.) □

2.3 Identity permutation

Let X be a set. We have defined $1_X : X \to X$ by $1_X(x) = x$. This function is a bijection from X to X and is therefore a permutation of X, that is, $1_X \in S_X$. The permutation 1_X is called the **identity permutation** of X.

The special case of Theorem 1.8.1 with $Y = X$ says that for each permutation $\sigma \in S_X$ we have

$$1_X\sigma = \sigma \quad \text{and} \quad \sigma 1_X = \sigma$$

so 1_X acts like the number 1 if we view composition as a type of multiplication.

When $X = \{1, 2, 3, \ldots, n\}$ we denote the identity permutation by ε:

$$\varepsilon = \begin{pmatrix} 1 & 2 & 3 & \cdots & n \\ 1 & 2 & 3 & \cdots & n \end{pmatrix}.$$

2.4 Inverse permutation

Let X be a set and let $\sigma : X \to X$ be an element of S_X (so σ is a permutation of X). Since σ is bijective, its inverse σ^{-1} exists by Theorem 1.9.1. Moreover, since σ^{-1} has an inverse, namely σ, Theorem 1.9.1 implies that σ^{-1} is bijective, that is, $\sigma^{-1} \in S_X$.

The special case of the second boxed statement in 1.9 with $Y = X$ says that

$$\sigma^{-1}\sigma = 1_X \quad \text{and} \quad \sigma\sigma^{-1} = 1_X.$$

Regarding composition as a type of multiplication, we have seen that 1_X acts like the number 1. The equations above show that σ^{-1} acts like the multiplicative inverse of σ (which is the reason for the superscript -1).

2.4.1 Example Let σ be the element of S_4 given by

$$\sigma = \begin{pmatrix} 1 & 2 & 3 & 4 \\ 3 & 1 & 2 & 4 \end{pmatrix}.$$

Find σ^{-1} and verify that $\sigma^{-1}\sigma = \varepsilon$.

Solution Since σ maps each number in the top row to the number directly below it, the inverse function σ^{-1} maps each number in the bottom row to the number directly above it. Therefore,

$$\sigma^{-1} = \begin{pmatrix} 1 & 2 & 3 & 4 \\ 2 & 3 & 1 & 4 \end{pmatrix}.$$

We have

$$\sigma^{-1}\sigma = \begin{pmatrix} 1 & 2 & 3 & 4 \\ 2 & 3 & 1 & 4 \end{pmatrix} \begin{pmatrix} 1 & 2 & 3 & 4 \\ 3 & 1 & 2 & 4 \end{pmatrix} = \begin{pmatrix} 1 & 2 & 3 & 4 \\ 1 & 2 & 3 & 4 \end{pmatrix} = \varepsilon$$

(see Example 2.2.2 for how to compute the composition). □

2 – Exercises

2–1 Let σ and τ be the elements of S_4 given by

$$\sigma = \begin{pmatrix} 1 & 2 & 3 & 4 \\ 2 & 3 & 4 & 1 \end{pmatrix}, \quad \tau = \begin{pmatrix} 1 & 2 & 3 & 4 \\ 2 & 1 & 4 & 3 \end{pmatrix}.$$

Find each of the following:

(a) $\sigma(2)$.

(b) $\tau^{-1}(1)$.

(c) $\sigma\tau$.

2–2 Let X be a set. For each $a \in X$, define

$$F_a = \{\sigma \in S_X \mid \sigma(a) = a\},$$

so F_a is the set of all permutations of X that fix a (i.e., leave a unmoved). Let $a \in X$. Prove that for each $\sigma \in F_a$ and $\tau \in S_X$, we have $\tau\sigma\tau^{-1} \in F_{\tau(a)}$.

3 Binary operation

A binary operation on a set is a way of combining two elements of the set to form another element of the set.

Addition (+) is an example of a binary operation on the set **Z** of integers. For instance, the numbers 5 and 3 are combined to produce $5 + 3$, which is 8.

Multiplication ($\cdot$) is another example of a binary operation on **Z**. For instance, the numbers 5 and 3 are combined to produce $5 \cdot 3$, which is 15.

3.1 Definition

Let X be a set. Informally, a binary operation $*$ on X is a rule that assigns to each pair x and y of elements of X an element $x * y$ of X.

The formal definition requires the notation

$$X \times X = \{(x, y) \,|\, x, y \in X\}.$$

So $X \times X$ denotes the set of all ordered pairs having entries coming from the set X.

Here is the formal definition:

A **binary operation** on X is a function $* : X \times X \to X$.

Let $* : X \times X \to X$ be a binary operation on X. For an input (x, y), instead of denoting the corresponding output by $*\big((x, y)\big)$ using usual function notation, it is customary to write $x * y$ instead.

The binary operation $*$ on X is **commutative** if $x * y = y * x$ for all $x, y \in X$. It is **associative** if $(x * y) * z = x * (y * z)$ for all $x, y, z \in X$.

3.2 Examples and nonexamples

3.2.1 Example The following are binary operations:

(a) Addition $(+)$ on $\mathbf{Z}$, $\mathbf{Q}$, $\mathbf{R}$, and $\mathbf{C}$. It is both associative and commutative.

(b) Multiplication $(\cdot)$ on $\mathbf{Z}$, $\mathbf{Q}$, $\mathbf{R}$, and $\mathbf{C}$. It is both associative and commutative.

(c) Addition $(+)$ on the set $\mathbf{R}^n$ of all n-tuples $(x_1, x_2, \ldots, x_n)$ with $x_i \in \mathbf{R}$ given by

$$(x_1, x_2, \ldots, x_n) + (y_1, y_2, \ldots, y_n) = (x_1 + y_1, x_2 + y_2, \ldots, x_n + y_n)$$

(called **componentwise addition**). It is both associative and commutative (see Exercise 3–3).

(d) Function addition $(+)$ on the set $\mathbf{F}_{\mathbf{R}}$ of all functions from $\mathbf{R}$ to $\mathbf{R}$ defined as follows: for $f, g \in \mathbf{F}_{\mathbf{R}}$, the sum $f+g$ is given by $(f+g)(x) = f(x)+g(x)$. It is associative (by Exercise 3–4) and commutative since, for $f, g \in \mathbf{F}_{\mathbf{R}}$, we have

$$(f + g)(x) = f(x) + g(x) = g(x) + f(x) = (g + f)(x)$$

for all $x \in \mathbf{R}$, implying $f + g = g + f$.

(e) Matrix addition $(+)$ on the set $\mathrm{Mat}_{m\times n}(\mathbf{R})$ ($m \times n$ matrices over $\mathbf{R}$). It is both associative and commutative.

(f) Matrix multiplication $(\cdot)$ on the set $\mathrm{Mat}_n(\mathbf{R})$ ($n \times n$ matrices over $\mathbf{R}$). We show that this binary operation is associative in general but not commutative when $n \geq 2$.

(Associative) Let $A = [a_{ij}]$, $B = [b_{ij}]$, and $C = [c_{ij}]$ be $n \times n$ matrices. The (i, j)-entry of the product AB is $p_{ij} = \sum_{k=1}^{n} a_{ik}b_{kj}$ (= dot product of ith row of A with jth column of B). Therefore, the (i, j)-entry of the product $(AB)C$ is

$$\begin{aligned}\sum_{l=1}^{n} p_{il}c_{lj} &= \sum_{l=1}^{n} \left(\sum_{k=1}^{n} a_{ik}b_{kl} \right) c_{lj} \\ &= \sum_{l=1}^{n} \sum_{k=1}^{n} (a_{ik}b_{kl})c_{lj} \qquad \text{(distributive law in } \mathbf{R}\text{)}.\end{aligned}$$

It is left as an exercise to show that this is also the (i, j)-entry of the product $A(BC)$ (see Exercise 3–5).

(Not commutative when $n \geq 2$.) When $n = 2$, we have

$$\begin{bmatrix} 1 & 0 \\ 0 & 0 \end{bmatrix} \cdot \begin{bmatrix} 0 & 1 \\ 0 & 0 \end{bmatrix} = \begin{bmatrix} 0 & 1 \\ 0 & 0 \end{bmatrix} \neq \begin{bmatrix} 0 & 0 \\ 0 & 0 \end{bmatrix} = \begin{bmatrix} 0 & 1 \\ 0 & 0 \end{bmatrix} \cdot \begin{bmatrix} 1 & 0 \\ 0 & 0 \end{bmatrix}.$$

For general $n \geq 2$, if A has upper left corner 1 and zeros elsewhere and B has upper right corner 1 and zeros elsewhere, then the upper right corner of AB is 1 and that of BA is 0, so $AB \neq BA$.

(g) Composition ($\circ$) on the set S_X (permutations of the set X). It is associative (see 1.7), but it is not commutative when $|X| \geq 3$ (see Exercise 3–6).

(h) Let n be a positive integer and let $\mathbf{Z}_n = \{0, 1, 2, \ldots, n-1\}$. Define **addition modulo** n, denoted $+$, on $\mathbf{Z}_n$ by letting $a + b$ be the remainder of the usual sum $a + b$ upon division by n. For instance, if $n = 5$, then $3 + 4 = 2$ (since the remainder of 7 upon division by 5 is 2). Then $+$ is a binary operation on $\mathbf{Z}_n$. It is both associative and commutative. (The direct proof that it is associative is a bit tedious, but we will see an easy indirect proof later, so we postpone the proof until then.)

Since a binary operation is technically a function, it is important, when attempting to define a particular binary operation, to check that a well-defined function results (see Section 1.2). For instance, the function must assign to every element (x, y) of the domain $X \times X$ a unique element of the codomain X. In other words, it must be the case that for every pair x and y in X, the expression $x * y$ is defined and is a single element of X.

3.2.2 Example Determine whether each of the following is a well-defined binary operation $*$.

(a) On $\mathbf{R}$, $x * y = x/y$.

(b) On $\mathbf{Z}$, $x * y = (x + y)/2$.

(c) On $\mathbf{Z}$, $x * y = c$, where $c > x + y$.

(d) On $\mathbf{Q}$, $x * y = (x + y)/2$.

Solution (a) This is not a binary operation since $1 * 0 = 1/0$, which is undefined.

(b) This is not a binary operation since $1 * 2 = (1 + 2)/2 = 3/2$, which is not in $\mathbf{Z}$.

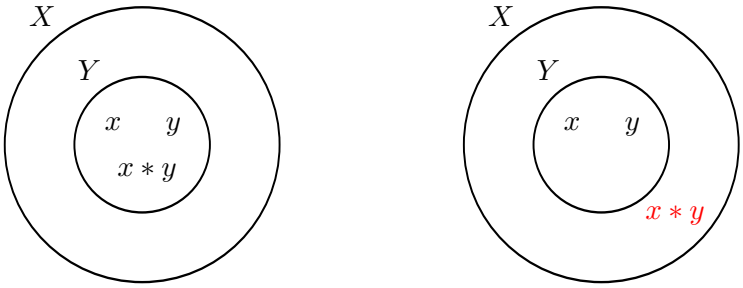
(c) This is not a binary operation. Indeed, $1 * 2 = 4$ (since $4 > 1 + 2$), but also $1 * 2 = 5$ (since $(5 > 1 + 2)$, so $1 * 2$ is not a *single* element of $\mathbf{Z}$.

(d) This is a binary operation since, for each pair x and y in $\mathbf{Q}$, the expression $(x + y)/2$ is defined and is a single element of $\mathbf{Q}$.

□

3.3 Closed subset

Let X be a set and let $*$ be a binary operation on X. A subset Y of X is **closed** under $*$ if whenever x and y are elements of Y, the element $x * y$ is also in Y:



Y closed $\qquad$ Y *not* closed

Put more succinctly,

The subset Y of X is closed under $*$ if $x, y \in Y \Rightarrow x * y \in Y$.

If Y is closed under $*$, then $*$ can be viewed as a binary operation on Y.

3.3.1 Example Addition (+) is a binary operation on $\mathbf{Z}$. Let $2\mathbf{Z}$ denote the set $\{2n \,|\, n \in \mathbf{Z}\}$ (even integers). Then $2\mathbf{Z}$ is a subset of $\mathbf{Z}$. Prove that $2\mathbf{Z}$ is closed under $+$.

Solution Let $x, y \in 2\mathbf{Z}$. Then $x = 2n$ and $y = 2m$ for some $n, m \in \mathbf{Z}$. We have $x + y = 2n + 2m = 2(n + m) \in 2\mathbf{Z}$. Therefore, $2\mathbf{Z}$ is closed under $+$. □

3.3.2 Example Matrix multiplication is a binary operation on $\mathrm{Mat}_n(\mathbf{R})$. Fix $n \in \mathbf{N}$ and let $\mathrm{GL}_n(\mathbf{R})$ be the set of invertible $n \times n$ matrices over $\mathbf{R}$. Then $\mathrm{GL}_n(\mathbf{R})$ is a subset of $\mathrm{Mat}_n(\mathbf{R})$. Prove that $\mathrm{GL}_n(\mathbf{R})$ is closed under matrix multiplication. ("GL" stands for General Linear.)

Solution Let $A, B \in \mathrm{GL}_n(\mathbf{R})$. Then the inverse matrices A^{-1} and B^{-1} exist. We have

$$(AB)(B^{-1}A^{-1}) = A(BB^{-1})A^{-1} = AIA^{-1} = AA^{-1} = I$$

and similarly $(B^{-1}A^{-1})(AB) = I$. Therefore, $(AB)^{-1}$ exists (it is $B^{-1}A^{-1}$), that is, $AB \in \mathrm{GL}_n(\mathbf{R})$. □

3.3.3 Example Let X be a set, let $*$ be a binary operation on X, and assume that $*$ is both commutative and associative. Let $Y = \{y \in X \,|\, y*y = y\}$. Then Y is a subset of X.

(a) Prove that Y is closed under $*$.

(b) Let $X = \mathbf{R}$ and let $*$ be multiplication $\cdot$ on $\mathbf{R}$. Identify the set Y in this case and verify that it is closed under $\cdot$ in agreement with part (a).

Solution

(a) Let $y, z \in Y$. (Must show $y * z$ is in Y, which amounts to showing $(y * z) * (y * z) = y * z$.) We have

$$\begin{aligned} (y*z)*(y*z) &= y*z*y*z && (* \text{ is associative}) \\ &= y*y*z*z && (* \text{ is commutative}) \\ &= y*z && (y, z \in Y) \end{aligned}$$

Therefore, Y is closed under $*$.

(b) In this case, Y consists of all real numbers y such that $y^2 = y$. Solving, we get $y(y-1) = 0$ so $y = 0, 1$. Thus $Y = \{0, 1\}$. Since $0 \cdot 0 = 0$, $0 \cdot 1 = 0$, and $1 \cdot 1 = 1$ (and $\cdot$ is commutative), we have checked all possible products of elements of Y and have shown that they all stay inside Y. Therefore, Y is closed under $\cdot$ in agreement with part (a).

□

3.4 Table

Let X be the set $\{a, b, c, d\}$. The following table gives a binary operation $*$ on X:

$*$	a	b	c	d
a	a	b	c	d
b	b	c	d	a
c	c	d	a	b
d	d	a	b	c

This table works much like a multiplication table. For instance, $b * c = d$. In general, the element $x * y$ is located at the intersection of the row labeled x and the column labeled y.

Because the table is symmetric about the 45° line from the upper left corner to the lower right corner, it follows that $*$ is commutative.

It turns out that $*$ is also associative (this follows from the fact that this is the table for the "group" $\mathbf{Z}_4$, as we will see). In general, it is difficult to use the table to tell that a binary operation is associative.

3 – Exercises

3–1 Determine whether each of the following is a well-defined binary operation $*$.

(a) On $\mathbf{R}$, $x * y = \sqrt{xy}$.

(b) On $[0, \infty)$, $x * y = |a + b|$, where $a^2 = x$ and $b^2 = y$ $(a, b \in \mathbf{R})$.

(c) On $\mathbf{N}$, $x * y = 2^{xy}$. ($\mathbf{N} = \{1, 2, 3, \dots\}$.)

(d) On $(1, \infty)$, $x * y = \dfrac{2xy - 3}{xy - 1}$.

3–2 Let $*$ be the binary operation on $\mathbf{N}$ given by $n * m = m^n$.

(a) Is $*$ commutative? Explain.

(b) Is $*$ associative? Explain.

3–3 For fixed n, let $\mathbf{R}^n$ denote the set of all n-tuples $(x_1, x_2, \dots, x_n)$ with $x_i \in \mathbf{R}$. Componentwise addition $+$ on $\mathbf{R}^n$ is given by

$$(x_1, x_2, \dots, x_n) + (y_1, y_2, \dots, y_n) = (x_1 + y_1, x_2 + y_2, \dots, x_n + y_n).$$

Prove that $+$ is associative and commutative.

3–4 Prove that function addition on $\mathbf{F}_\mathbf{R}$ is associative (see Example 3.2.1).

3–5 Finish the proof begun in Example 3.2.1 that matrix multiplication on $\mathrm{Mat}_n(\mathbf{R})$ is associative.

3–6 Let X be a set and assume that $|X| \geq 3$ (i.e., X has at least three elements). Prove that composition on S_X is not commutative. (Do not assume that X is finite.)

3–7 Matrix addition and matrix multiplication are binary operations on the set $\mathrm{Mat}_2(\mathbf{R})$ of 2×2 matrices over $\mathbf{R}$. Let Y be the subset of $\mathrm{Mat}_2(\mathbf{R})$ consisting of matrices of the form

$$\begin{bmatrix} a & b \\ b & a \end{bmatrix} \qquad (a, b \in \mathbf{R}).$$

Prove or disprove the following statements:

(a) Y is closed under matrix addition.

(b) Y is closed under matrix multiplication.

3–8 Let X be a set and let $*$ be an associative binary operation on X. Let $Y = \{y \in X \mid y * x = x * y \text{ for all } x \in X\}$. Then Y is a subset of X. Prove that Y is closed under $*$.

3–9 Let $X = \{a, b, c, d\}$ and let $*$ be the binary operation on X given by the following table:

$*$	a	b	c	d
a	d	c	a	b
b	c	b	a	c
c	a	a	d	c
d	b	d	c	a

(a) Find $a * c$.

(b) Is $*$ commutative? Explain.

(c) Compute $(a * d) * c$ and $a * (d * c)$. Can you tell, based on this computation, whether $*$ is associative? Explain.

(d) Compute $(c * a) * b$ and $c * (a * b)$. Can you tell, based on this computation, whether $*$ is associative? Explain.

(e) Is the subset $Y = \{a, c, d\}$ of X closed under $*$? Explain.

4 Group

4.1 Definition

A **group** is a pair $(G, *)$, where G is a set and $*$ is a binary operation on G satisfying the following properties:

(G1) $*$ is associative,

(G2) there exists an element e of G such that $e * x = x$ and $x * e = x$ for all $x \in G$,

(G3) for each element x of G there exists an element x' of G such that $x' * x = e$ and $x * x' = e$.

If $(G, *)$ is a group, we say that G is a group under $*$.

Although the definition leaves open the possibility that there is more than one element of G satisfying the condition stated for e, it is a consequence of the assumptions that there is only one such element (see 4.3). It is called the **identity** element of the group.

Similarly, for each element x of G, it is a consequence of the assumptions that there is only one element of G satisfying the condition stated for x' (see 4.3). It is called the **inverse** of x.

If the binary operation $*$ is commutative, the group $(G, *)$ is an **abelian group** (named after the Norwegian mathematician Abel, who was one of the first to use group theory to solve important problems of his day).

$|G|$ is the **order** of G. The group G is **finite** if $|G|$ is finite.

4.2 Examples, nonexamples

4.2.1 Example

(a) $\mathbf{R}$ is a group under addition $(+)$.

Axiom G1 holds since $+$ is associative. Axiom G2 holds with $e = 0$ since $0 + x = x$ and $x + 0 = x$ for all $x \in \mathbf{R}$. Axiom G3 holds since,

for each $x \in \mathbf{R}$, we can let x' be $-x$ noting that $(-x) + x = 0$ and $x + (-x) = 0$.

(b) Similarly, each set $\mathbf{Z}$, $\mathbf{Q}$, and $\mathbf{C}$ is a group under addition with 0 playing the role of e and $-x$ playing the role of x'.

(c) $\mathbf{R}^\times$ (= the set $\mathbf{R}$ with 0 removed) is a group under multiplication $(\cdot)$.

Axiom G1 holds since $\cdot$ is associative. Axiom G2 holds with $e = 1$ since $1 \cdot x = x$ and $x \cdot 1 = x$ for all $x \in \mathbf{R}^\times$. Axiom G3 holds since, for each $x \in \mathbf{R}^\times$, we can let x' be x^{-1} (defined since $x \neq 0$) noting that $x^{-1} \cdot x = 1$ and $x \cdot x^{-1} = 1$.

(d) Similarly, both sets $\mathbf{Q}^\times$ and $\mathbf{C}^\times$ (the symbol $\times$ signifying that 0 is removed) are groups under multiplication with 1 playing the role of e and x^{-1} playing the role of x'.

(e) For fixed n, the set $\mathbf{Z}_n = \{0, 1, 2, \ldots, n-1\}$ is a group under addition $+$ modulo n (see Section 3.2).

We are postponing the proof that $+$ is associative. The role of e is played by 0. The role of $0'$ is played by 0 and if $x \in \mathbf{Z}_n$ with $x \neq 0$, the role of x' is played by $n - x$.

(f) For fixed n, the set $\mathbf{R}^n$ of n-tuples $(x_1, x_2, \ldots, x_n)$ with $x_i \in \mathbf{R}$ is a group under componentwise addition.

Componentwise addition is an associative binary operation on $\mathbf{R}^n$ by Exercise 3–3. The role of e is played by the n-tuple $0 = (0, 0, \ldots, 0)$. Given $x = (x_1, x_2, \ldots, x_n) \in \mathbf{R}^n$, the role of x' is played by $-x = (-x_1, -x_2, \ldots, -x_n)$.

(g) The set $\mathbf{F}_\mathbf{R}$ of all functions from $\mathbf{R}$ to $\mathbf{R}$ is a group under function addition.

Function addition is associative by Exercise 3–4. The role of e is played by the zero function 0 given by $0(x) = 0$, and for $f \in \mathbf{F}_\mathbf{R}$, the role of f' is played by $-f$ given by $(-f)(x) = -f(x)$.

(h) For fixed m and n, $\mathrm{Mat}_{m\times n}(\mathbf{R})$ is a group under matrix addition.

Matrix addition is associative (proof similar to Exercise 3–3). The matrix 0 having each entry 0 plays the role of e, and for $A = [a_{ij}] \in \mathrm{Mat}_{m\times n}(\mathbf{R})$, the matrix $-A = [-a_{ij}]$ plays the role of A'.

(i) For fixed n, the set $\mathrm{GL}_n(\mathbf{R})$ (invertible $n \times n$ matrices over $\mathbf{R}$) is a group under matrix multiplication.

Matrix multiplication is a binary operation on $\mathrm{GL}_n(\mathbf{R})$ by Example 3.3.2. It is associative by Example 3.2.1. The role of e is played by the identity matrix I, and for each $A \in \mathrm{GL}_n(\mathbf{R})$, we can let A' be A^{-1} (inverse matrix of A).

(j) For each set X, the set S_X is a group under composition. In particular, S_n is a group under composition for all $n \in \mathbf{N}$.

Composition is an associative binary operation on S_X (see Example 3.2.1). The role of e is played by the identity function 1_X since $1_X\sigma = \sigma$ and $\sigma 1_X = \sigma$ for each $\sigma \in S_X$ (see Section 2.3). For each $\sigma \in S_X$, we can let σ' be the inverse function σ^{-1} (which exists because σ is bijective) noting that $\sigma^{-1}\sigma = 1_X$ and $\sigma\sigma^{-1} = 1_X$ (see Section 2.4).

(k) $G = \{e\}$ is a group with binary operation given by $ee = e$. It is the **trivial group**.

All of these groups are abelian except for $(\mathrm{GL}_n(\mathbf{R}), \cdot)$ when $n \geq 2$ (see Exercise 4–2) and $(S_X, \circ)$ when $|X| \geq 3$ (see Exercise 3–6).

4.2.2 Example The following are *not* groups.

(i) $\mathbf{Z} = \{\ldots, -2, -1, 0, 1, 2, \ldots\}$ under subtraction.

We have $(0 - 0) - 1 = -1 \neq 1 = 0 - (0 - 1)$, so G1 fails.

(ii) $(0, \infty)$ under addition.

Addition is associative (G1), but G2 fails since there is no identity element. Indeed, suppose that $e \in (0, \infty)$ is an identity. Since $1 \in (0, \infty)$, we have $e + 1 = 1$. But this implies $e = 0$, contradicting that $e > 0$.

(iii) $\mathbf{R}$ under multiplication.

Multiplication is associative (G1) and 1 is an identity (G2) (and it is the only identity), but 0 has no inverse, so G3 fails.

4.3 Uniqueness of identity, inverse

Let $(G, *)$ be a group.

4.3.1 Theorem.

(i) *G has a unique identity element.*

(ii) *Each element of G has a unique inverse element.*

Proof. (i) If e and e_1 are identity elements of G, then

$$\begin{aligned} e_1 &= e_1 * e && (e \text{ is identity}) \\ &= e && (e_1 \text{ is identity}). \end{aligned}$$

Therefore, G has a unique identity element.

(ii) Let $x \in G$ and let x' and x'' be inverses of x. Then

$$\begin{aligned} x'' &= x'' * e \\ &= x'' * (x * x') && (x' \text{ is inverse of } x) \\ &= (x'' * x) * x' \\ &= e * x' && (x'' \text{ is inverse of } x) \\ &= x'. \end{aligned}$$

Therefore, x has a unique inverse. □

4.4 Generalized associativity

Let $(G, *)$ be a group and let $x, y, z \in G$. The assumption that $*$ is associative means that we can write $x * y * z$ without parentheses and no confusion will arise. Indeed, whether this expression is interpreted as $(x * y) * z$ or $x * (y * z)$ the result will be the same.

A routine proof by induction shows that this is true if there are more than three elements of G involved as well. For instance, for $x, y, z, u, v \in G$ the expression

$$x * y * z * u * v$$

can be computed like this

$$(((x * y) * z) * u) * v,$$

or like this

$$((x * y) * (z * u)) * v,$$

or using any of the other possible groupings, and the result will be the same (provided the order of the factors remains the same).

This is the **generalized associativity property**.

Even though parentheses are unnecessary, they are often used, nonetheless, to draw the reader's attention to particular groupings.

4.5 Multiplicative notation

In the definition of group the symbol $*$ is used to emphasize the fact that the notation for the binary operation can be anything (e.g., $+$, $\cdot$, $\circ$).

However, when referring to a group in general we always use multiplicative notation; that is, we write $x * y$ simply as xy and call this the product of x and y, and instead of x' we write x^{-1} (though we continue to denote the identity element by e instead of 1).

Let G be a group and let $x \in G$. We define

$$x^0 = e$$

and for a positive integer n we define

$$x^n = xx \cdots x \qquad (n \text{ factors})$$

and

$$x^{-n} = \left(x^{-1}\right)^n = x^{-1}x^{-1} \cdots x^{-1} \qquad (n \text{ factors}).$$

This defines x^n for every integer n.

In applying general results about groups to a specific group it is sometimes necessary to translate notation. For instance, suppose that in our general group G we have a statement concerning an element $a = x^3y^{-2}$ $(x, y \in G)$. If the statement is applied to the specific group $(\mathbf{Z}, +)$, this element would be

$$\begin{aligned} a &= x^3y^{-2} \\ &= x^3\left(y^{-1}\right)^2 \\ &= x * x * x * y' * y' \\ &= x + x + x + (-y) + (-y) \\ &= 3x - 2y, \end{aligned}$$

so $3x - 2y$ is the additive analog of the multiplicative expression x^3y^{-2}.

4.6 Cancellation properties

Let G be a group and let $x, y, z \in G$.

4.6.1 Theorem.

(i) *If* $xy = xz$, *then* $y = z$.

(ii) *If* $xz = yz$, *then* $x = y$.

Proof. (i) If $xy = xz$, then $y = ey = x^{-1}xy = x^{-1}xz = ez = z$.

(Second proof:

$$\begin{aligned} xy = xz \quad &\Rightarrow \quad x^{-1}xy = x^{-1}xz \\ &\Rightarrow \quad ey = ez \\ &\Rightarrow \quad y = z.) \end{aligned}$$

(ii) Similar. □

The statements (i) and (ii) are the **left** and **right cancellation properties**, respectively.

4.7 Properties of inverse

Let G be a group and let $x \in G$. The first theorem we have about inverses says that if an element acts as a "right inverse" of x, then it must be the inverse of x (and similarly for a "left inverse").

4.7.1 Theorem. *Let* $x, y \in G$.

(i) *If* $xy = e$, *then* $y = x^{-1}$.

(ii) *If* $yx = e$, *then* $y = x^{-1}$.

Proof. (i) Assume $xy = e$. We have $xy = e = xx^{-1}$, so $y = x^{-1}$ by the left cancellation property (see Section 4.6).

(ii) Similar. □

4.7.2 Theorem. *Let* $x, y \in G$.

(i) $\left(x^{-1}\right)^{-1} = x$,

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

Proof. (i) Since $x^{-1}x = e$, it follows from part (i) of the preceding theorem that x is the inverse of x^{-1}, that is, $x = \left(x^{-1}\right)^{-1}$.

(ii) Since

$$(xy)\left(y^{-1}x^{-1}\right) = x(yy^{-1})x^{-1} = xex^{-1} = xx^{-1} = e,$$

it follows from part (i) of the preceding theorem that $y^{-1}x^{-1}$ is the inverse of xy, that is $y^{-1}x^{-1} = (xy)^{-1}$. □

4.8 Laws of exponents

Let G be a group and let $x \in G$. Recall that we have defined x^n for every integer n (see Section 4.5). The next theorem says that two familiar laws of exponents are valid for groups.

4.8.1 Theorem. *For $x \in G$ and $m, n \in \mathbf{Z}$,*

(i) $x^m x^n = x^{m+n}$,

(ii) $(x^m)^n = x^{mn}$.

A careful proof of this theorem would require mathematical induction and the consideration of cases depending on whether m and n are > 0, $= 0$, or < 0. Instead of giving such a proof, we consider just a few special cases to show the main ideas:

$$x^3x^2 = (xxx)(xx) = x^5 = x^{3+2} \qquad \text{(see (i))}$$

$$\begin{aligned} x^{-2}x^3 &= (x^{-1}x^{-1})(xxx) = x^{-1}\left(x^{-1}x\right)xx = x^{-1}exx \\ &= x^{-1}xx = ex = x = x^1 = x^{(-2)+3} \qquad \text{(see (i))} \end{aligned}$$

$$\left(x^2\right)^3 = x^2x^2x^2 = (xx)(xx)(xx) = x^6 = x^{2\cdot 3} \qquad \text{(see (ii))}.$$

It should be pointed out that $(xy)^n$ need not equal $x^n y^n$ for $x, y \in G$ and $n \in \mathbf{Z}$. If $n = 2$, for instance, then we have

$$(xy)^2 = (xy)(xy) = xyxy$$

and if $yx \neq xy$, then we cannot rearrange the middle factors to get $xxyy$, which is x^2y^2.

However, if $yx = xy$, then we *can* rearrange the factors so that in this case $(xy)^n = x^n y^n$.

4.9 Direct product, direct sum

Let G_1 and G_2 be two groups. Let $G_1 \times G_2$ denote the set of all ordered pairs with first component coming from the group G_1 and second component coming from the group G_2:

$$G_1 \times G_2 = \{(x_1, x_2) \mid x_1 \in G_1, x_2 \in G_2\}.$$

Define **componentwise multiplication** on $G_1 \times G_2$ by

$$(x_1, x_2)(y_1, y_2) = (x_1 y_1, x_2 y_2).$$

4.9.1 Theorem. *$G_1 \times G_2$ is a group under componentwise multiplication.*

Proof. We need to check the three group axioms.

(G1) The proof of associativity of componentwise multiplication is similar to Exercise 3–3.

(G2) We claim that (e_1, e_2) is an identity element, where e_i is the identity element of G_i $(i = 1, 2)$. For $(x_1, x_2) \in G_1 \times G_2$, we have

$$(e_1, e_2)(x_1, x_2) = (e_1 x_1, e_2 x_2) = (x_1, x_2)$$

and similarly $(x_1, x_2)(e_1, e_2) = (x_1, x_2)$. Therefore, (e_1, e_2) is an identity element.

(G3) Let $(x_1, x_2) \in G_1 \times G_2$. We claim that (x_1^{-1}, x_2^{-1}) is an inverse of (x_1, x_2). We have

$$(x_1^{-1}, x_2^{-1})(x_1, x_2) = (x_1^{-1} x_1, x_2^{-1} x_2) = (e_1, e_2)$$

and similarly $(x_1, x_2)(x_1^{-1}, x_2^{-1}) = (e_1, e_2)$. Therefore, (x_1^{-1}, x_2^{-1}) is an inverse of (x_1, x_2).

This finishes the proof that $G_1 \times G_2$ is a group under componentwise multiplication. □

$G_1 \times G_2$ is the **direct product** of the groups G_1 and G_2.

If the groups G_1 and G_2 are *additive* groups (i.e., the binary operations are both $+$), then the direct product is called the **direct sum** and it is denoted $G_1 \oplus G_2$. In this case, the operation is denoted $+$ and it is called **componentwise addition**:

$$(x_1, x_2) + (y_1, y_2) = (x_1 + y_1, x_2 + y_2).$$

4.10 Isomorphism

Consider the group $\mathbf{Z} = \{\dots, -2, -1, 0, 1, 2, \dots\}$ under addition. If we create a new group

$$\overline{\mathbf{Z}} = \{\dots, \overline{-2}, \overline{-1}, \overline{0}, \overline{1}, \overline{2}, \dots\}$$

by putting bars over each element of $\mathbf{Z}$ and by using a binary operation $\diamond$ that acts just like $+$ acts on the unadorned integers (so, for instance, $\overline{2} \diamond \overline{3} = \overline{5}$), then the group $(\overline{\mathbf{Z}}, \diamond)$ is essentially the same as the original group $(\mathbf{Z}, +)$. We say that these two groups are "isomorphic" (the precise definition is given below).

One often encounters two groups like this that are essentially the same in the sense that the only difference between them is the symbols used for their elements and the symbols used for their binary operations. Usually when this happens it is not as obvious as it was here, so we need a methodical way to identify such a situation. That is what this section is about.

Let G and G' be two groups.

An **isomorphism** from G to G' is a bijection $\varphi : G \to G'$ satisfying the "homomorphism property"

$$\varphi(xy) = \varphi(x)\varphi(y) \qquad \text{for all } x, y \in G.$$

Caution: On the left of the equation the product xy is computed using the binary operation of G, while on the right the product $\varphi(x)\varphi(y)$ is computed using the binary operation of G'.

4.10.1 Example The set $U_4 = \{1, i, -1, -i\}$, where $i = \sqrt{-1}$, is a group under multiplication. Show that the function $\varphi : \mathbf{Z}_4 \to U_4$ given by

$$\begin{array}{ccc} 0 & \longmapsto & 1 \\ 1 & \longmapsto & i \\ 2 & \longmapsto & -1 \\ 3 & \longmapsto & -i \end{array}$$

is an isomorphism.

Solution Since φ never sends two elements to the same place it is injective, and since every element of the codomain has an arrow coming to it, φ is surjective. Therefore, φ is bijective.

The homomorphism property is the statement that

$$\varphi(x + y) = \varphi(x) \cdot \varphi(y)$$

for each $x, y \in \mathbf{Z}_4$ (see "Caution" above). The easiest way to check this property in this case is by looking at the binary operation tables for the two groups:

$+$	0	1	2	3
0	0	1	2	3
1	1	2	3	0
2	2	3	0	1
3	3	0	1	2

$\xrightarrow{\varphi}$

$\cdot$	1	i	-1	$-i$
1	1	i	-1	$-i$
i	i	-1	$-i$	1
-1	-1	$-i$	1	i
$-i$	$-i$	1	i	-1

In words, the homomorphism property is satisfied if adding two elements of $\mathbf{Z}_4$ and applying φ to the result yields the same thing as first applying φ to the elements separately and then multiplying the results. This property is satisfied if the second table is obtained from the first by applying φ to all of the entries. The reader can check that this is indeed the case here. Therefore, φ is an isomorphism. □

Because of the existence of the isomorphism φ from $\mathbf{Z}_4$ to U_4, it follows that these two groups are essentially the same. One can think of φ as a renaming function: it gives to 0 the new name 1, to 1 the new name i, to 2 the new name -1, and to 3 the new name $-i$. Moreover, because of the homomorphism property, this renaming is compatible with the binary

operations of the two groups. In short, the only difference between the two groups is the names we give their elements and the symbol we use for their binary operations ($+$ for $\mathbf{Z}_4$ and $\cdot$ for U_4).

> The groups G and G' are **isomorphic**, written $G \cong G'$, if there exists an isomorphism from G to G'.

If $\varphi : G \to G'$ is an isomorphism, then $\varphi^{-1} : G' \to G$ is also an isomorphism (Exercise 4–10). Therefore, $G \cong G'$ if and only if $G' \cong G$.

In the example given at the first of the section $\mathbf{Z}$ is isomorphic to $\overline{\mathbf{Z}}$. Indeed, an isomorphism $\varphi : \mathbf{Z} \to \overline{\mathbf{Z}}$ is given by $\varphi(x) = \overline{x}$. Note that the homomorphism property is satisfied by the way we defined $\diamond$:

$$\varphi(x + y) = \overline{x + y} = \overline{x} \diamond \overline{y} = \varphi(x) \diamond \varphi(y).$$

4.10.2 Example Let $\mathbf{R}$ be viewed as a group under addition and let $\mathbf{R}^+$ (positive reals) be viewed as a group under multiplication. Prove that $\mathbf{R} \cong \mathbf{R}^+$.

Solution Define $\varphi : \mathbf{R} \to \mathbf{R}^+$ by $\varphi(x) = e^x$. Since e^x is defined and positive for every $x \in \mathbf{R}$, the function φ is well defined.

From calculus, we know that $\varphi^{-1} : \mathbf{R}^+ \to \mathbf{R}$ exists (it is given by $\varphi^{-1}(y) = \ln y$), so φ is bijective by Theorem 1.9.1.

For $x, y \in \mathbf{R}$, we have

$$\varphi(x + y) = e^{x+y} = e^x e^y = \varphi(x)\varphi(y),$$

so φ satisfies the homomorphism property. Therefore, φ is an isomorphism and we conclude that $\mathbf{R} \cong \mathbf{R}^+$. □

4.10.3 Example Is $\mathbf{R}$ isomorphic to $\mathbf{Z}$?

Solution It was pointed out in Section 1.6 that $|\mathbf{R}| \neq |\mathbf{Z}|$, that is, there is no bijection from $\mathbf{R}$ to $\mathbf{Z}$. In particular, there cannot be an isomorphism from $\mathbf{R}$ to $\mathbf{Z}$. Therefore, $\mathbf{R}$ is not isomorphic to $\mathbf{Z}$. □

If $G \cong G'$, then G and G' are indistinguishable as groups. If G has a property that can be described just using its elements and its binary operation, then G' must have that same property, and vice versa.

The next example illustrates this principle. (Recall that G is "abelian" if $xy = yx$ for all $x, y \in G$.)

4.10.4 Example Assume that $G \cong G'$. Prove that G is abelian if and only if G' is abelian.

Solution Since $G \cong G'$, there exists an isomorphism $\varphi : G \to G'$.

($\Rightarrow$) Assume that G is abelian. Let $x', y' \in G'$. (Must show $x'y' = y'x'$.) Since φ is surjective, we have $x' = \varphi(x)$ and $y' = \varphi(y)$ for some $x, y \in G$. Then

$$\begin{aligned} x'y' &= \varphi(x)\varphi(y) \\ &= \varphi(xy) && \text{(homomorphism property)} \\ &= \varphi(yx) && (G \text{ is abelian}) \\ &= \varphi(y)\varphi(x) && \text{(homomorphism property)} \\ &= y'x'. \end{aligned}$$

Therefore, G' is abelian.

($\Leftarrow$) Assume that G' is abelian. Since $G \cong G'$ we have $G' \cong G$ as well. Therefore the proof above shows that G is abelian. □

Recall that the symmetric group S_3 has order $3! = 6$. Since $\mathbf{Z}_6$ also has order 6, there exists a bijection from S_3 to $\mathbf{Z}_6$, so one might wonder whether these two groups are actually isomorphic.

4.10.5 Example Is S_3 isomorphic to $\mathbf{Z}_6$?

Solution According to Exercise 3–6 the group S_3 is not abelian. Since $\mathbf{Z}_6$ is abelian, we conclude from the preceding example that S_3 is not isomorphic to $\mathbf{Z}_6$. □

4.10.6 Example Is $\mathbf{Q}$ isomorphic to $\mathbf{Z}$? (both viewed as groups under addition).

Solution It was pointed out in Section 2 that $|\mathbf{Q}| = |\mathbf{Z}|$, which is to say that

there exists a bijection from $\mathbf{Q}$ to $\mathbf{Z}$. So we cannot immediately conclude, as we did in Example 4.10.3, that $\mathbf{Q} \ncong \mathbf{Z}$. Instead, we might try to imagine some property that $\mathbf{Q}$ has that $\mathbf{Z}$ does not have. We observe that between any two distinct elements x and y of $\mathbf{Q}$ there exists another element of $\mathbf{Q}$ (namely, $(x+y)/2$). But this is not the case for $\mathbf{Z}$ since, for instance, there is no integer between the integers 1 and 2. However, this is not a valid argument for showing that $\mathbf{Q} \ncong \mathbf{Z}$ since it uses *order* properties of numbers and not just the binary operations involved.

Nonetheless, it is the case that $\mathbf{Q} \ncong \mathbf{Z}$ (see Exercise 4–11). □

4 – Exercises

4–1 In each case, the set with the stated binary operation is *not* a group. State the first of the three group axioms (G1, G2, G3) that fails to hold and justify your claim.

(a) $\mathbf{N} = \{1, 2, 3, \dots\}$ under multiplication.

(b) $\mathbf{R}^\times$ (nonzero reals) under $*$ given by $x * y = x/y$.

(c) $\mathbf{R}$ under $*$ given by $x * y = |xy|$.

4–2 Prove that $\mathrm{GL}_n(\mathbf{R})$ is nonabelian for $n \geq 2$.

HINT: First handle the case $n = 2$. (Recall that a matrix is invertible if and only if its determinant is nonzero, so in particular the matrices of Example 3.2.1(f) cannot be used.) For the general case, use the fact that if A and B are 2×2 matrices, then

$$\begin{bmatrix} A & 0 \\ 0 & I \end{bmatrix} \begin{bmatrix} B & 0 \\ 0 & I \end{bmatrix} = \begin{bmatrix} AB & 0 \\ 0 & I \end{bmatrix},$$

where the first matrix on the left denotes the $n \times n$ matrix with A in the upper left corner and the $(n-2) \times (n-2)$ identity matrix I in the lower right corner and zeros elsewhere, and similarly for the other matrices.

4–3 Let $G = \mathbf{R} \backslash \{-1\}$ (reals without -1). Define $*$ on G by

$$x * y = x + y + xy.$$

Prove that $(G, *)$ is a group. (Be sure to check first that $*$ is a well-defined binary operation on G.)

4–4 Let G be a group and let $a, b \in G$. Prove that there exist elements x and y of G such that $ax = b$ and $ya = b$.

4–5 Let G be a finite group. Prove that each element of G appears precisely once in each row and each column of the binary table of G.

HINT: Use a cancellation property (4.6) to show that an element of G can appear at most once in a given row of the table. Then use the fact that each row has as many entries as there are elements in the group to argue that every element of the group appears in each row.

4–6 Let G be a group and assume that $x^2 = e$ for all $x \in G$. Prove that G is abelian.

4–7 Let G_1 and G_2 be groups. Prove that $G_1 \times G_2 \cong G_2 \times G_1$.

4–8 Let G be a finite group and let x be an element of G. Prove that $x^n = e$ for some positive integer n.

HINT: Use the fact that the elements $x^1, x^2, x^3, \ldots$ cannot be distinct.

4–9 Let G be a group of even order. Prove that there exists a *nonidentity* element x of G such that $x^2 = e$.

4–10 Let $\varphi : G \to G'$ be an isomorphism from the group G to the group G'. In particular, φ is bijective so that its inverse $\varphi^{-1} : G' \to G$ exists (see 1.9.1). Prove that φ^{-1} is an isomorphism.

4–11 Prove that $\mathbf{Q}$ is not isomorphic to $\mathbf{Z}$ (both groups under addition).

HINT: Suppose that $\varphi : \mathbf{Q} \to \mathbf{Z}$ is an isomorphism. Then $1 = \varphi(x)$ for some $x \in \mathbf{Q}$. Write $x = \frac{x}{2} + \frac{x}{2}$ and derive a contradiction.

5 Subgroup

Sometimes it happens that a subset of a group is a group in its own right (using the same binary operation as in the larger group). When this happens, the smaller group is called a "subgroup" of the larger group.

For instance, $\mathbf{Z}$ is a subset of the additive group $\mathbf{R}$ and it is also a group under addition, so $\mathbf{Z}$ is a subgroup of $\mathbf{R}$.

5.1 Definition

Let G be a group.

> A subset H of G is a **subgroup** (written $H \leq G$) if it is a group under the binary operation of G.

5.1.1 Example We have $\mathbf{Z} \leq \mathbf{Q} \leq \mathbf{R} \leq \mathbf{C}$, meaning each is a subgroup of the next (under addition). □

It is possible for one group to be a subset of another group without the former being a subgroup of the latter. For instance, $\mathbf{R}^+$ (positive reals) is a subset of $\mathbf{R}$, and we have that $\mathbf{R}^+$ is a group under multiplication and $\mathbf{R}$ is a group under addition. But $\mathbf{R}^+$ is not a subgroup of $\mathbf{R}$ since $\mathbf{R}^+$ does not use the same binary operation as $\mathbf{R}$.

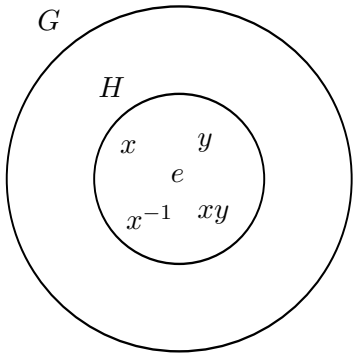
The following theorem provides the most common way to check whether a subset of a group is a subgroup.

5.1.2 Subgroup Theorem. *A subset H of the group G is a subgroup if and only if the following hold:*

(i) $e \in H$,

(ii) $x, y \in H \Rightarrow xy \in H$,

(iii) $x \in H \Rightarrow x^{-1} \in H$.



Note: (i) says that the identity element e of G is in H, (ii) says that H is closed under the binary operation of G, and (iii) says that H is closed under inversion.

Proof. Let H be a subset of G.

($\Rightarrow$) Assume that H is a subgroup of G. Then H has an identity element e_1. Since $e_1 e = e_1 = e_1 e_1$ it follows from the left cancellation property that $e = e_1 \in H$, so (i) holds. By the definition of subgroup, H is closed under the binary operation of G, so (ii) holds. Let $x \in H$. Then x has an inverse x' in H. Since $xx^{-1} = e = e_1 = xx'$ it follows from the left cancellation property that $x^{-1} = x' \in H$, so (iii) holds.

($\Leftarrow$) By property (ii), H is closed under the binary operation on G, so we get an induced binary operation on H. Since $(xy)z = x(yz)$ for every $x, y, z \in G$, this equation holds for every $x, y, z \in H$, so (G1) is satisfied. The identity e of G is in H by property (i) and this same element acts as an identity element of H, so (G2) is satisfied. Finally, if $x \in H$, then its inverse x^{-1} (which exists in G) is actually in H by property (iii) and since $x^{-1}x = e$ and $xx^{-1} = e$, (G3) is satisfied. Therefore, H is a group. □

The group G is a subgroup of itself. If H is a subgroup of G and $H \neq G$, then H is a **proper subgroup** of G.

The subset $\{e\}$ of G consisting of the identity alone is a subgroup of G. It is the **trivial subgroup**.

5.2 Examples

5.2.1 Example Put $3\mathbf{Z} = \{3m \mid m \in \mathbf{Z}\}$ (multiples of 3). Prove that $3\mathbf{Z}$ is a subgroup of the additive group $\mathbf{Z}$.

Solution We use the Subgroup Theorem (5.1.2) with $G = \mathbf{Z}$ and $H = 3\mathbf{Z}$. The role of e in the group $\mathbf{Z}$ is played by the integer 0. Since the binary operation of $\mathbf{Z}$ is $+$, we need to translate the multiplicative notation of the theorem into additive notation (see Section 4.5).

(i) ($0 \in 3\mathbf{Z}$?) We have $0 = 3 \cdot 0 \in 3\mathbf{Z}$ as desired.

(ii) ($x, y \in 3\mathbf{Z} \Rightarrow x + y \in 3\mathbf{Z}$?) Let $x, y \in 3\mathbf{Z}$. We have $x = 3m$ and $y = 3m'$ for some $m, m' \in \mathbf{Z}$. So

$$x + y = 3m + 3m' = 3(m + m') \in 3\mathbf{Z}.$$

(iii) ($x \in 3\mathbf{Z} \Rightarrow -x \in 3\mathbf{Z}$?) Let $x \in 3\mathbf{Z}$. We have $x = 3m$ for some $m \in \mathbf{Z}$. So

$$-x = -(3m) = 3(-m) \in 3\mathbf{Z}.$$

By the Subgroup Theorem, $3\mathbf{Z}$ is a subgroup of $\mathbf{Z}$. □

More generally, $n\mathbf{Z} = \{nm \mid m \in \mathbf{Z}\}$ is a subgroup of $\mathbf{Z}$ for every integer n (same proof with n replacing 3).

5.2.2 Example Let X be a set and let x_0 be a fixed element of X. Define

$$H = \{\sigma \in S_X \mid \sigma(x_0) = x_0\}.$$

Prove that H is a subgroup of S_X.

Solution We use the Subgroup Theorem (5.1.2). The binary operation of S_X is composition $\circ$ (but we have decided to write $\sigma \circ \tau$ simply as $\sigma\tau$) and the role of the identity e is played by the identity function 1_X.

(i) ($1_X \in H$?) We have $1_X(x_0) = x_0$, so $1_X \in H$.

(ii) $(\sigma, \tau \in H \Rightarrow \sigma\tau \in H?)$ Let $\sigma, \tau \in H$. We have

$$\begin{aligned}(\sigma\tau)(x_0) &= \sigma(\tau(x_0)) \\ &= \sigma(x_0) && (\tau \in H) \\ &= x_0 && (\sigma \in H).\end{aligned}$$

Therefore, $\sigma\tau \in H$.

(iii) $(\sigma \in H \Rightarrow \sigma^{-1} \in H?)$ Let $\sigma \in H$. We have

$$\begin{aligned}\sigma^{-1}(x_0) &= \sigma^{-1}\big(\sigma(x_0)\big) && (\sigma \in H) \\ &= x_0 && (\text{definition of inverse function}).\end{aligned}$$

Therefore, $\sigma^{-1} \in H$.

By the Subgroup Theorem, H is a subgroup of S_X. □

5.2.3 Example Let G be an abelian group and let $H = \{x \in G \mid x^2 = e\}$. Prove that H is a subgroup of G.

Solution We use the Subgroup Theorem (5.1.2).

(i) $(e \in H?)$ We have $e^2 = ee = e$, so $e \in H$.

(ii) $(x, y \in H \Rightarrow xy \in H?)$ Let $x, y \in H$. We have

$$\begin{aligned}(xy)^2 &= xyxy \\ &= xxyy && (G \text{ is abelian}) \\ &= x^2y^2 \\ &= ee && (x, y \in H) \\ &= e.\end{aligned}$$

Therefore, $xy \in H$.

(iii) $(x \in H \Rightarrow x^{-1} \in H?)$ Let $x \in H$. We have

$$\begin{aligned}\left(x^{-1}\right)^2 &= x^{-2} && (\text{law of exponents}) \\ &= \left(x^2\right)^{-1} && (\text{law of exponents}) \\ &= e^{-1} && (x \in H) \\ &= e.\end{aligned}$$

Therefore, $x^{-1} \in H$.

By the Subgroup Theorem, H is a subgroup of G. □

5.3 Cyclic subgroup

Let G be a group and let a be a fixed element of G. Put

$$\langle a \rangle = \{a^m \mid m \in \mathbf{Z}\}.$$

5.3.1 Theorem. *$\langle a \rangle$ is a subgroup of G.*

Proof. We use the Subgroup Theorem (5.1.2).

(i) ($e \in \langle a \rangle$?) We have $e = a^0 \in \langle a \rangle$.

(ii) ($x, y \in \langle a \rangle \Rightarrow xy \in \langle a \rangle$?) Let $x, y \in \langle a \rangle$. Then $x = a^m$ and $y = a^n$ for some $m, n \in \mathbf{Z}$. So $xy = a^m a^n = a^{m+n} \in \langle a \rangle$.

(iii) ($x \in \langle a \rangle \Rightarrow x^{-1} \in \langle a \rangle$?) Let $x \in \langle a \rangle$. Then $x = a^m$ for some $m \in \mathbf{Z}$. So $x^{-1} = (a^m)^{-1} = a^{-m} \in \langle a \rangle$.

By the Subgroup Theorem, $\langle a \rangle$ is a subgroup of G. □

We call $\langle a \rangle$ the (**cyclic**) **subgroup of G generated by** a.

5.3.2 Example

(a) Find $\langle 3 \rangle$ in $\mathbf{Q}^\times$ (under multiplication).

(b) Find $\langle 3 \rangle$ in $\mathbf{Z}$ (under addition).

Solution

(a) In $\mathbf{Q}^\times$ we have

$$\begin{aligned}\langle 3 \rangle &= \{3^m \mid m \in \mathbf{Z}\} = \{\dots, 3^{-2}, 3^{-1}, 3^0, 3^1, 3^2, \dots\} \\ &= \{\dots, \tfrac{1}{9}, \tfrac{1}{3}, 1, 3, 9, \dots\}.\end{aligned}$$

(b) In $\mathbf{Z}$ we have

$$\begin{aligned}\langle 3 \rangle &= \{m3 \mid m \in \mathbf{Z}\} \qquad (m3 \text{ is the additive notation of } 3^m) \\ &= \{\dots, (-2)3, (-1)3, (0)3, (1)3, (2)3, \dots\} \\ &= \{\dots, -6, -3, 0, 3, 6, \dots\} = 3\mathbf{Z}.\end{aligned}$$

□

The cyclic subgroup $\langle a \rangle$ is the smallest subgroup of G containing a in the following sense:

5.3.3 Theorem. *If H is any subgroup of G with $a \in H$, then $\langle a \rangle \subseteq H$.*

Proof. Let $H \leq G$ with $a \in H$. We have, using closure, $a^1 = a \in H$, $a^2 = aa \in H$, $a^3 = a^2 a \in H$ and in general $a^m \in H$ for every positive integer m. Also, for each positive integer m, we have, using closure under inversion, $a^{-m} = (a^m)^{-1} \in H$ (since $a^m \in H$ as was just shown). Finally, $a^0 = e \in H$. Therefore, $a^m \in H$ for all $m \in \mathbf{Z}$, whence $\langle a \rangle \subseteq H$. □

5.4 Order of element

Let G be a group and let $x \in G$.

If $x^n = e$ for some positive integer n, then the least such integer is the **order** of x, written $\text{ord}(x)$. If no such positive integer exists, then x has **infinite order**, written $\text{ord}(x) = \infty$.

5.4.1 Example In the multiplicative group $\mathbf{C}^\times$, find

(a) $\text{ord}(i) \quad (i = \sqrt{-1})$,

(b) $\text{ord}(3)$.

Solution In this group, 1 plays the role of e.

(a) Since

$$\begin{aligned} i^1 &= i \\ i^2 &= -1 \\ i^3 &= i^2 i = -i \\ i^4 &= i^3 i = -i^2 = 1 = e, \end{aligned}$$

it follows that $\text{ord}(i) = 4$.

(b) We have $3^1 = 3$, $3^2 = 9$, $3^3 = 27$, and in general, $3^n \neq 1$ for every positive integer n. Therefore, $\text{ord}(3) = \infty$.

□

5.4.2 Example Find the order of the element 3 in $\mathbf{Z}_{12}$.

Solution Put $x = 3$. Since $\mathbf{Z}_{12}$ uses additive notation, the expression x^n in the definition really means nx. We have

$$\begin{aligned} 1x &= 3 \\ 2x &= 3 + 3 = 6 \\ 3x &= 3 + 3 + 3 = 9 \\ 4x &= 3 + 3 + 3 + 3 = 0 = e \qquad \text{(addition modulo 12)} \end{aligned}$$

Therefore, 3 has order 4. □

If we continue computing multiples of $x = 3$ in the preceding example, we get

$$\begin{array}{llll} 1x = 3 & 5x = 3 & 9x = 3 & \dots \\ 2x = 6 & 6x = 6 & 10x = 6 & \dots \\ 3x = 9 & 7x = 9 & 11x = 9 & \dots \\ 4x = 0 & 8x = 0 & 12x = 0 & \dots . \end{array}$$

Evidently $mx = 0$ if and only if 4 divides m. Noting that 4 is the order of x in the example, we see that this illustrates the general property of the order of an element stated in the following theorem (expressed in multiplicative notation as usual).

5.4.3 Theorem. *Let G be a group and let x be an element of G of finite order n. If m is an integer, then $x^m = e$ if and only if n divides m.*

The proof of this theorem requires the following standard fact about integers.

5.4.4 Theorem (Division algorithm). *Let m and n be integers with $n > 0$. There exist unique integers q and r with $0 \leq r < n$ such that*

$$m = qn + r.$$

We omit the proof and instead appeal to the reader's knowledge of long division, which is used to divide m by n as follows:

$$\begin{array}{r} q \\ n\overline{)\,m} \\ \vdots \\ \hline r \end{array} \qquad \Rightarrow \qquad \begin{array}{l} \dfrac{m}{n} = q + \dfrac{r}{n} \\ \\ \Rightarrow \;\; m = qn + r. \end{array}$$

So the q in the theorem corresponds to the whole part of the quotient and the r corresponds to the remainder. In long division, one continues the algorithm until the remainder is less than the divisor, that is, $0 \leq r < n$ (cf. theorem).

Proof of Theorem 5.4.3. Let m be an integer.

($\Rightarrow$) Assume that $x^m = e$. By the Division Algorithm (5.4.4), there exist (unique) integers q and r with $0 \leq r < n$ such that $m = qn + r$. So

$$x^r = x^{m-qn} = x^m(x^n)^{-q} = ee^{-q} = e,$$

where we have used laws of exponents (see 4.8). Since n is the least positive integer for which $x^n = e$ and $0 \leq r < n$, we conclude from this equation that $r = 0$. Therefore, $m = qn$, implying that n divides m.

($\Leftarrow$) Assume that n divides m. Then $m = kn$ for some integer k. Hence,

$$x^m = x^{kn} = (x^n)^k = e^k = e,$$

as desired. □

The following theorem relates the order of an element to the cyclic subgroup the element generates.

5.4.5 Theorem. *Let G be a group and let $x \in G$.*

(i) *If* $\operatorname{ord}(x) = \infty$, *then*

$$\langle x \rangle = \{\dots, x^{-2}, x^{-1}, e, x, x^2, x^3, \dots\}$$

and the elements x^i, $i \in \mathbf{Z}$, are all distinct.

(ii) *If* $\operatorname{ord}(x) = n$, *then*

$$\langle x \rangle = \{e, x, x^2, x^3, \dots, x^{n-1}\}$$

and the elements x^i, $0 \leq i < n$, are all distinct.

(iii) $|\langle x \rangle| = \operatorname{ord}(x)$.

Proof.

(i) Assume that $\operatorname{ord}(x) = \infty$. By definition, $\langle x \rangle$ consists of all powers x^i with $i \in \mathbf{Z}$, so the equation follows once we observe that $x^0 = e$ and $x^1 = x$. (Distinct?) Suppose that $x^i = x^j$ with $i \leq j$. Then

$$x^{j-i} = x^j x^{-i} = x^j (x^i)^{-1} = x^j (x^j)^{-1} = e.$$

Now $j - i$ is a nonnegative integer and, since $\operatorname{ord}(x) = \infty$, this number cannot be positive. Therefore, $j - i = 0$, that is, $j = i$. This proves that the elements x^i, $i \in \mathbf{Z}$, are all distinct.

(ii) Assume that $\operatorname{ord}(x) = n$. Put $S = \{e, x, x^2, x^3, \dots, x^{n-1}\}$. We prove that $\langle x \rangle = S$ by showing that each set is contained in the other.

($\subseteq$) Let $y \in \langle x \rangle$. Then $y = x^m$ for some $m \in \mathbf{Z}$. By the Division Algorithm (5.4.4), there exist (unique) integers q and r with $0 \leq r < n$ such that $m = qn + r$. Therefore,

$$y = x^m = x^{qn+r} = (x^n)^q x^r = e^q x^r = x^r \in S.$$

($\supseteq$) This follows immediately from the definition of $\langle x \rangle$.

(Distinct?) Assume that $x^i = x^j$ with $0 \leq i \leq j < n$. Then $0 \leq j - i < n$ and, arguing just as in the proof of (i), we get $x^{j-i} = e$. Since $\operatorname{ord}(x) = n$, it follows that $j - i = 0$, that is, $j = i$. This proves that the elements x^i, $0 \leq i < n$, are distinct.

(iii) This follows from (i) and (ii). (In the case $\text{ord}(x) = \infty$, we interpret $|\langle x \rangle| = \infty$ as simply saying that the set $\langle x \rangle$ is not finite.)

□

5.4.6 Example Find the cyclic subgroup of $\mathbf{Z}_{12}$ generated by 3.

Solution In Example 5.4.2 it was shown that $\text{ord}(3) = 4$. Put $x = 3$. According to part (ii) of the preceding theorem, we have

$$\begin{aligned} \langle 3 \rangle = \langle x \rangle &= \{e, x, 2x, 3x\} \qquad \text{(additive notation)} \\ &= \{0, 3, 6, 9\}. \end{aligned}$$

□

5.4.7 Example Find $\langle \sigma \rangle$, where σ is the element of S_3 given by

$$\sigma = \begin{pmatrix} 1 & 2 & 3 \\ 2 & 3 & 1 \end{pmatrix}.$$

Solution We have

$$\begin{aligned} \sigma &= \begin{pmatrix} 1 & 2 & 3 \\ 2 & 3 & 1 \end{pmatrix}, \\ \sigma^2 = \sigma\sigma &= \begin{pmatrix} 1 & 2 & 3 \\ 2 & 3 & 1 \end{pmatrix} \begin{pmatrix} 1 & 2 & 3 \\ 2 & 3 & 1 \end{pmatrix} = \begin{pmatrix} 1 & 2 & 3 \\ 3 & 1 & 2 \end{pmatrix}, \\ \sigma^3 = \sigma^2\sigma &= \begin{pmatrix} 1 & 2 & 3 \\ 3 & 1 & 2 \end{pmatrix} \begin{pmatrix} 1 & 2 & 3 \\ 2 & 3 & 1 \end{pmatrix} = \begin{pmatrix} 1 & 2 & 3 \\ 1 & 2 & 3 \end{pmatrix} = \varepsilon. \end{aligned}$$

Therefore, σ has order 3 and, according to Theorem 5.4.5,

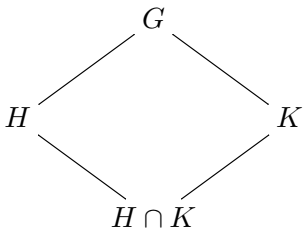
$$\begin{aligned} \langle \sigma \rangle &= \{\varepsilon, \sigma, \sigma^2\} \\ &= \left\{ \begin{pmatrix} 1 & 2 & 3 \\ 1 & 2 & 3 \end{pmatrix}, \begin{pmatrix} 1 & 2 & 3 \\ 2 & 3 & 1 \end{pmatrix}, \begin{pmatrix} 1 & 2 & 3 \\ 3 & 1 & 2 \end{pmatrix} \right\}. \end{aligned}$$

□

5.5 Subgroup diagram

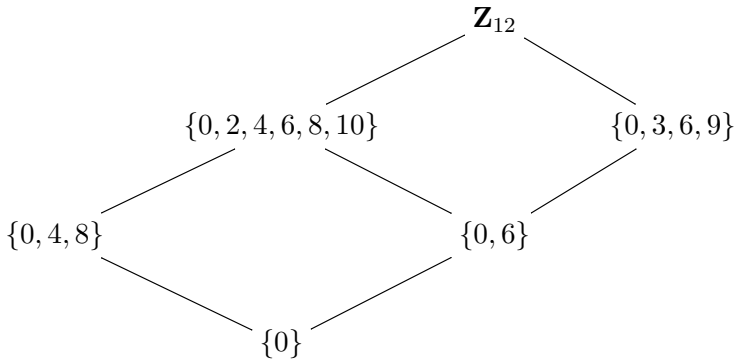
We sometimes draw a **subgroup diagram** to show the inclusion relationships between subgroups of a given group. For instance, if a group G has

subgroups H and K, then $H \cap K$ is also a subgroup of G (Exercise 5–7) and we draw

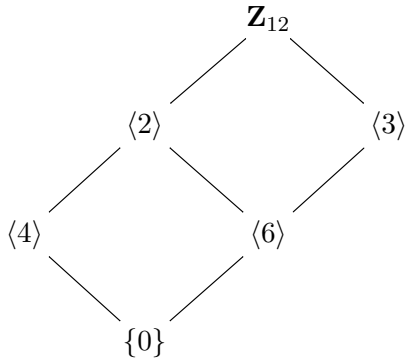


The line segment joining H to G indicates that H is contained in G (the smaller set is lower than the larger one) and so forth.

Here is the subgroup diagram for the group $\mathbf{Z}_{12} = \{0, 1, 2, \ldots, 11\}$:



An easy way to tell that the indicated sets are actually subgroups is to note that each is a cyclic subgroup. For instance, $\{0, 2, 4, 6, 8, 10\} = \langle 2 \rangle$. Here is the diagram again using just the cyclic subgroup notation:



It turns out that this is the *full* subgroup diagram of $\mathbf{Z}_{12}$, meaning that all of the subgroups of $\mathbf{Z}_{12}$ are represented (see 6.3.1).

5 – Exercises

5–1 Let G be a group. The **center** of G, denoted $Z(G)$, is the set of those elements of G that commute with every element of G:

$$Z(G) = \{z \in G \mid zx = xz \text{ for all } x \in G\}.$$

Prove that $Z(G)$ is a subgroup of G.

5–2 Fix $n \in \mathbf{N}$. Let $\mathrm{SL}_n(\mathbf{R})$ be the set of all $n \times n$ matrices over $\mathbf{R}$ having determinant 1:

$$\mathrm{SL}_n(\mathbf{R}) = \{A \in \mathrm{Mat}_n(\mathbf{R}) \mid \det(A) = 1\}.$$

Prove that $\mathrm{SL}_n(\mathbf{R})$ is a subgroup of $\mathrm{GL}_n(\mathbf{R})$ (= invertible $n \times n$ matrices over $\mathbf{R}$). ("SL" stands for Special Linear.)

HINT: From linear algebra, we know that a square matrix is invertible if and only if its determinant is nonzero. Use the fact that $\det(AB) = \det(A)\det(B)$ for $A, B \in \mathrm{Mat}_n(\mathbf{R})$.

5–3

(a) Find the order of the element 9 in $\mathbf{Z}_{15}$.

(b) Find the order of the matrix $A = \begin{bmatrix} 0 & -1 \\ 1 & 0 \end{bmatrix}$ in the group $\mathrm{Mat}_{2\times 2}(\mathbf{R})$.

(c) Find the order of the matrix $A = \begin{bmatrix} 0 & -1 \\ 1 & 0 \end{bmatrix}$ in the group $\mathrm{GL}_2(\mathbf{R})$.

5–4

(a) Compute $\langle 6 \rangle$ in the group $\mathbf{Z}_{15}$.

(b) Compute $\langle \sigma \rangle$, where σ is the element of S_4 given by

$$\sigma = \begin{pmatrix} 1 & 2 & 3 & 4 \\ 3 & 1 & 4 & 2 \end{pmatrix}.$$

5–5 Compute $\langle A \rangle$ in the group $\mathrm{GL}_2(\mathbf{R})$, where $A = \begin{bmatrix} 1 & 1 \\ 0 & 1 \end{bmatrix}$.

5–6 Draw a subgroup diagram for the group $\mathbf{Z}_{18}$ including the subgroups $\{0\}$, $\langle 2 \rangle$, $\langle 3 \rangle$, $\langle 6 \rangle$, $\langle 9 \rangle$, and $\mathbf{Z}_{18}$.

5–7 Let G be a group and let H and K be subgroups of G.

(a) Prove that the intersection $H \cap K$ is a subgroup of G.

(b) Give an example to show that the union $H \cup K$ need not be a subgroup of G.

6 Cyclic group

6.1 Definition and examples

Let G be a group. Recall that if g is an element of G, then $\langle g \rangle$ denotes the set of all powers of g:

$$\langle g \rangle = \{g^m \mid m \in \mathbf{Z}\}.$$

> G is **cyclic** if $G = \langle g \rangle$ for some $g \in G$.

In other words, G is cyclic if there exists some element g in G having the property that every element of G equals g^m for some integer m.

If G is cyclic, then any $g \in G$ for which $G = \langle g \rangle$ is called a **generator** of G.

6.1.1 Example Prove that the group $\mathbf{Z}$ (under addition) is cyclic and find all generators of $\mathbf{Z}$.

Solution The set $\langle 1 \rangle$ consists of all multiples of 1, so $\mathbf{Z} = \langle 1 \rangle$. Therefore, $\mathbf{Z}$ is cyclic and 1 is a generator.

For any integer n, the set $\langle n \rangle$ consists of all multiples of n, so $\langle n \rangle = \mathbf{Z}$ if and only if $n = \pm 1$. Therefore, ± 1 are the only generators of $\mathbf{Z}$. □

6.1.2 Example Let $n \in \mathbf{N}$. Prove that the group $\mathbf{Z}_n$ (under addition modulo n) is cyclic.

Solution We claim that $\mathbf{Z}_n = \langle 1 \rangle$. The element 1 of $\mathbf{Z}_n$ has order n, so by Theorem 5.4.5, we have

$$\begin{aligned} \langle 1 \rangle &= \{0, 1, (2)1, (3)1, \ldots, (n-1)1\} \\ &= \{0, 1, 2, 3, \ldots, n-1\} \\ &= \mathbf{Z}_n \end{aligned}$$

as claimed. Therefore, $\mathbf{Z}_n$ is cyclic. □

In Section 6.4 we will see that $\mathbf{Z}$ and $\mathbf{Z}_n$ ($n \in \mathbf{N}$) are essentially the *only* cyclic groups in the sense that any cyclic group is isomorphic to one of these.

6.1.3 Example Prove that the group $\mathbf{Q}$ (under addition) is *not* cyclic.

Solution We give a proof by contradiction. Suppose that $\mathbf{Q}$ is cyclic. Then $\mathbf{Q} = \langle g \rangle$ for some $g \in \mathbf{Q}$. Then $g/2 \in \mathbf{Q} = \langle g \rangle$, so $g/2 = kg$ for some $k \in \mathbf{Z}$. Now $g \neq 0$ (otherwise we get the contradiction $\mathbf{Q} = \langle 0 \rangle = \{0\}$), so we can divide both sides of $g/2 = kg$ by g to get the contradiction $1/2 = k \in \mathbf{Z}$.

We conclude that $\mathbf{Q}$ is *not* cyclic. □

6.2 Cyclic group is abelian

6.2.1 Theorem. *Every cyclic group is abelian.*

Proof. Exercise 6–2. □

6.3 Subgroup of cyclic group is cyclic

The group $\mathbf{Z}$ is cyclic since $\mathbf{Z} = \langle 1 \rangle$. The set $3\mathbf{Z} = \{3m \mid m \in \mathbf{Z}\}$ (multiples of 3) is a subgroup of $\mathbf{Z}$ by Example 5.2.1. Note that

$$\begin{aligned} 3\mathbf{Z} &= \{\ldots, -6, -3, 0, 3, 6, \ldots\} \\ &= \{\ldots, (-2)3, (-1)3, (0)3, (1)3, (2)3, \ldots\} \\ &= \langle 3 \rangle, \end{aligned}$$

so $3\mathbf{Z}$ itself is cyclic.

The following theorem shows that this is no coincidence.

6.3.1 Theorem. *Every subgroup of a cyclic group is cyclic.*

Proof. Let G be a cyclic group and let H be a subgroup of G. Since G is cyclic, there exists $g \in G$ such that $G = \langle g \rangle$.

If $H = \{e\}$, then $H = \langle e \rangle$ and H is cyclic. Now suppose $H \neq \{e\}$. Since every element of G, and hence H, is a power of g, it follows that $g^n \in H$ for some nonzero integer n. Now $g^{-n} = (g^n)^{-1} \in H$ as well, so by replacing n by $-n$, if necessary, we may assume that n is positive. Furthermore, replacing n again, if necessary, we may assume that it is the least positive integer for which $g^n \in H$.

We claim that $H = \langle g^n \rangle$. Let $h \in H$. We have $h = g^m$ for some integer m. By the division algorithm, there exist integers q and r with $0 \leq r < n$ such that $m = nq + r$. Therefore,

$$g^r = g^{m-nq} = g^m (g^n)^{-q} \in H,$$

which implies, due to the minimality of n, that $r = 0$. Thus, $h = g^m = g^{nq} = (g^n)^q \in \langle g^n \rangle$. This proves that $H \subseteq \langle g^n \rangle$ and, since the other inclusion is immediate, the theorem follows. □

Since $\mathbf{Z}$ is cyclic, every subgroup of $\mathbf{Z}$ is cyclic and hence of the form $\langle n \rangle = n\mathbf{Z}$ for some $n \in \mathbf{Z}$.

6.4 Classification of cyclic groups

The following theorem says that every cyclic group is isomorphic to either $\mathbf{Z}$ or $\mathbf{Z}_n$, some n.

6.4.1 Theorem. *Let G be a cyclic group.*

(i) *If $|G|$ is infinite, then $G \cong \mathbf{Z}$.*

(ii) *If $|G| = n$, then $G \cong \mathbf{Z}_n$.*

Proof. Since G is cyclic, we have $G = \langle g \rangle$ for some $g \in G$.

(i) Assume that $|G|$ is infinite. By Theorem 5.4.5, g has infinite order,

$$G = \langle g \rangle = \{\dots, g^{-2}, g^{-1}, g^0, g^1, g^2, \dots\},$$

and the powers g^k with $k \in \mathbf{Z}$ are distinct.

Define $\varphi : \mathbf{Z} \to G$ by $\varphi(m) = g^m$. We claim that φ is an isomorphism.

(φ injective?) Let $m, n \in \mathbf{Z}$ and assume that $\varphi(m) = \varphi(n)$. Then $g^m = g^n$ and, since the powers g^k with $k \in \mathbf{Z}$ are distinct, it follows that $m = n$. Hence, φ is injective.

(φ surjective?) Let $x \in G$. Since $G = \langle g \rangle$, we have $x = g^m$ for some $m \in \mathbf{Z}$. Then $\varphi(m) = g^m = x$. Hence, φ is surjective.

(Homomorphism property?) For $m, m' \in \mathbf{Z}$, we have

$$\varphi(m + m') = g^{m+m'} = g^m g^{m'} = \varphi(m)\varphi(m'),$$

so φ satisfies the homomorphism property.

Therefore, $\varphi : \mathbf{Z} \to G$ is an isomorphism. We conclude that $\mathbf{Z} \cong G$ and hence $G \cong \mathbf{Z}$ (see Section 4.10).

(ii) Assume that $|G| = n$. By Theorem 5.4.5, g has order n,

$$G = \langle g \rangle = \{g^0, g^1, g^2, \ldots, g^{n-1}\},$$

and the powers g^k with $0 \leq k < n$ are distinct.

Define $\varphi : \mathbf{Z}_n \to G$ by $\varphi(m) = g^m$. An argument very similar to that in part (i) shows that φ is bijective.

(Homomorphism property?) Let $m, m' \in \mathbf{Z}_n$. By the division algorithm (Theorem 5.4.4), there exist integers q and r with $0 \leq r < n$ such that $m + m' = qn + r$. By the definition of addition modulo n, the sum $m + m'$ computed in $\mathbf{Z}_n$ is r. Therefore,

$$\begin{aligned} \varphi(m + m') = \varphi(r) = g^r &= g^{m+m'-qn} \\ &= g^m g^{m'} (g^n)^{-q} = g^m g^{m'} = \varphi(m)\varphi(m'), \end{aligned}$$

using the fact that g has order n so that $g^n = e$. Hence, φ satisfies the homomorphism property.

We have shown that φ is an isomorphism, so we conclude that $G \cong \mathbf{Z}_n$.

□

6.5 Direct sum of cyclic groups

The following example illustrates one implication in the main theorem of this section.

6.5.1 Example Show that $\mathbf{Z}_2 \oplus \mathbf{Z}_3 \cong \mathbf{Z}_6$.

Solution Put $x = (1, 1) \in \mathbf{Z}_2 \oplus \mathbf{Z}_3$. We have

$$\begin{aligned} 1x &= (1, 1) \\ 2x &= x + x = (0, 2) \\ 3x &= 2x + x = (1, 0) \\ 4x &= 3x + x = (0, 1) \\ 5x &= 4x + x = (1, 2) \\ 6x &= 5x + x = (0, 0) = e, \end{aligned}$$

so $\langle x \rangle = \mathbf{Z}_2 \oplus \mathbf{Z}_3$. This shows that $\mathbf{Z}_2 \oplus \mathbf{Z}_3$ is cyclic. By Theorem 6.4.1(ii), we get $\mathbf{Z}_2 \oplus \mathbf{Z}_3 \cong \mathbf{Z}_6$, as claimed. □

Let m and n be positive integers. We denote by $\gcd(m, n)$ the greatest common divisor of m and n. For instance $\gcd(12, 18) = 6$. If $\gcd(m, n) = 1$, the integers m and n have no prime factors in common and they are said to be *relatively prime*.

Looking at the computations in the example, we see that the two components are out of sync, reaching 0 at different steps. They get together only at the step $6 = (2)(3)$. This occurs because 2 and 3 are relatively prime.

6.5.2 Theorem. $\mathbf{Z}_m \oplus \mathbf{Z}_n \cong \mathbf{Z}_{mn}$ *if and only if* $\gcd(m, n) = 1$.

Proof.

($\Rightarrow$) Assume that $\mathbf{Z}_m \oplus \mathbf{Z}_n \cong \mathbf{Z}_{mn}$. Then there exists an isomorphism $\varphi : \mathbf{Z}_{mn} \to \mathbf{Z}_m \oplus \mathbf{Z}_n$. We have $\varphi(1) = (a, b)$ for some $a \in \mathbf{Z}_m$ and $b \in \mathbf{Z}_n$. Since the element 1 of $\mathbf{Z}_{mn}$ has order mn, the element (a, b) of $\mathbf{Z}_m \oplus \mathbf{Z}_n$ must also have order mn.

Let $k = \gcd(m, n)$. Then $m = km'$ and $n = kn'$ for some integers m' and n'. We have

$$km'n'(a, b) = (km'n'a, km'n'b) = (n'ma, m'nb) = (0, 0).$$

Since (a, b) has order mn and $km'n' > 0$ it follows that $mn \leq km'n'$. So

$$mn \leq km'n' \leq km'kn' = mn.$$

Since the ends of this string are the same, the intermediate $\leq$ signs must actually be equalities. Thus $km'n' = km'kn'$ which implies $k = 1$ as desired.

($\Leftarrow$) Assume that $\gcd(m, n) = 1$. Let k be the order of the element $(1, 1)$ of $\mathbf{Z}_m \oplus \mathbf{Z}_n$. Then

$$(k1, k1) = k(1, 1) = (0, 0).$$

so by Theorem 5.4.3, m divides k and n divides k. Since $\gcd(m, n) = 1$, it follows that mn divides k. In particular, $mn \leq k$. On the other hand k is the order of the cyclic subgroup of $\mathbf{Z}_m \oplus \mathbf{Z}_n$ generated by $(1, 1)$, so k is less than or equal to the order of $\mathbf{Z}_m \oplus \mathbf{Z}_n$, which is mn. We conclude that $k = mn$, so in fact $\langle (1, 1) \rangle = \mathbf{Z}_m \oplus \mathbf{Z}_n$. Therefore $\mathbf{Z}_m \oplus \mathbf{Z}_n$ is cyclic. By Theorem 6.4.1, $\mathbf{Z}_m \oplus \mathbf{Z}_n \cong \mathbf{Z}_{mn}$. □

6 – Exercises

6–1 Let G be a cyclic group of order n. Prove that if d is a positive integer dividing n, then G has a subgroup of order d.

HINT: The desired subgroup is necessarily cyclic by Theorem 6.3.1. First work with the special case $G = \mathbf{Z}_{12}$ to get an idea for the proof.

6–2 Prove Theorem 6.2.1, which says the following: Every cyclic group is abelian.

6–3 Prove or disprove: The group S_{12} is cyclic.

6–4 Draw the full subgroup diagram for $\mathbf{Z}_{10}$.

HINT: Theorem 6.3.1.

6–5 Let G be a cyclic group and let g be a generator of G. Prove that g^{-1} is also a generator of G.

6–6 Let m and n be positive integers.

(a) Prove that $H := \{am + bn \mid a, b \in \mathbf{Z}\}$ is a subgroup of $\mathbf{Z}$.

(b) By part (a) and Theorem 6.3.1, $H = \langle d \rangle$ for some integer d. By Exercise 6–5, we may assume that d is positive. Prove that d is the **greatest common divisor** of m and n in the following sense:

(i) $d \mid m$ and $d \mid n$,

(ii) if k is a positive integer such that $k \mid m$ and $k \mid n$, then $k \mid d$.

(The notation $d \mid m$ stands for "d divides m," which means that $m = dj$ for some integer j.)

7 Symmetric group

Recall that if X is a set, then S_X denotes the group of all permutations of X with binary operation being function composition. It is the **symmetric group on** X.

In the special case $X = \{1, 2, \ldots, n\}$ ($n \in \mathbf{N}$) this group is denoted S_n and is called the **symmetric group of degree** n.

We study the symmetric group in this section, focusing primarily on S_n.

7.1 Cycle

A "cycle" is an element of S_n represented by an ordered list of numbers from the set $\{1, 2, \ldots, n\}$. For instance, in S_5 the cycle $(1, 5, 2, 4)$ is the function that does this:

$$1 \mapsto 5 \mapsto 2 \mapsto 4 \mapsto 1 \qquad 3 \mapsto 3.$$

So the cycle $(1, 5, 2, 4)$ sends each number in the list to the next number to the right, except for the last number, which gets sent to the first. Any number not appearing in the list (3 in this case) is fixed, that is, sent to itself.

The matrix representation of this cycle is

$$\sigma = \begin{pmatrix} 1 & 2 & 3 & 4 & 5 \\ 5 & 4 & 3 & 1 & 2 \end{pmatrix}.$$

More generally, let n be a positive integer and let $i_1, i_2, \ldots, i_r$ be distinct integers with $1 \leq i_j \leq n$. We write $\sigma = (i_1, i_2, \ldots, i_r)$ for the element of S_n satisfying

$$\sigma(i_j) = \begin{cases} i_{j+1} & j < r, \\ i_1 & j = r, \end{cases}$$

and $\sigma(k) = k$ for all $k \notin \{i_1, i_2, \ldots, i_r\}$. This permutation is called an r**-cycle** (or a **cycle** of **length** r) and we write $\text{length}(\sigma) = r$.

A cycle is unchanged if the last number is moved to the first. For instance:

$$(1, 5, 2, 4) = (4, 1, 5, 2) = (2, 4, 1, 5) = (5, 2, 4, 1).$$

These arrangements of the numbers $1, 5, 2, 4$ are called "cyclic permutations." If the numbers are arranged in order around a circle, then a cyclic permutation corresponds to a rotation of the circle.

The inverse of a cycle is obtained by writing the entries in reverse order. For example,

$$(1, 5, 2, 4)^{-1} = (4, 2, 5, 1).$$

A **transposition** is a 2-cycle. The transposition (i_1, i_2) transposes (interchanges) the two numbers i_1 and i_2 and fixes every other number.

A 1-cycle (i_1) is the identity since it fixes i_1 as well as every other number.

7.1.1 Example Let σ and τ be the cycles in S_7 given by

$$\sigma = (1, 3, 7, 2, 5) \quad \text{and} \quad \tau = (1, 7, 4, 5).$$

(a) $\sigma(3) = 7$.

Reason: σ sends 3 to the number in the list just to its right, which is 7.

(b) $(\sigma\tau)(1) = 2$.

Reason: The notation $\sigma\tau$ really means $\sigma \circ \tau$, so recalling how to compose functions, we get $(\sigma\tau)(1) = \sigma(\tau(1)) = \sigma(7) = 2$. One can avoid writing so much by just thinking "τ moves 1 to 7 and then σ moves 7 to 2, so $\sigma\tau$ moves 1 to 2." Using symbols,

$$1 \overset{\tau}{\mapsto} 7 \overset{\sigma}{\mapsto} 2.$$

In computing the product $\sigma\tau$ it is important to remember to work from right to left.

(c) $(\tau\sigma\tau)(2) = 1$.

Reason:

$$2 \overset{\tau}{\mapsto} 2 \overset{\sigma}{\mapsto} 5 \overset{\tau}{\mapsto} 1.$$

(d) $\sigma^{-1}(7) = 3$.

Reason: Since σ moves numbers to the right, σ^{-1} moves numbers to the left, so σ^{-1} moves 7 to 3.

□

7.2 Permutation is product of disjoint cycles

The cycles $(1, 4, 2, 6)$ and $(3, 8, 7)$ in S_8 have no numbers in common; they are said to be "disjoint."

Generally, two cycles $(i_1, i_2, \ldots, i_r)$ and $(k_1, k_2, \ldots, k_s)$ are **disjoint** if

$$\{i_1, i_2, \ldots, i_r\} \cap \{k_1, k_2, \ldots, k_s\} = \emptyset.$$

The following theorem says that disjoint cycles commute.

7.2.1 Theorem. *If σ and τ are disjoint cycles in S_n, then $\sigma\tau = \tau\sigma$.*

Proof. Let σ and τ be disjoint cycles in S_n. We can write $\sigma = (i_1, i_2, \ldots, i_r)$ and $\tau = (k_1, k_2, \ldots, k_s)$. Put $I = \{i_1, i_2, \ldots, i_r\}$ and $K = \{k_1, k_2, \ldots, k_s\}$.

To show that the two functions $\sigma\tau$ and $\tau\sigma$ are equal, we need to show that $(\sigma\tau)(m) = (\tau\sigma)(m)$ for all m in their common domain, which is $\{1, 2, \ldots, n\}$.

Let $m \in \{1, 2, \ldots, n\}$. First assume that $m \notin I \cup K$ (in other words, assume that m does not appear in either cycle). Then σ and τ both fix m giving

$$(\sigma\tau)(m) = \sigma(\tau(m)) = \sigma(m) = m = \tau(m) = \tau(\sigma(m)) = (\tau\sigma)(m).$$

Now assume that $m \in I$. Then $\sigma(m) \in I$, as well. Since I and K are disjoint by assumption, m and $\sigma(m)$ are not in K, so they are fixed by τ. Therefore,

$$(\sigma\tau)(m) = \sigma(\tau(m)) = \sigma(m) = \tau(\sigma(m)) = (\tau\sigma)(m).$$

Similarly, if $m \in K$, then $(\sigma\tau)(m) = (\tau\sigma)(m)$.

We have shown that in all cases $(\sigma\tau)(m) = (\tau\sigma)(m)$. Since m was an arbitrary element of $\{1, 2, \ldots, n\}$, we conclude that $\sigma\tau = \tau\sigma$ as desired. □

Let

$$\sigma = \begin{pmatrix} 1 & 2 & 3 & 4 & 5 & 6 & 7 & 8 & 9 \\ 3 & 7 & 8 & 9 & 5 & 4 & 2 & 1 & 6 \end{pmatrix} \in S_9$$

We can write σ as a product (meaning composition) of pairwise disjoint cycles by following an algorithm as illustrated here:

- Start with 1. We have $\sigma : 1 \mapsto 3 \mapsto 8 \mapsto 1$ (back to where we started). This completes the cycle
$$(1, 3, 8).$$

- Pick the smallest number not yet appearing, namely, 2. We have $\sigma : 2 \mapsto 7 \mapsto 2$. This completes the cycle $(2, 7)$, which we compose with the cycle above to get
$$(1, 3, 8)(2, 7).$$

- Again, pick the smallest number not yet appearing, namely, 4. We have $\sigma : 4 \mapsto 9 \mapsto 6 \mapsto 4$ giving the cycle $(4, 9, 6)$, so we now have
$$(1, 3, 8)(2, 7)(4, 9, 6).$$

- Only 5 remains, and since $\sigma : 5 \mapsto 5$ we get the cycle (5). Since this cycle is the identity permutation (as is every cycle of length one), it has no effect on the composition and we omit it.

- We have accounted for all of the numbers $1, 2, \ldots, 9$, and we are left with
$$(1, 3, 8)(2, 7)(4, 9, 6).$$

It is a fact that σ actually equals this product:

$$\sigma = (1, 3, 8)(2, 7)(4, 9, 6) \qquad (*)$$

The product on the right of this equation is the composition of the three indicated cycles.

Each side of (*) represents a function from the set $\{1, 2, \ldots, 9\}$ to itself, so the equation asserts that both functions send each of these numbers to the same output.

Let's use 7 as a test. The effect of the right-hand side of (*) on 7 is

$$7 \overset{(4,9,6)}{\longmapsto} 7 \overset{(2,7)}{\longmapsto} 2 \overset{(1,3,8)}{\longmapsto} 2,$$

so 7 is sent to 2. Since σ also sends 7 to 2, both sides of (*) send 7 to the same output as expected.

The process we used to write σ as a product of disjoint cycles generalizes to an arbitrary element of S_n:

7.2.2 Theorem. *Any element of S_n can be written as a product of disjoint cycles. Moreover, any two such factorizations are the same except possibly for the order of the factors (provided all cycles of length one are included).*

Proof. Let $\sigma \in S_n$. The algorithm illustrated above produces a product $\sigma_1\sigma_2\cdots\sigma_m$ of disjoint cycles. The proof that σ actually equals this product is Exercise 7–6. The proof of the uniqueness statement in the theorem is omitted. □

In the statement of the theorem the word "product" has a broad meaning including any number of factors, with the case of a product of one factor meaning that element itself.

7.3 Permutation is product of transpositions

Recall that a cycle of length two, like $(3, 5)$, is called a transposition. The theorem of this section states that any element of S_n can be written as a product (meaning composition) of transpositions. For instance,

$$\begin{pmatrix} 1 & 2 & 3 & 4 & 5 & 6 \\ 4 & 1 & 3 & 2 & 6 & 5 \end{pmatrix} = (1, 4)(4, 2)(5, 6)$$

as the reader can check.

7.3.1 Theorem. *Any element of S_n can be written as a product of transpositions.*

Note: The case $n = 1$ is included by allowing the possibility of a product with no factors, which is interpreted to be the identity. (This is necessary since $S_1 = \{\varepsilon\}$ has no transpositions at all.)

Proof. By Section 7.2 it suffices to show that every cycle can be written as a product of transpositions. Let $\sigma = (i_1, i_2, \ldots, i_r)$ be a cycle. We proceed by induction on r. If $r = 1$, then σ is the identity, which, according to our convention, is a product of transpositions with no factors.

Assume that $r > 1$. We claim that $(i_1, i_2)\sigma = \sigma'$, where $\sigma' = (i_2, i_3, \ldots, i_r)$. We have,

$$\begin{aligned}
(i_1, i_2)\sigma(i_1) &= i_1 = \sigma'(i_1), \\
(i_1, i_2)\sigma(i_r) &= i_2 = \sigma'(i_r), \\
(i_1, i_2)\sigma(i_j) &= i_{j+1} = \sigma'(i_j), \quad 1 < j < r, \\
(i_1, i_2)\sigma(k) &= k = \sigma'(k), \quad k \neq i_1, i_2, \ldots, i_r,
\end{aligned}$$

so the claim is established. Now the cycle σ' has length $r-1$, so the induction hypothesis says that it is a product of transpositions. Therefore, $\sigma = (i_1, i_2)\sigma'$ is a product of transpositions as well. □

The proof of the theorem provides an algorithm for writing a given element of S_n as a product of transpositions: write the element as a product of disjoint cycles and then write each cycle as a product of transpositions using the formula

$$(i_1, i_2, \ldots, i_r) = (i_1, i_2)(i_2, i_3)(i_3, i_4)\cdots(i_{r-1}, i_r).$$

7.3.2 Example Write the permutation

$$\sigma = \begin{pmatrix} 1 & 2 & 3 & 4 & 5 & 6 & 7 & 8 & 9 \\ 4 & 1 & 3 & 6 & 9 & 2 & 5 & 8 & 7 \end{pmatrix}$$

as a product of transpositions.

Solution We first use the method of Section 7.2 to write the permutation as a product of disjoint cycles, and then we use the formula above to write each of the resulting cycles as a product of transpositions:

$$\begin{aligned} \sigma &= (1, 4, 6, 2)(5, 9, 7) \\ &= (1, 4)(4, 6)(6, 2)(5, 9)(9, 7). \end{aligned}$$

□

It is important to note that an element of S_n can be written as a product of transpositions in more than one way. For instance, if $\sigma = (1, 2, 3)$, then

$$\begin{aligned} \sigma &= (1, 2)(2, 3), \\ \sigma &= (2, 3)(1, 3), \\ \sigma &= (1, 3)(2, 3)(1, 2)(1, 3), \\ \sigma &= (1, 3)(2, 3)(1, 2)(1, 3)(1, 2)(1, 2) \end{aligned}$$

as the reader can check.

However, we will see in the next section that if one such factorization has an even number of factors, then every other such factorization will also have an even number of factors (as the example suggests). Likewise, if one factorization has an odd number of factors, then every other factorization will have an odd number of factors as well.

7.4 Even permutation, odd permutation

Let n be a positive integer. An element of S_n is **even** if it can be written as a product of an even number of transpositions. An element of S_n is **odd** if it can be written as a product of an odd number of transpositions.

By Theorem 7.3.1 an element of S_n is either even or odd, but possibly *both* for all we know at this point. Choosing to apply these terms to permutations would be a bad idea if a permutation could be both even and odd. However, this is not the case:

7.4.1 Theorem. *An element of S_n is not both even and odd.*

Proof. Let $\sigma \in S_n$. Let $\sigma = \sigma_1\sigma_2\cdots\sigma_t$ be a factorization of σ as a product of disjoint cycles. Define $N(\sigma) = \sum_i(\text{length}(\sigma_i) - 1)$ (well defined by the uniqueness statement of 7.2.2). Let $1 \leq a, b \leq n$ with $a \neq b$. Any cycle in which a and b appear can be written $(a, c_1, \ldots, c_h, b, d_1, \ldots, d_k)$ (after applying a cyclic permutation to the elements, if necessary). For such a cycle, a routine check verifies the equation

$$(a, b)(a, c_1, \ldots, c_h, b, d_1, \ldots, d_k) = (b, d_1, \ldots, d_k)(a, c_1, \ldots, c_h).$$

Multiplying both sides of this equation by $(a, b)^{-1} = (a, b)$ gives

$$(a, b)(b, d_1, \ldots, d_k)(a, c_1, \ldots, c_h) = (a, c_1, \ldots, c_h, b, d_1, \ldots, d_k).$$

It follows from these equations that

$$N((a, b)\sigma) = \begin{cases} N(\sigma) - 1, & \text{if } a \text{ and } b \text{ appear in the same } \sigma_i, \\ N(\sigma) + 1, & \text{otherwise.} \end{cases}$$

Indeed, assuming that a and b both appear in σ_i for some i, we may (and do) assume that $i = 1$ (since disjoint cycles commute) and $\sigma_1 = (a, c_1, \ldots, c_h, b, d_1, \ldots, d_k)$, so that, writing $\sigma' = \sigma_2\cdots\sigma_t$,

$$\begin{aligned} N((a, b)\sigma) &= N((a, b)\sigma_1) + N(\sigma') \\ &= k + h + N(\sigma') \\ &= N(\sigma_1) - 1 + N(\sigma') \\ &= N(\sigma) - 1, \end{aligned}$$

and similarly for the other case. In particular, $N((a, b)\sigma)$ and $N(\sigma)$ always have opposite parities (i.e., if one is even, then the other is odd).

Let $\sigma = \tau_1\tau_2\cdots\tau_s$ be a factorization of σ with each τ_i a transposition. Then $\tau_s\tau_{s-1}\cdots\tau_1\sigma = \varepsilon$, so $N(\tau_s\tau_{s-1}\cdots\tau_1\sigma) = N(\varepsilon) = 0$, which is an even number. By repeated application of the observation above, we find that $N(\sigma)$ is even or odd according as s is even or odd. This is to say that the parity of the number s of factors in our factorization $\sigma = \tau_1\tau_2\cdots\tau_s$ is the same as the parity of the number $N(\sigma)$. Since this latter depends only on σ the proof is complete. □

7.4.2 Example Determine whether the permutation

$$\sigma = \begin{pmatrix} 1 & 2 & 3 & 4 & 5 & 6 & 7 & 8 & 9 \\ 4 & 1 & 3 & 6 & 9 & 2 & 5 & 8 & 7 \end{pmatrix}$$

is even or odd.

Solution In Example 7.3.2 we found that

$$\sigma = (1,4)(4,6)(6,2)(5,9)(9,7).$$

Therefore, σ is odd (since it can be expressed as a product of an odd number of transpositions, namely, five). □

7.5 Alternating group

Let $n \in \mathbf{N}$. Let A_n be the set of all even permutations in S_n:

$$A_n = \{\sigma \in S_n \mid \sigma \text{ is even}\}.$$

7.5.1 Theorem. *A_n is a subgroup of S_n.*

Proof. We use the Subgroup Theorem (5.1.2).

($\varepsilon \in A_n$?) By convention, ε is a product of zero transpositions, and since zero is even, we have $\varepsilon \in A_n$.

($\sigma, \tau \in A_n \Rightarrow \sigma\tau \in A_n$?) Let $\sigma, \tau \in A_n$. We can write

$$\sigma = \sigma_1\sigma_2\cdots\sigma_s \quad \text{and} \quad \tau = \tau_1\tau_2\cdots\tau_t$$

for some transpositions σ_i and τ_i with s and t both even. Then

$$\sigma\tau = \sigma_1\sigma_2\cdots\sigma_s\tau_1\tau_2\cdots\tau_t.$$

This expresses $\sigma\tau$ as a product of transpositions. The number of factors is $s+t$, which is even since both s and t are even. We conclude that $\sigma\tau \in A_n$.

($\sigma \in A_n \Rightarrow \sigma^{-1} \in A_n$?) Let $\sigma \in A_n$. We can write

$$\sigma = \sigma_1\sigma_2\cdots\sigma_s$$

for some transpositions σ_i with s even. Using Theorem 4.7.2 and then the fact that each transposition is its own inverse, we get

$$\begin{aligned}\sigma^{-1} &= (\sigma_1\sigma_2\cdots\sigma_s)^{-1}\\ &= \sigma_s^{-1}\sigma_{s-1}^{-1}\cdots\sigma_1^{-1}\\ &= \sigma_s\sigma_{s-1}\cdots\sigma_1.\end{aligned}$$

This expresses σ^{-1} as a product of transpositions. The number of factors is s, which is even. Therefore, $\sigma^{-1} \in A_n$.

By the Subgroup Theorem, A_n is a subgroup of S_n. □

The group A_n is the **alternating group of degree** n.

7.5.2 Theorem. *If $n \geq 2$, then $|A_n| = n!/2$.*

Proof. See Exercise 7–8. □

We note that $A_1 = \{\epsilon\}$, so that $|A_1| = 1$.

7.6 Dihedral group

Let ρ and τ be the elements of the symmetric group S_4 given by

$$\rho = \begin{pmatrix}1 & 2 & 3 & 4\\ 2 & 3 & 4 & 1\end{pmatrix} = (1,2,3,4)$$

and

$$\tau = \begin{pmatrix}1 & 2 & 3 & 4\\ 1 & 4 & 3 & 2\end{pmatrix} = (2,4).$$

The subset D_4 of S_4 given by

$$D_4 = \{\varepsilon, \rho, \rho^2, \rho^3, \tau, \rho\tau, \rho^2\tau, \rho^3\tau\}$$

is a subgroup of S_4 called the **dihedral group** (of degree 4).

To verify that D_4 is indeed a subgroup, one can use the Subgroup Theorem and the following multiplication (i.e., composition) table:

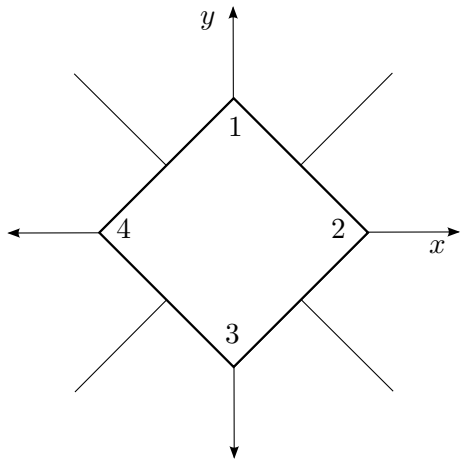
$\circ$	ε	ρ	ρ^2	ρ^3	τ	$\rho\tau$	$\rho^2\tau$	$\rho^3\tau$
ε	ε	ρ	ρ^2	ρ^3	τ	$\rho\tau$	$\rho^2\tau$	$\rho^3\tau$
ρ	ρ	ρ^2	ρ^3	ε	$\rho\tau$	$\rho^2\tau$	$\rho^3\tau$	τ
ρ^2	ρ^2	ρ^3	ε	ρ	$\rho^2\tau$	$\rho^3\tau$	τ	$\rho\tau$
ρ^3	ρ^3	ε	ρ	ρ^2	$\rho^3\tau$	τ	$\rho\tau$	$\rho^2\tau$
τ	τ	$\rho^3\tau$	$\rho^2\tau$	$\rho\tau$	ε	ρ^3	ρ^2	ρ
$\rho\tau$	$\rho\tau$	τ	$\rho^3\tau$	$\rho^2\tau$	ρ	ε	ρ^3	ρ^2
$\rho^2\tau$	$\rho^2\tau$	$\rho\tau$	τ	$\rho^3\tau$	ρ^2	ρ	ε	ρ^3
$\rho^3\tau$	$\rho^3\tau$	$\rho^2\tau$	$\rho\tau$	τ	ρ^3	ρ^2	ρ	ε

The following formulas aid in the verification of the table:

$$\rho^4 = \varepsilon, \qquad \tau^2 = \varepsilon, \qquad \tau\rho^i = \rho^{-i}\tau$$

(see Exercise 7–10).

There is a geometrical interpretation of the group D_4. Consider a square oriented in the plane like this:



With the corners numbered as indicated, the permutation $\rho = (1, 2, 3, 4)$ corresponds to 90° clockwise rotation of the square. The corner labeled 1 is sent to the 2-position ($1 \mapsto 2$), the corner labeled 2 is sent to the 3-position

$(2 \mapsto 3)$, the corner labeled 3 is sent to the 4-position $(3 \mapsto 4)$, and the corner labeled 4 is sent to the 1-position $(4 \mapsto 1)$.

Similarly, the permutation $\tau = (2,4)$ corresponds to a flip of the square about the y-axis. The corner labeled 2 is sent to the 4-position $(2 \mapsto 4)$, the corner labeled 4 is sent to the 2-position $(4 \mapsto 2)$ and the other two corners are fixed $(1 \mapsto 1,\ 3 \mapsto 3)$.

The reader can check that the group elements have these geometrical interpretations:

$\varepsilon = (1)$	no movement
$\rho = (1,2,3,4)$	90° clockwise rotation
$\rho^2 = (1,3)(2,4)$	180° clockwise rotation
$\rho^3 = (1,4,3,2)$	270° clockwise rotation
$\tau = (2,4)$	flip about y-axis
$\rho\tau = (1,2)(3,4)$	flip about line $y = x$
$\rho^2\tau = (1,3)$	flip about x-axis
$\rho^3\tau = (1,4)(2,3)$	flip about line $y = -x$.

These movements are called "symmetries of the square." They represent all possible ways of reorienting the square.

The definition of D_4 generalizes. Let n be any integer greater than two. The set D_n of all symmetries of a regular n-gon is a subgroup of the symmetric group S_n called the **dihedral group of degree** n.

So D_3 is the group of symmetries of an equilateral triangle; D_4, a square; D_5, a regular pentagon; etc.

We have $D_n = \{\rho^i\tau^j \,|\, 0 \le i < n, 0 \le j < 2\}$, where ρ is a rotation and τ is a flip. In particular $|D_n| = 2n$.

7.7 Equivalence relation

Let S be a set. A **relation** on S is a subset R of $S \times S = \{(x,y) \,|\, x,y \in S\}$. If $(x,y) \in R$, we write xRy and if $(x,y) \notin R$, we write $x\not Ry$. Informally, R is a rule that some pairs (x,y) of elements satisfy and some don't.

For example, $<$ is a relation on $\mathbf{Z}$. We have $3 < 5$, but $4 \not< 1$.

A relation $\sim$ on S is an **equivalence relation** if it satisfies these three properties:

- (Reflexive) $x \sim x$ for all $x \in S$;
- (Symmetric) if $x \sim y$, then $y \sim x$ $(x, y \in S)$;
- (Transitive) if $x \sim y$ and $y \sim z$, then $x \sim z$ $(x, y, z \in S)$.

If $\sim$ is an equivalence relation on S and $x \sim y$, we say that x is **equivalent** to y.

Equality $(=)$ is an equivalence relation on the set $\mathbf{Z}$.

7.7.1 Example Let $\sim$ be the relation on $\mathbf{Z}$ given by $x \sim y$ if $x - y \in 3\mathbf{Z}$, where $3\mathbf{Z} = \{3m \mid m \in \mathbf{Z}\}$. Prove that $\sim$ is an equivalence relation.

Solution We check the three properties:

(Reflexive) For $x \in \mathbf{Z}$, we have $x - x = 0 = 3(0) \in 3\mathbf{Z}$, so $x \sim x$.

(Symmetric) Let $x, y \in \mathbf{Z}$ and assume that $x \sim y$. (Must show that $y \sim x$.) By the definition of $\sim$, we have $x - y \in 3\mathbf{Z}$, so that $x - y = 3m$ for some $m \in \mathbf{Z}$. Therefore, $y - x = -3m = 3(-m) \in 3\mathbf{Z}$, implying $y \sim x$.

(Transitive) Let $x, y, z \in \mathbf{Z}$ and assume that $x \sim y$ and $y \sim z$. (Must show that $x \sim z$.) By the definition of $\sim$, we have $x - y \in 3\mathbf{Z}$ and $y - z \in 3\mathbf{Z}$, so that $x - y = 3m$ and $y - z = 3n$ for some $m, n \in \mathbf{Z}$. Therefore, $x - z = (x - y) + (y - z) = 3m + 3n = 3(m + n) \in 3\mathbf{Z}$, implying $x \sim z$.

This shows that $\sim$ is an equivalence relation on $\mathbf{Z}$. □

Let $\sim$ be an equivalence relation on the set S. The **equivalence class** of $x \in S$, denoted $[x]$, is the set of all elements of S that are equivalent to x:

$$[x] = \{y \in S \mid y \sim x\}.$$

7.7.2 Theorem. *For $x, y \in S$, we have $[x] = [y]$ if and only if $x \sim y$.*

Proof. See Exercise 7–13. □

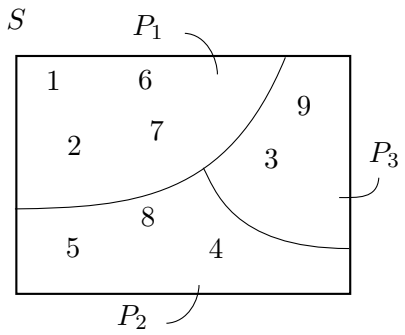
A notion closely related to an equivalence relation on the set S is a "partition" of S. If $S = \{1, 2, 3, 4, 5, 6, 7, 8, 9\}$, then putting

$$P_1 = \{1, 2, 6, 7\}, \quad P_2 = \{5, 8, 4\}, \quad P_3 = \{3, 9\}$$

we get a partition

$$\mathcal{P} = \{P_1, P_2, P_3\}$$

of S. This is visualized as follows:



So informally, a partition of S is a way of breaking S up into pieces. Here is the formal definition:

A **partition** of the set S is a set $\mathcal{P}$ of subsets of S satisfying the following properties:

- (Union) $\bigcup_{P \in \mathcal{P}} P = S$,
- (Disjoint) if $P, Q \in \mathcal{P}$ and $P \neq Q$, then $P \cap Q = \emptyset$.

The elements of $\mathcal{P}$ are called the **cells** of the partition. The properties imply that each element of S lies in a unique cell of the partition.

The following theorem says that any equivalence relation on S gives rise to a partition of S and, conversely, any partition of S gives rise to an equivalence relation on S.

7.7.3 Theorem.

(i) *If $\sim$ is an equivalence relation on S, then $\{[x] \mid x \in S\}$ is a partition of S, where $[x]$ denotes the equivalence class of x relative to $\sim$.*

(ii) *If $\mathcal{P}$ is a partition of S and if, for $x, y \in S$, we put $x \sim y$ if x and y lie in the same cell of $\mathcal{P}$, then $\sim$ is an equivalence relation on S.*

Proof. (i) Let $\sim$ be an equivalence relation on S. We show that $\mathcal{P} = \{[x] \,|\, x \in S\}$ is a partition of S by checking the two properties.

(Union) Let $x \in S$. By the reflexive property of $\sim$, we have $x \sim x$, so $x \in [x]$. Since $[x] \in \mathcal{P}$, we get $x \in \bigcup_{P \in \mathcal{P}} P$. This shows that $S = \bigcup_{P \in \mathcal{P}} P$. (It shows the inclusion $\subseteq$ and the other inclusion is immediate.)

(Disjoint) Let $P, Q \in \mathcal{P}$ and assume that $P \cap Q \neq \emptyset$. (We are proving the contrapositive of this property, so we need to show that $P = Q$.) Then there exists $x \in P \cap Q$. We have $P = [y]$ and $Q = [z]$ for some $y, z \in S$. Now $x \in P = [y]$, so $x \sim y$. Similarly, $x \in Q = [z]$, so $x \sim z$. By symmetry of $\sim$ we have $y \sim x$ and then by transitivity of $\sim$ we have $y \sim z$. Therefore, by Theorem 7.7.2, we get $P = [y] = [z] = Q$.

This finishes the proof that $\mathcal{P}$ is a partition of S.

(ii) Let $\mathcal{P}$ be a partition of S and let $\sim$ be defined as stated. We show that $\sim$ is an equivalence relation by checking the three properties.

(Reflexive) Let $x \in S$. Since the union of the cells of the partition $\mathcal{P}$ is all of S, x must lie in some cell. Therefore, $x \sim x$ (since x and x lie in the same cell).

(Symmetric) Let $x, y \in S$ and assume that $x \sim y$. Then x and y lie in the same cell of the partition $\mathcal{P}$. Therefore y and x lie in the same cell of the partition, implying $y \sim x$.

(Transitive) Let $x, y, z \in S$ and assume $x \sim y$ and $y \sim z$. Then $x, y \in P$ and $y, z \in Q$ for some cells P and Q of the partition $\mathcal{P}$. Since $y \in P \cap Q$, we have $P \cap Q \neq \emptyset$, so $P = Q$. Therefore, $x, z \in P$, so that $x \sim z$.

This finishes the proof that $\sim$ is an equivalence relation on S. □

7.7.4 Example Find the partition of $\mathbf{Z}$ corresponding to the equivalence relation of Example 7.7.1.

Solution The cells of the partition are the equivalence classes $[x]$ with $x \in \mathbf{Z}$.

Let $x \in \mathbf{Z}$. We claim that $[x] = 3\mathbf{Z} + x := \{m + x \,|\, m \in 3\mathbf{Z}\})$. For $y \in \mathbf{Z}$,

we have

$$\begin{aligned} y \in [x] &\iff y \sim x \\ &\iff y - x \in 3\mathbf{Z}, \\ &\iff y \in 3\mathbf{Z} + x, \end{aligned}$$

so $[x] = 3\mathbf{Z} + x$ as claimed. In particular,

$$\begin{aligned} [0] &= 3\mathbf{Z} + 0 = \{\dots, -6, -3, 0, 3, 6, \dots\}, \\ [1] &= 3\mathbf{Z} + 1 = \{\dots, -5, -2, 1, 4, 7, \dots\}, \\ [2] &= 3\mathbf{Z} + 2 = \{\dots, -4, -1, 2, 5, 8, \dots\}. \end{aligned}$$

Therefore, the corresponding partition of $\mathbf{Z}$ is $\{[0], [1], [2]\}$. □

7.8 Orbit

Let σ be a fixed element of S_n. Define a relation $\sim$ on the set $\{1, 2, \dots, n\}$ by putting

$$x \sim y \quad \text{if } x = \sigma^k(y) \text{ for some } k \in \mathbf{Z}.$$

7.8.1 Theorem. *$\sim$ is an equivalence relation on $\{1, 2, \dots, n\}$.*

Proof. We check the three properties:

(Reflexive) For $x \in \{1, 2, \dots, n\}$, we have $x = \varepsilon(x) = \sigma^0(x)$, so $x \sim x$.

(Symmetric) Let $x, y \in \{1, 2, \dots, n\}$ and assume that $x \sim y$. (Must show that $y \sim x$.) By the definition of $\sim$, we have $x = \sigma^k(y)$ for some $k \in \mathbf{Z}$. Then $y = \sigma^{-k}(x)$, implying $y \sim x$.

(Transitive) See Exercise 7–14. □

For $x \in \{1, 2, \dots, n\}$, the equivalence class $[x]$ of x relative to the equivalence relation $\sim$ is called the **orbit** of x relative to σ.

Consider the special case $\sigma = (1, 4, 2, 7)(3, 9, 6)(5)(8) \in S_9$. With the equivalence relation $\sim$ as defined above, we claim that $[1] = \{1, 4, 2, 7\}$. We

have

$$\begin{aligned} 1 = \sigma^0(1) &\quad \Rightarrow \quad 1 \sim 1 \\ 4 = \sigma^1(1) &\quad \Rightarrow \quad 4 \sim 1 \\ 2 = \sigma^2(1) &\quad \Rightarrow \quad 2 \sim 1 \\ 7 = \sigma^3(1) &\quad \Rightarrow \quad 7 \sim 1 \end{aligned}$$

and for any other $k \in \mathbf{Z}$, we get that $\sigma^k(1)$ is either $1, 4, 2$, or 7. Therefore,

$$[1] = \{1, 4, 2, 7\}.$$

Similarly, $[3] = \{3, 9, 6\}$, $[5] = \{5\}$, and $[8] = \{8\}$.

This shows that the orbits of the elements of $X = \{1, 2, \ldots, 9\}$ relative to σ are precisely the subsets of X consisting of the cycle entries in the decomposition of σ as a product of disjoint cycles.

In particular, the partition of X corresponding to the equivalence relation $\sim$ determined by $\sigma = (1, 4, 2, 7)(3, 9, 6)(5)(8)$ is

$$\big\{\{1, 4, 2, 7\}, \{3, 9, 6\}, \{5\}, \{8\}\big\}.$$

This observation generalizes to give a similar result for any element σ of S_n.

7 – Exercises

7–1 Let σ be the element of S_9 given by

$$\sigma = (1, 6, 2, 8, 3, 4).$$

Find the following:

(a) $\sigma(8)$,

(b) $\sigma(4)$,

(c) $\sigma(5)$,

(d) $\sigma^{-1}(2)$,

(e) $\sigma^4(3)$.

7–2 Let σ be the element of S_9 given by

$$\sigma = (2, 7, 9, 8)(2, 7, 4)(3, 4, 8).$$

Find the following:

(a) $\sigma(4)$,

(b) $\sigma(3)$,

(c) $\sigma(5)$,

(d) $\sigma^{-1}(9)$,

(e) $\sigma^2(2)$.

7–3 Let $\sigma = (i_1, i_2, \ldots, i_r)$ be a cycle in S_n. Prove that for every τ in S_n, we have $\tau\sigma\tau^{-1} = (\tau(i_1), \tau(i_2), \ldots, \tau(i_r))$.

7–4

(a) Find ord(σ), where $\sigma = (1, 5, 2) \in S_5$.

(b) Generalize part (a) by stating the order of an r-cycle. (No proof required.)

(c) Let σ_1 be a 4-cycle and let σ_2 be a 6-cycle and assume that σ_1 and σ_2 are disjoint. Find the order of $\sigma_1\sigma_2$. (Hint: Use Theorem 7.2.1.)

(d) Let $\sigma_1, \sigma_2, \ldots, \sigma_m$ be disjoint cycles and let $r_i = \text{length}(\sigma_i)$ $(1 \leq i \leq m)$. Generalize part (c) by stating the order of the composition $\sigma_1\sigma_2 \cdots \sigma_m$ in terms of the r_i. (No proof required.)

7–5 Let σ be the element of S_{10} given by

$$\sigma = \begin{pmatrix} 1 & 2 & 3 & 4 & 5 & 6 & 7 & 8 & 9 & 10 \\ 8 & 1 & 7 & 4 & 9 & 10 & 5 & 2 & 3 & 6 \end{pmatrix}.$$

(a) Write σ as a product of disjoint cycles.

(b) Verify that σ and the product of disjoint cycles found in part (a) both send the number 5 to the same output.

7–6 Let $\sigma \in S_n$. Let $\sigma_1\sigma_2\cdots\sigma_m$ be the product of disjoint cycles as found using the algorithm described in Section 7.2 applied to σ. Explain why $\sigma = \sigma_1\sigma_2\cdots\sigma_m$.

7–7 Let σ be the element of S_9 given by

$$\sigma = \begin{pmatrix} 1 & 2 & 3 & 4 & 5 & 6 & 7 & 8 & 9 \\ 4 & 2 & 1 & 6 & 8 & 9 & 5 & 7 & 3 \end{pmatrix}.$$

(a) Determine whether σ is even or odd.

(b) Write σ as a product of transpositions in two distinct ways.

(c) Compute $N(\sigma)$ as defined in the proof of Theorem 7.4.1 and verify that it has the same parity as σ (i.e., both even or both odd).

7–8 Prove that $|A_n| = n!/2$ if $n \geq 2$. (The restriction on n is essential since $|A_1| = 1$.)

HINT: For $\sigma \in S_n$, use the fact that if σ is even, then $(1,2)\sigma$ is odd to define a bijection between the set of even elements of S_n and the set of odd elements of S_n.

7–9 Prove that if $\tau \in A_n$ and $\sigma \in S_n$, then $\sigma^{-1}\tau\sigma \in A_n$.

7–10 Put $\rho = (1,2,3,4)$ and $\tau = (2,4)$ as in the definition of the dihedral group D_4 (Section 7.6).

(a) Verify that

$$\rho^4 = \varepsilon \quad \text{and} \quad \tau^2 = \varepsilon.$$

Hint: You may use an earlier exercise.

(b) Give a proof by induction that $\tau\rho^i = \rho^{-i}\tau$ for all $i \in \mathbf{N}$.

Method: First establish the case $i = 1$. Then let $i > 1$ and establish the formula under the assumption that the formula holds with i replaced by $i - 1$ ("Induction Hypothesis").

(c) Verify the following products as stated in the multiplication table of the dihedral group:

$$\rho^2\rho^3 = \rho, \quad \tau(\rho\tau) = \rho^3, \quad (\rho^2\tau)\rho = \rho\tau.$$

Hint: Use parts (a) and (b).

7–11

(a) Draw a subgroup diagram for the dihedral group D_4 showing all of its cyclic subgroups.

(b) Find a proper, noncyclic subgroup of D_4.

7–12 Let G be a group and let H be a subgroup of G. Define a relation $\sim$ on G by putting $x \sim y$ if $x^{-1}y \in H$. Prove that $\sim$ is an equivalence relation.

7–13 Let S be a set, let $\sim$ be an equivalence relation on S, and let $x, y \in S$. Prove that $[x] = [y]$ if and only if $x \sim y$.

7–14 Let $\sigma \in S_n$ and let $\sim$ be the relation on $\{1, 2, \ldots, n\}$ defined by putting $x \sim y$ if $x = \sigma^k(y)$ for some $k \in \mathbf{Z}$. Prove that $\sim$ satisfies the transitive property: If $x \sim y$ and $y \sim z$, then $x \sim z \quad (x, y, z \in \{1, 2, \ldots, n\})$.

8 Coset

8.1 Definition

Let G be a group, let H be a subgroup of G, and let $a \in G$. The **left coset** of H containing a is the set

$$aH = \{ah \,|\, h \in H\},$$

and the **right coset** of H containing a is the set

$$Ha = \{ha \,|\, h \in H\}.$$

Note that, since $e \in H$, these sets do indeed each contain a.

If the notation for the binary operation of G is $+$, then these cosets are written

$$a + H = \{a + h \,|\, h \in H\}$$

and

$$H + a = \{h + a \,|\, h \in H\},$$

respectively.

8.2 Examples of cosets

8.2.1 Example Let $G = S_3$ and $H = \langle \rho \rangle = \{\varepsilon, \rho\}$, where $\rho = (1, 2)$. Find the left coset of H containing the element ε, as well as the one containing $\sigma = (1, 3)$, and the one containing $\tau = (2, 3)$.

Solution We have

$$\begin{aligned} \varepsilon H &= \{\varepsilon\varepsilon, \varepsilon\rho\} = \{\varepsilon, (1, 2)\} = H, \\ \sigma H &= \{\sigma\varepsilon, \sigma\rho\} = \{(1, 3), (1, 2, 3)\}, \\ \tau H &= \{\tau\varepsilon, \tau\rho\} = \{(2, 3), (1, 3, 2)\}. \end{aligned}$$

□

8.2.2 Example Let $G = \mathbf{Z}$ and $H = \langle 3 \rangle = 3\mathbf{Z}$. Find the left cosets of H containing 0, 1, 2, 3, and 4, respectively.

Solution We have

$$\begin{aligned}
0 + H &= \{\ldots, -6, -3, 0, 3, 6, \ldots\} = H,\\
1 + H &= \{\ldots, -5, -2, 1, 4, 7, \ldots\},\\
2 + H &= \{\ldots, -4, -1, 2, 5, 8, \ldots\},\\
3 + H &= \{\ldots, -3, 0, 3, 6, 9 \ldots\} = H,\\
4 + H &= \{\ldots, -2, 1, 4, 7, 10, \ldots\} = 1 + H.
\end{aligned}$$

□

This example shows that it is possible to have $a + H = b + H$ with $a \neq b$.

8.2.3 Example Let $G = \mathbf{R} \oplus \mathbf{R} = \{(x, y) \mid x, y \in \mathbf{R}\}$ and let $H = \{(0, y) \mid y \in \mathbf{R}\}$ (y-axis). Then H is a subgroup of G. Give a geometrical description of the left cosets of H.

Solution Let (a, b) be an arbitrary element of G. The left coset of H containing (a, b) is

$$\begin{aligned}
(a, b) + H &= \{(a, b) + h \mid h \in H\}\\
&= \{(a, b) + (0, y) \mid y \in \mathbf{R}\}\\
&= \{(a, b + y) \mid y \in \mathbf{R}\}\\
&= \{(a, y) \mid y \in \mathbf{R}\},
\end{aligned}$$

which is the vertical line passing through the x-axis at the number a.

Therefore, the left cosets of H are the vertical lines in the plane. □

8.2.4 Example Let G be the dihedral group

$$D_4 = \{\varepsilon, \rho, \rho^2, \rho^3, \tau, \rho\tau, \rho^2\tau, \rho^3\tau\}$$

(see Section 7.6) and let $H = \langle\tau\rangle = \{\varepsilon, \tau\}$. Find the left and right cosets of H containing ρ.

Solution We have

$$\begin{aligned}
\rho H &= \{\rho, \rho\tau\}\\
H\rho &= \{\rho, \tau\rho\} = \{\rho, \rho^3\tau\}.
\end{aligned}$$

□

This example shows that it is possible to have $aH \neq Ha$. In other words, left and right cosets need not coincide.

8.3 Equality of cosets

Let G be a group, let H be a subgroup of G, and let $a, b \in G$. As Example 8.2.2 shows, it is possible to have $aH = bH$ with $a \neq b$. Here is a useful criterion for equality of cosets:

8.3.1 Theorem.

(i) *$aH = bH$ if and only if $a^{-1}b \in H$,*

(ii) *$Ha = Hb$ if and only if $ab^{-1} \in H$.*

Proof. (i) ($\Rightarrow$) Assume that $aH = bH$. Then $b = be \in bH = aH$ so $b = ah$ for some $h \in H$. Thus, $a^{-1}b = h \in H$.

($\Leftarrow$) Now assume that $a^{-1}b \in H$. (Must show $aH = bH$.)

($\supseteq$) Let $x \in bH$. Then $x = bh$ for some $h \in H$, so

$$x = bh = a(a^{-1}b)h \in aH$$

since H is closed under multiplication. Thus, $aH \supseteq bH$.

($\subseteq$) Since H is closed under inversion, our assumption implies $b^{-1}a = (a^{-1}b)^{-1} \in H$, so the preceding argument, with the roles of a and b switched, gives $aH \subseteq bH$ as well.

Therefore, $aH = bH$.

The proof of (ii) is similar. □

For example, it was observed in Example 8.2.2 that if $H = 3\mathbf{Z} \leq \mathbf{Z}$, then $4 + H = 1 + H$ and we check that $-4 + 1 = -3$ is indeed in H in agreement with part (i) of the theorem (noting that the additive notation of $a^{-1}b$ is $-a + b$).

The following is a useful consequence of the previous theorem.

8.3.2 Corollary.

(i) $aH = H$ *if and only if* $a \in H$,

(ii) $Ha = H$ *if and only if* $a \in H$.

Proof. (i) We have

$$\begin{aligned} aH = H \quad &\Leftrightarrow \quad aH = eH \\ &\Leftrightarrow \quad a^{-1}e \in H \\ &\Leftrightarrow \quad a^{-1} \in H \\ &\Leftrightarrow \quad a \in H. \end{aligned}$$

The proof of (ii) is similar. □

8.4 Congruence modulo a subgroup

Let G be a group and let H be a subgroup of G. Define a relation $\equiv_l$ on G by putting $a \equiv_l b$ if $a^{-1}b \in H$. Then $\equiv_l$ is an equivalence relation on G (Exercise 7–12), called **left congruence modulo** H. Denote by $[a]_l$ the equivalence class of $a \in G$ relative to $\equiv_l$. Thus, $[a]_l = \{b \in G \mid b \equiv_l a\}$.

Similarly, **right congruence modulo** H is the equivalence relation $\equiv_r$ on G obtained by putting $a \equiv_r b$ if $ab^{-1} \in H$. The equivalence class of $a \in G$ relative to $\equiv_r$ is denoted $[a]_r$.

$a \equiv_l b$ is written $a \equiv_l b \mod H$ if the subgroup H is not clear from the context, and similarly for $\equiv_r$.

The next theorem says that the equivalence class of an element a relative to left congruence modulo H is precisely the left coset of H containing a (and a similar statement with right replacing left).

8.4.1 Theorem. *For* $a \in G$

(i) $[a]_l = aH$,

(ii) $[a]_r = Ha$.

Proof. (i) Let $x \in G$. Then

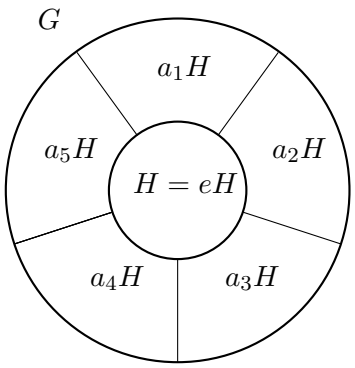
$$\begin{aligned} x \in [a]_l &\Leftrightarrow x \equiv_l a \\ &\Leftrightarrow a \equiv_l x \\ &\Leftrightarrow a^{-1}x \in H \\ &\Leftrightarrow a^{-1}x = h \text{ for some } h \in H \\ &\Leftrightarrow x = ah \text{ for some } h \in H \\ &\Leftrightarrow x \in aH. \end{aligned}$$

Thus, $[a]_l = aH$.

The proof of (ii) is similar. □

8.5 Cosets partition the group

Let G be a group and let H be a subgroup of G. The theorem of this section says that the left cosets of H form a partition of G:



8.5.1 Theorem. *The set of left cosets of H is a partition of G, that is,*

(i) $G = \bigcup_{a \in G} aH$,

(ii) *if $a, b \in G$ and $aH \neq bH$, then $aH \cap bH = \emptyset$.*

Proof. By Theorem 8.4.1, the set of left cosets of H is precisely the set of equivalence classes of G relative to left congruence modulo H (i.e. $\equiv_l$). So the set of left cosets of H is the partition of G corresponding to this equivalence relation $\equiv_l$. □

(The set of right cosets of H also forms a partition of G.)

Example 8.2.2 provides an illustration of this theorem with $G = \mathbf{Z}$ and $H = 3\mathbf{Z}$. The set of left cosets is $\{a + H \mid a \in \mathbf{Z}\} = \{0 + H, 1 + H, 2 + H\}$. $\mathbf{Z}$ is the union of $0 + H$, $1 + H$, and $2 + H$, and these cosets are pairwise disjoint.

8.6 Cosets have same cardinality

Let G be a group and let H be a subgroup of G.

8.6.1 Theorem. *For all $a \in G$,*

(i) $|aH| = |H|$,

(ii) $|Ha| = |H|$.

Proof. (i) Let $a \in G$. Define $f : H \to aH$ by $f(h) = ah$. We claim that f is a bijection.

(f injective?) Let $h, k \in H$ and assume that $f(h) = f(k)$. Then $ah = ak$, so $h = k$ by left cancellation. Therefore, f is injective.

(f surjective?) Let $x \in aH$. Then $x = ah$ for some $h \in H$ and $f(h) = ah = x$. Therefore, f is surjective.

This shows that f is a bijection. We conclude that $|aH| = |H|$.

The proof of (ii) is similar. □

A consequence of this theorem is that any two left cosets of H have the same cardinality (since each has the same cardinality as H). Another consequence is that any left coset of H has the same cardinality as any right coset of H (again, since each has the same cardinality as H).

8.7 Index of subgroup

Let G be a group and let H be a subgroup of G. Let L be the set of left cosets of H and let R be the set of right cosets of H:

$$L = \{aH \mid a \in G\},$$
$$R = \{Ha \mid a \in G\}.$$

Since left and right cosets need not coincide (see Example 8.2.4), it is possible for these sets to be unequal. However, the next theorem says that they at least have the same cardinality.

8.7.1 Theorem. $|L| = |R|$.

Proof. Define $f : L \to R$ by $f(aH) = Ha^{-1}$. We claim that f is a (well-defined) bijection.

(f well defined?) The issue is this: If the same input is written two ways, like aH and bH, then will the corresponding outputs Ha^{-1} and Hb^{-1} necessarily be the same? So let $a, b \in G$ and suppose $aH = bH$. By Theorem 8.3.1, we have $a^{-1}b \in H$. Rewriting this element as $a^{-1}(b^{-1})^{-1}$ we have $a^{-1}(b^{-1})^{-1} \in H$, which gives $Ha^{-1} = Hb^{-1}$, again by Theorem 8.3.1. Therefore, f is well defined.

(f injective?) Let $a, b \in G$ and assume that $f(aH) = f(bH)$. Then $Ha^{-1} = Hb^{-1}$, implying $a^{-1}(b^{-1})^{-1} \in H$. But this gives $a^{-1}b \in H$, so that $aH = bH$. Therefore, f is injective.

(f surjective?) Let $Ha \in R$. Then $a^{-1}H \in L$ and $f(a^{-1}H) = H(a^{-1})^{-1} = Ha$. Therefore, f is surjective.

This finishes the proof that f is a well-defined bijection. We conclude that $|L| = |R|$. □

The **index** of the subgroup H in G, denoted $|G : H|$, is the cardinality of the set of left cosets of H in G, that is, $|G : H| = |\{aH \mid a \in G\}|$. According to the theorem, $|G : H|$ is also the cardinality of the set of right cosets of H in G.

8.7.2 Example Find the index $|\mathbf{Z} : 3\mathbf{Z}|$.

Solution In Example 8.2.2, we found that the distinct left cosets of $3\mathbf{Z}$ in $\mathbf{Z}$ are

$$\begin{aligned} 0 + 3\mathbf{Z} &= \{\ldots, -6, -3, 0, 3, 6, \ldots\}, \\ 1 + 3\mathbf{Z} &= \{\ldots, -5, -2, 1, 4, 7, \ldots\}, \\ 2 + 3\mathbf{Z} &= \{\ldots, -4, -1, 2, 5, 8, \ldots\}. \end{aligned}$$

Since there are three cosets, we have $|\mathbf{Z} : 3\mathbf{Z}| = 3$. □

8.8 Lagrange's theorem

Let G be a *finite* group and let H be a subgroup of G. Lagrange's theorem says that the order of G is the product of the index of H in G and the order of H.

8.8.1 Theorem (Lagrange's Theorem).

$$|G| = |G : H| \cdot |H|.$$

Proof. Let $a_1H, a_2H, \ldots, a_nH$ be the distinct left cosets of H in G. By Theorem 8.5.1, these cosets form a partition of G. By Theorem 8.6.1, each of these cosets has the same number of elements as does H. Therefore,

$$|G| = \sum_{i=1}^{n} |a_iH| = \sum_{i=1}^{n} |H| = n \cdot |H| = |G : H| \cdot |H|.$$

□

For instance, if $G = \mathbf{Z}_{12}$ and $H = \langle 3 \rangle = \{0, 3, 6, 9\}$, then the set of left cosets of H in G is $\{0 + H, 1 + H, 2 + H\}$, so $|G| = 12 = 3 \cdot 4 = |G : H| \cdot |H|$ in agreement with the theorem.

The theorem gives a formula for the index of H in G:

$$|G : H| = \frac{|G|}{|H|}.$$

We have assumed, for the sake of simplicity, that G is a finite group. But actually, Lagrange's theorem is valid for an arbitrary group G given a suitable interpretation of the product $|G : H||H|$ when either factor is infinite. By definition, $|G : H| = |L|$ where L is the set of left cosets of H in G. So Lagrange's theorem says $|G| = |L||H|$ and we interpret $|L||H|$ to mean $|L \times H|$, where $L \times H = \{(l, h) \,|\, l \in L, h \in H\}$.

8.9 Corollaries of Lagrange's theorem

Let G be a *finite* group.

8.9.1 Corollary. *If H is a subgroup of G, then $|H|$ divides $|G|$.*

Proof. Let H be a subgroup of G. By Lagrange's theorem, $|G| = |G : H| \cdot |H|$, and since $|G : H|$ is an integer the claim follows. □

For instance, a group of order 12 can only have subgroups of orders $1, 2, 3, 4, 6$, and 12.

8.9.2 Corollary. *If the order of G is prime, then G is cyclic.*

Proof. Assume that the order of G is prime. Since a prime is at least two, G has a nonidentity element a. The order of the subgroup $\langle a \rangle$ generated by a is greater than one and divides $|G|$ by Corollary 8.9.1. Therefore, $|\langle a \rangle| = |G|$ and we have $G = \langle a \rangle$. Thus, G is cyclic. □

8.9.3 Corollary. *The order of each element of G divides the order of G.*

Proof. The order of an element equals the number of elements in the cyclic subgroup generated by that element (see Theorem 5.4.5), so the claim follows immediately from Corollary 8.9.1. □

8.9.4 Corollary. *For each $x \in G$ we have $x^{|G|} = e$.*

Proof. Let $x \in G$. By Corollary 8.9.3, $|G| = \text{ord}(x)n$ for some $n \in \mathbf{N}$. Thus $x^{|G|} = (x^{\text{ord}(x)})^n = e^n = e$. □

8 – Exercises

8–1 Let $G = \mathbf{Z}_{12}$.

(a) Find the left cosets of $H = \langle 4 \rangle$.

(b) Find the left cosets of $H = \langle 6 \rangle$.

8–2 Let G be a group and let H be a subgroup of G. Prove that $aH = Ha$ for every $a \in G$ if and only if $a^{-1}ha \in H$ for every $a \in G$ and every $h \in H$.

8–3

(a) Let $H = \langle 3 \rangle$ in the group $\mathbf{Z}_{12}$. Determine whether $4 \equiv_r 10 \mod H$.

(b) Let $H = \langle \tau \rangle$ in the dihedral group D_4. Determine whether $\rho \equiv_l \rho\tau \mod H$ and also whether $\rho \equiv_r \rho\tau \mod H$.

(c) Let $H = A_n$ (alternating group) and let $\sigma, \tau \in S_n$. Complete the statement

$$\text{“}\sigma \equiv_l \tau \mod H \text{ if and only if } \ldots\text{”}$$

by filling in the dots with a condition expressed in terms of the parities (even or odd) of σ and τ. Prove your claim.

8–4 Let G be a group and let H be a subgroup of G. Let $\mathcal{P} = \{aH \mid a \in G\}$. Give a direct proof (i.e., without using equivalence classes as in the proof of Theorem 8.5.1) that $\mathcal{P}$ is a partition of G.

8–5 Let $H = \mathrm{SL}_n(\mathbf{R})$ be the subgroup of $\mathrm{GL}_n(\mathbf{R})$ consisting of $n \times n$ matrices having determinant 1. For $d \in \mathbf{R}$, let I_d denote the $n \times n$ identity matrix with the upper left entry replaced by d:

$$I_d = \begin{bmatrix} d & 0 & 0 & \cdots & 0 & 0 \\ 0 & 1 & 0 & \cdots & 0 & 0 \\ 0 & 0 & 1 & \cdots & 0 & 0 \\ \vdots & \vdots & \vdots & \ddots & \vdots & \vdots \\ 0 & 0 & 0 & \cdots & 1 & 0 \\ 0 & 0 & 0 & \cdots & 0 & 1 \end{bmatrix}.$$

Prove that the cosets $I_d H$, $d \in \mathbf{R}^\times$, are distinct and that each left coset of H is equal to one of these.

8–6 Find the following indices:

(a) $|\mathbf{Z}_{18} : \langle 4 \rangle|$,

(b) $|2\mathbf{Z} : 8\mathbf{Z}|$,

(c) $|S_5 : \langle \sigma \rangle|$, where $\sigma = (1, 2)(3, 4, 5)$,

(d) $|\mathrm{GL}_n(\mathbf{R}) : \mathrm{SL}_n(\mathbf{R})|$.

8–7 Let G be a group, let H and K be finite subgroups of G, and assume that $\gcd(|H|, |K|) = 1$. Prove that $H \cap K = \{e\}$.

HINT: Use Exercise 5–7 and a corollary of Lagrange's theorem.

8–8 Let G be an abelian group of order $2m$ with m odd. Prove that G has a unique element of order two.

HINT: Use Exercise 4–9 and a corollary of Lagrange's theorem.

9 Normal subgroup

If G is a group and H is a subgroup of G it is sometimes possible to define a natural binary operation on the set of left cosets of H in G in such a way that this set becomes a group. This construction requires that H be a "normal" subgroup of G. In this section, we study the concept of normality.

9.1 Definition and examples

Let G be a group.

> A subgroup N of G is **normal**, written $N \lhd G$, if $g^{-1}ng \in N$ for every $n \in N$ and every $g \in G$.

9.1.1 Example Show that if G is abelian, then every subgroup of G is normal.

Solution Assume that G is abelian and let N be a subgroup of G. Let $n \in N$ and $g \in G$. (Must show that $g^{-1}ng \in N$.) We have

$$g^{-1}ng = g^{-1}gn = en = n \in N.$$

Therefore, N is normal. □

9.1.2 Example Let $n \in \mathbf{N}$. Prove that $A_n \lhd S_n$.

Solution This proof was the point of Exercise 7–9. Here is the argument.

Let $\tau \in A_n$ and $\sigma \in S_n$. We can write

$$\tau = \tau_1\tau_2\cdots\tau_t \quad \text{and} \quad \sigma = \sigma_1\sigma_2\cdots\sigma_s$$

for some transpositions τ_i and σ_i with t even (since $\tau \in A_n$). Using Theorem 4.7.2 and then the fact that each transposition is its own inverse, we get

$$\begin{aligned}\sigma^{-1} &= (\sigma_1\sigma_2\cdots\sigma_s)^{-1} \\ &= \sigma_s^{-1}\sigma_{s-1}^{-1}\cdots\sigma_1^{-1} \\ &= \sigma_s\sigma_{s-1}\cdots\sigma_1.\end{aligned}$$

Hence

$$\sigma^{-1}\tau\sigma = \sigma_s\sigma_{s-1}\cdots\sigma_1\tau_1\tau_2\cdots\tau_t\sigma_1\sigma_2\cdots\sigma_s.$$

This expresses $\sigma^{-1}\tau\sigma$ as a product of transpositions. The number of factors is $2s+t$, which is even since t is even. We conclude that $\sigma^{-1}\tau\sigma$ is even, that is, $\sigma^{-1}\tau\sigma \in A_n$.

Therefore, $A_n \lhd S_n$. □

9.1.3 Example Let $\tau = (2,4) \in D_4$ and put $H = \langle\tau\rangle = \{\varepsilon, \tau\}$. Prove that $H \not\lhd D_4$.

Solution We have $\tau \in H$ and $\rho = (1,2,3,4) \in D_4$, but

$$\rho^{-1}\tau\rho = \rho^{-1}\rho^{-1}\tau = \rho^{-2}\tau = \rho^2\tau \notin H,$$

where we have used the formulas in Exercise 7–10. Therefore, $H \not\lhd D_4$. □

9.2 Normality and left/right cosets

Let G be a group and let H be a subgroup of G.

9.2.1 Theorem. *$H \lhd G$ if and only if $aH = Ha$ for every $a \in G$.*

Proof.

($\Rightarrow$) Assume that $H \lhd G$. Let $a \in G$. (Must show that $aH = Ha$.)

> ($\subseteq$) Let $x \in aH$. Then $x = ah$ for some $h \in H$. By assumption, $aha^{-1} = (a^{-1})^{-1}ha^{-1} \in H$, so $x = ah = (aha^{-1})a \in Ha$.
>
> ($\supseteq$) Let $x \in Ha$. Then $x = ha$ for some $h \in H$. By assumption, $a^{-1}ha \in H$, so $x = ha = a(a^{-1}ha) \in aH$.

Therefore $aH = Ha$, as desired.

($\Leftarrow$) Assume that $aH = Ha$ for every $a \in G$. (Must show that $H \lhd G$, that is, $a^{-1}ha \in H$ for every $h \in H$, $a \in G$.) Let $h \in H$, $a \in G$. We have $ha \in Ha = aH$, so $ha = ak$ for some $k \in H$. So $a^{-1}ha = k \in H$. This shows that $H \lhd G$.

(This was Exercise 8–2.) □

9.3 Index two subgroup is normal

Let G be a group and let H be a subgroup of G.

9.3.1 Theorem. *If* $|G : H| = 2$, *then* $H \lhd G$.

Proof. See Exercise 9–4. □

9.4 Normality is not transitive

The following example shows that normality is not transitive. In other words, it is possible to have subgroups H and K of a group G such that $H \lhd K$ and $K \lhd G$, but $H \not\lhd G$.

9.4.1 Example In the dihedral group $G = D_4$, put $H = \langle \tau \rangle = \{\varepsilon, \tau\}$ and $K = \{\varepsilon, \rho^2, \tau, \rho^2\tau\}$. Prove that $H \lhd K$ and $K \lhd G$, but $H \not\lhd G$.

Solution First, H is a subgroup of G (as is every cyclic subgroup generated by an element) and K is seen to be a subgroup of G by using the Subgroup Theorem and the table in Section 7.6. Moreover, $H \leq K$.

By Lagrange's theorem, $|K : H| = |K|/|H| = 4/2 = 2$, so $H \lhd K$ by Theorem 9.3.1. Similarly, $|G : K| = |G|/|K| = 8/4 = 2$, so $K \lhd G$.

Finally, $H \not\lhd G$ by Example 9.1.3. □

9 – Exercises

9–1 Let G be a group and let $Z(G) = \{z \in G \mid zx = xz \text{ for all } x \in G\}$ (center of G). Prove that if N is a subgroup of G contained in $Z(G)$, then $N \lhd G$.

9–2 Prove that $\mathrm{SL}_n(\mathbf{R}) \lhd \mathrm{GL}_n(\mathbf{R})$. ($\mathrm{SL}_n(\mathbf{R})$ is the subgroup of $\mathrm{GL}_n(\mathbf{R})$ consisting of $n \times n$ matrices over $\mathbf{R}$ having determinant 1.)

9–3 Let G be a group and let N and M be normal subgroups of G. Prove that $N \cap M \lhd G$. (By Exercise 5–7 we already know that $N \cap M$ is a subgroup of G, so just the normality condition needs to be checked.)

9–4 Let G be a group and let H be a subgroup of G. Prove that if $|G : H| = 2$, then $H \lhd G$.

HINT: Use Theorem 9.2.1.

9–5 Let G be a group, let H be a subgroup of G, and let $g \in G$. Prove that $g^{-1}Hg$ is a subgroup of G, where

$$g^{-1}Hg := \{g^{-1}hg \mid h \in H\}.$$

9–6 Let G be a group and let H and K be subgroups of G.

(a) Prove that if K is normal, then HK is a subgroup of G, where

$$HK := \{hk \mid h \in H, k \in K\}.$$

(b) Give an example to show that if K is not normal, then HK need not be a subgroup.

10 Quotient group

10.1 Definition

Let G be a group and let N be a normal subgroup of G. Let G/N denote the set of (left) cosets of N in G:

$$G/N = \{aN \mid a \in G\}.$$

Define a binary operation on G/N by the rule

$$aNbN = abN.$$

10.1.1 Theorem.

(i) *The above rule is a well-defined binary operation on G/N.*

(ii) *With this binary operation G/N is a group with identity element eN $(= N)$ and with inverse of aN given by $a^{-1}N$ for $a \in G$.*

Proof. (i) Suppose $aN = a_1N$ and $bN = b_1N$ with $a, a_1, b, b_1 \in G$. (Must show that $abN = a_1b_1N$). By Theorem 8.3.1, we have $n := a^{-1}a_1 \in N$ and $m := b^{-1}b_1 \in N$. Therefore,

$$\begin{aligned}(ab)^{-1}a_1b_1 &= b^{-1}a^{-1}a_1b_1 \\ &= b^{-1}b_1b_1^{-1}a^{-1}a_1b_1 \\ &= m(b_1^{-1}nb_1) \in N,\end{aligned}$$

where we have used that $b_1^{-1}nb_1 \in N$ since $n \in N$ and N is normal. By Theorem 8.3.1 we have $abN = a_1b_1N$ as desired.

(ii) First, for $aN, bN, cN \in G/N$ we have

$$(aNbN)cN = abNcN = (ab)cN = a(bc)N = aNbcN = aN(bNcN),$$

so the binary operation is associative.

Next, for any $aN \in G/N$ we have

$$eNaN = eaN = aN \qquad \text{and} \qquad aNeN = aeN = aN,$$

so eN is an identity element of G/N.

Finally, given $aN \in G/N$ we have

$$a^{-1}NaN = a^{-1}aN = eN \qquad \text{and} \qquad aNa^{-1}N = aa^{-1}N = eN,$$

so $a^{-1}N$ is an inverse of aN.

Therefore, G/N is a group. □

The group G/N is the **quotient group** (or **factor group**) of G by N.

The notation G/N is read "G modulo N" (or just "G mod N").

If the binary operation of G is $+$, then the binary operation on G/N is written this way:

$$(a + N) + (b + N) = (a + b) + N.$$

10.2 Examples

10.2.1 Example Let $G = \mathbf{Z}$ and $N = 3\mathbf{Z}$. The cosets of N are

$$\begin{aligned} 0 + N &= \{\dots, -6, -3, 0, 3, 6, \dots\} \\ 1 + N &= \{\dots, -5, -2, 1, 4, 7, \dots\} \\ 2 + N &= \{\dots, -4, -1, 2, 5, 8, \dots\}, \end{aligned}$$

so

$$G/N = \{0 + N, 1 + N, 2 + N\}.$$

Here are a couple of computations in the group G/N:

$$(1 + N) + (2 + N) = (1 + 2) + N = 3 + N = 0 + N$$

(the last equality since $-3 + 0 = -3 \in N$),

$$(2 + N) + (2 + N) = (2 + 2) + N = 4 + N = 1 + N$$

(the last equality since $-4 + 1 = -3 \in N$).

Similar computations can be used to complete the addition table for G/N:

$+$	$0+N$	$1+N$	$2+N$
$0+N$	$0+N$	$1+N$	$2+N$
$1+N$	$1+N$	$2+N$	$0+N$
$2+N$	$2+N$	$0+N$	$1+N$

The group G/N is isomorphic to the group $\mathbf{Z}_3$, which has addition table

$+$	0	1	2
0	0	1	2
1	1	2	0
2	2	0	1

An isomorphism $\varphi : \mathbf{Z}_3 \to G/N$ is given by $\varphi(a) = a + N$. More generally, $\mathbf{Z}/n\mathbf{Z} \cong \mathbf{Z}_n$ for any $n \in \mathbf{N}$.

10.2.2 Example Let $G = \mathbf{Z}_4 \oplus \mathbf{Z}_3$ and let $N = \langle (0,1) \rangle$. Find the addition table for the quotient group G/N and state a familiar group to which this group is isomorphic.

Solution Recall that $\mathbf{Z}_4 \oplus \mathbf{Z}_3$ is the set of all ordered pairs (x, y) with $x \in \mathbf{Z}_4$ and $y \in \mathbf{Z}_3$, viewed as a group using componentwise addition.

We have

$$N = \{(0,0), (0,1), (0,2)\}$$

so the cosets of N are

$$\begin{aligned} N_0 &:= (0,0) + N = \{(0,0), (0,1), (0,2)\}, \\ N_1 &:= (1,0) + N = \{(1,0), (1,1), (1,2)\}, \\ N_2 &:= (2,0) + N = \{(2,0), (2,1), (2,2)\}, \\ N_3 &:= (3,0) + N = \{(3,0), (3,1), (3,2)\}. \end{aligned}$$

Therefore,

$$G/N = \{N_0, N_1, N_2, N_3\}.$$

As an example of coset addition, we have

$$N_2 + N_3 = [(2,0) + N] + [(3,0) + N] = [(2,0) + (3,0) + N] = (1,0) + N = N_1.$$

The complete addition table for G/N is

$+$	N_0	N_1	N_2	N_3
N_0	N_0	N_1	N_2	N_3
N_1	N_1	N_2	N_3	N_0
N_2	N_2	N_3	N_0	N_1
N_3	N_3	N_0	N_1	N_2

It follows that G/N is isomorphic to $\mathbf{Z}_4$, which has addition table

$+$	0	1	2	3
0	0	1	2	3
1	1	2	3	0
2	2	3	0	1
3	3	0	1	2

An isomorphism $\varphi : \mathbf{Z}_4 \to G/N$ is given by $\varphi(m) = N_m$. □

10.3 Extreme cases

In this section, we study the quotient group G/N in the two extreme cases $N = G$ and $N = \{e\}$, that is, when N is as large as it can be and when N is as small as it can be. Both of these are normal subgroups of G so that the quotient group is defined.

10.3.1 Theorem.

(i) $G/G \cong \{e\}$ (= *trivial group*),

(ii) $G/\{e\} \cong G$.

Proof. (i) Since $eG = G$, this is the only (left) coset of G. So $G/G = \{eG\}$ and this group is isomorphic to the trivial group $\{e\}$ (as is any group having only one element).

(ii) Put $N = \{e\}$. For $a \in G$, we have $aN = \{ae\} = \{a\}$. Therefore $G/N = \{\{a\} \mid a \in G\}$, that is, the elements of G/N are simply the elements of G with braces written around them. The function $\varphi : G \to G/N$ given by $\varphi(a) = \{a\}$ is a bijection. Moreover, for $a, b \in G$,

$$\varphi(ab) = \{ab\} = abN = aNbN = \{a\}\{b\} = \varphi(a)\varphi(b),$$

so φ is an isomorphism. Thus, $G \cong G/N = G/\{e\}$ and the claim follows. □

10.4 Quotient and powers

This section and the next illustrate how sometimes one can pass to a quotient group to create a group possessing a certain property that the original group does not necessarily have.

10.4.1 Theorem. *Let G be a group, let N be a normal subgroup of G. Fix an integer m and assume that $a^m \in N$ for every $a \in G$. Then the order of every element of G/N divides m.*

Proof. Let $aN \in G/N$. Since $a^m \in N$ by assumption, we have

$$(aN)^m = a^m N = N = eN \ (= \text{identity of } G/N)$$

using Corollary 8.3.2. Therefore, by Theorem 5.4.3, it follows that the order of aN divides m. □

In the theorem, since every power a^m is in N, by passing to the quotient it is as though we are making these powers equal to the identity (strictly speaking, making their corresponding cosets equal to the identity). The result is that, in the quotient, raising every element to the mth power produces the identity, which implies that every element has order dividing m.

10.5 Quotient and commutator

Let G be a group and let $a, b \in G$. The **commutator** of a and b is the element $[a, b] := a^{-1}b^{-1}ab$ of G.

Saying that the elements a and b of G commute is the same as saying that their commutator equals the identity:

$$ab = ba \qquad \Leftrightarrow \qquad a^{-1}b^{-1}ab = e \qquad \Leftrightarrow \qquad [a, b] = e.$$

In particular, the group G is abelian if and only if $[a, b] = e$ for all $a, b \in G$. The following theorem generalizes this statement.

10.5.1 Theorem. *Let $N \lhd G$. The quotient group G/N is abelian if and only if $[a, b] \in N$ for all $a, b \in G$.*

Proof. We can prove both directions at the same time:

$$\begin{array}{lllll} G/N \text{ is abelian} & \Leftrightarrow & aNbN = bNaN & \forall a, b \in G & \\ & \Leftrightarrow & abN = baN & \forall a, b \in G & \\ & \Leftrightarrow & (ba)^{-1}ab \in N & \forall a, b \in G & \text{(Theorem 8.3.1)} \\ & \Leftrightarrow & a^{-1}b^{-1}ab \in N & \forall a, b \in G & \\ & \Leftrightarrow & [a, b] \in N & \forall a, b \in G. & \end{array}$$

□

Letting $N = \{e\}$ in the theorem we recover the statement that G is abelian if and only if $[a, b] = e$ for all $a, b \in G$ (using the fact that $G/\{e\} \cong G$).

Consider the direction "$\Leftarrow$" of the theorem. Since every commutator $[a, b]$ is in N, by passing to the quotient it is as though we are making these commutators equal to the identity (strictly speaking, making their corresponding cosets equal to the identity). The result is that, in the quotient, all commutators equal the identity, which is the same as saying the quotient is abelian.

10 – Exercises

10–1

(a) Write the addition table for the quotient group $\mathbf{Z}_{12}/\langle 4 \rangle$.

(b) To which familiar group is $\mathbf{Z}_{12}/\langle 4 \rangle$ isomorphic? Explain.

10–2 Let $G = D_4$ (= dihedral group) and let $N = \langle \rho^2 \rangle$.

(a) Prove that $N \lhd G$.

(b) Write the multiplication (i.e., composition) table for the quotient group G/N.

(c) To which familiar group is the quotient group G/N isomorphic? Explain.

10–3 Let G be a group and let $Z(G) = \{z \in G \mid zx = xz \text{ for all } x \in G\}$ (center of G). Then $Z(G) \lhd G$ by Exercise 9–1. Assume that the quotient group $G/Z(G)$ is cyclic. Prove that G is abelian.

10–4 Let G be a finite group and let $N \lhd G$. Prove that for every $a \in G$, we have $a^{|G:N|} \in N$.

HINT: Let $a \in G$. Consider the element aN of the quotient group G/N and use a corollary of Lagrange's theorem.

10–5 Put $G = \mathbf{F_R}$, where $\mathbf{F_R}$ is the additive group of all functions from $\mathbf{R}$ to $\mathbf{R}$. An element f of $F_\mathbf{R}$ is a **constant function** if there exists $c \in \mathbf{R}$ such that $f(x) = c$ for every $x \in \mathbf{R}$. Let N be the set of all constant functions in $\mathbf{F_R}$, and let

$$H = \{f \in \mathbf{F_R} \mid f(0) = 0\}$$

(the set of all functions having graphs that pass through the origin).

(a) Prove that $N \lhd G$.

(b) Prove that $H \leq G$.

(c) Prove that $H \cong G/N$.

11 Homomorphism

In the definition of an isomorphism, if we leave out the assumption of bijectivity we are left with a "homomorphism."

The existence of a homomorphism from one group to another does not imply that the groups are identical like the existence of an isomorphism does, but it does imply that a certain quotient of the first group is identical to the image of the homomorphism (see "First Isomorphism Theorem").

11.1 Definition

Let G and G' be groups. A **homomorphism** from G to G' is a function $\varphi : G \to G'$ satisfying

$$\varphi(xy) = \varphi(x)\varphi(y) \text{ for all } x, y \in G.$$

Caution: On the left of the equation the product xy is computed using the binary operation of G, while on the right the product $\varphi(x)\varphi(y)$ is computed using the binary operation of G'.

Here are four special types of homomorphisms:

- A **monomorphism** is an injective homomorphism.
- An **epimorphism** is a surjective homomorphism.
- An **isomorphism** is a bijective homomorphism.
- An **automorphism** is an isomorphism from a group to itself.

11.2 Examples

11.2.1 Example Prove that the determinant function $\varphi : \mathrm{GL}_n(\mathbf{R}) \to \mathbf{R}^\times$ given by $\varphi(A) = \det A$ is a homomorphism.

Solution For $A, B \in \mathrm{GL}_n(\mathbf{R})$, we have

$$\varphi(AB) = \det(AB) = (\det A)(\det B) = \varphi(A)\varphi(B),$$

where the second equality uses a well-known property of the determinant. Therefore, φ is a homomorphism as claimed. □

11.2.2 Example Fix $n \in \mathbf{N}$ and let $\varphi : \mathbf{Z} \to \mathbf{Z}_n$ be given by $\varphi(x) = r$ where r is the remainder of x upon division by n. For instance, if $n = 5$, then $\varphi(12) = 2$ since $12 = (2)(5) + 2$. Prove that φ is a homomorphism. (This homomorphism is called **reduction modulo** n.)

Solution Let $x, y \in \mathbf{Z}$. (Must show that $\varphi(x + y) = \varphi(x) + \varphi(y)$.) By the division algorithm, we have

$$\begin{aligned} x &= q_1 n + r_1 \\ y &= q_2 n + r_2 \\ r_1 + r_2 &= q_3 n + r_3 \end{aligned}$$

for integers $q_1, q_2, q_3, r_1, r_2, r_3$ with $0 \leq r_1, r_2, r_3 < n$. Then

$$x + y = (q_1 n + r_1) + (q_2 n + r_2) = (q_1 + q_2)n + (r_1 + r_2) = (q_1 + q_2 + q_3)n + r_3,$$

so

$$\varphi(x + y) = r_3 = r_1 + r_2 = \varphi(x) + \varphi(y),$$

where we have used that $r_1 + r_2 = r_3$ in the group $\mathbf{Z}_n$. Therefore, φ is a homomorphism. □

11.2.3 Example Let G be a group, let a be a fixed element of G, and define $\varphi : \mathbf{Z} \to G$ by $\varphi(n) = a^n$.

(a) Prove that φ is a homomorphism.

(b) What is the image of φ?

Solution

(a) For $m, n \in \mathbf{Z}$, we have

$$\varphi(m + n) = a^{m+n} = a^m a^n = \varphi(m)\varphi(n),$$

where we have used a law of exponents (see Section 4.8). Therefore, φ is a homomorphism.

(b) The image of φ is $\{a^n \mid n \in \mathbf{Z}\}$, which equals $\langle a \rangle$, the cyclic subgroup of G generated by a.

□

11.2.4 Example Prove that the function $\varphi : \mathbf{R} \to \mathrm{GL}_2(\mathbf{R})$ given by $\varphi(x) = \begin{bmatrix} 1 & x \\ 0 & 1 \end{bmatrix}$ is a monomorphism.

Solution The claim is that φ is a homomorphism that is injective.

(Homomorphism?) For $x, y \in \mathbf{R}$, we have

$$\begin{aligned} \varphi(x+y) &= \begin{bmatrix} 1 & x+y \\ 0 & 1 \end{bmatrix} \\ &= \begin{bmatrix} 1 & x \\ 0 & 1 \end{bmatrix} \begin{bmatrix} 1 & y \\ 0 & 1 \end{bmatrix} \\ &= \varphi(x)\varphi(y), \end{aligned}$$

so φ is a homomorphism.

(Injective?) Let $x, y \in \mathbf{R}$ and assume that $\varphi(x) = \varphi(y)$. Then

$$\begin{bmatrix} 1 & x \\ 0 & 1 \end{bmatrix} = \begin{bmatrix} 1 & y \\ 0 & 1 \end{bmatrix}.$$

Since two matrices are equal only if their corresponding entries are equal, we conclude that $x = y$. Therefore, φ is injective.

This shows that φ is a monomorphism. □

11.2.5 Example The set $\mathbf{D_R}$ of differentiable functions from $\mathbf{R}$ to $\mathbf{R}$ is a group under addition of functions. Prove that the derivative function $\varphi : \mathbf{D_R} \to \mathbf{F_R}$ given by

$$[\varphi(f)](x) = \frac{d}{dx}[f(x)]$$

is a homomorphism. ($\mathbf{F_R}$ is the group of all functions from $\mathbf{R}$ to $\mathbf{R}$.)

Solution Let $f, g \in \mathbf{D_R}$. For every $x \in \mathbf{R}$, we have

$$\begin{aligned} [\varphi(f+g)](x) &= \frac{d}{dx}[(f+g)(x)] \\ &= \frac{d}{dx}[f(x)+g(x)] && \text{(definition of function addition)} \\ &= \frac{d}{dx}[f(x)] + \frac{d}{dx}[g(x)] && \text{(derivative sum law)} \\ &= [\varphi(f)](x) + [\varphi(g)](x) \\ &= [\varphi(f)+\varphi(g)](x) && \text{(definition of function addition)} \end{aligned}$$

implying, $\varphi(f+g) = \varphi(f) + \varphi(g)$. Therefore, φ is a homomorphism. □

11.2.6 Example Fix $n \in \mathbf{N}$ and define $\varphi : S_n \to \mathbf{Z}_2$ by

$$\varphi(\sigma) = \begin{cases} 0 & \text{if } \sigma \text{ is even,} \\ 1 & \text{if } \sigma \text{ is odd.} \end{cases}$$

(a) Prove that φ is a homomorphism.

(b) Under what conditions is φ an *epi*morphism?

Solution

(a) Let $\sigma, \tau \in S_n$. (Must show that $\varphi(\sigma\tau) = \varphi(\sigma) + \varphi(\tau)$.) The proof requires a consideration of cases, and this is facilitated by the use of a table:

σ	τ	$\sigma\tau$	$\varphi(\sigma)$	$\varphi(\tau)$	$\varphi(\sigma\tau)$	$\varphi(\sigma) + \varphi(\tau)$
even	even	even	0	0	0	0
even	odd	odd	0	1	1	1
odd	even	odd	1	0	1	1
odd	odd	even	1	1	0	0

(the final entry is due to the fact that $1 + 1 = 0$ in $\mathbf{Z}_2$). Since the last two columns are equal the equation $\varphi(\sigma\tau) = \varphi(\sigma) + \varphi(\tau)$ is verified in all four cases, so φ is a homomorphism.

(b) Since φ is a homomorphism by part (a), it remains to find conditions under which φ is surjective. If $n = 1$, then $S_n = \{\varepsilon\}$, so the image of φ is $\{0\} \neq \mathbf{Z}_2$, whence φ is *not* surjective. On the other hand, if $n > 1$, then the transposition $(1, 2)$ is an element of S_n and we have $\varphi((1, 2)) = 1$ and $\varphi(\varepsilon) = 0$, so the image of φ is $\{0, 1\} = \mathbf{Z}_2$, whence φ is surjective.

In view of this and part (a), we conclude that φ is an epimorphism if and only if $n > 1$.

□

11.3 Elementary properties

Let G and G' be groups and let $\varphi : G \to G'$ be a homomorphism. We denote by e and e' the identity elements of G and G', respectively.

11.3.1 Theorem.

(i) $\varphi(e) = e'$,

(ii) $\varphi(x^{-1}) = \varphi(x)^{-1}$ *for each* $x \in G$.

Proof. (i) We have

$$\varphi(e)\varphi(e) = \varphi(ee) = \varphi(e) = \varphi(e)e',$$

so by left cancellation, $\varphi(e) = e'$.

(ii) Let $x \in G$. Using part (i), we have

$$\varphi(x)\varphi(x^{-1}) = \varphi(xx^{-1}) = \varphi(e) = e',$$

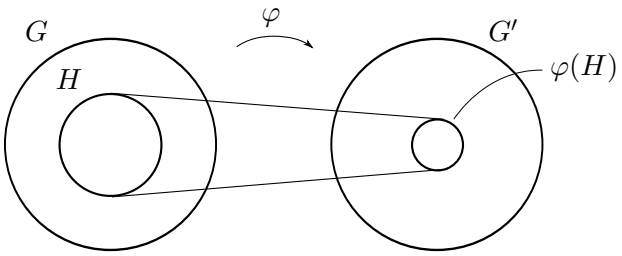
so $\varphi(x^{-1}) = \varphi(x)^{-1}$ by Theorem 4.7.1. □

11.4 Image, preimage, kernel

Let $\varphi : G \to G'$ be a group homomorphism.

Let H be a subset of G. The **image** of H under φ is the set

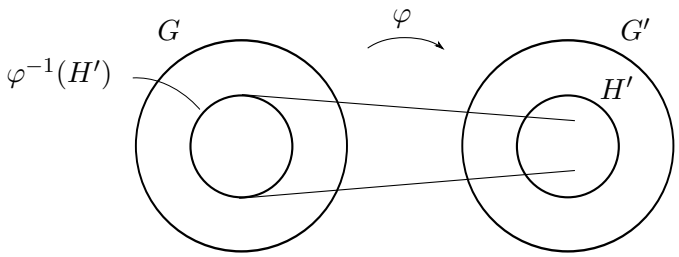
$$\varphi(H) := \{\varphi(h) \mid h \in H\}.$$



In view of the definition given in Section 1.5 of the image of a function, we have $\operatorname{im}\varphi = \varphi(G)$, that is, the image of φ is the image of G under φ.

Let H' be a subset of G'. The **preimage** of H' under φ is the set

$$\varphi^{-1}(H') = \{x \in G \mid \varphi(x) \in H'\}.$$



The preimage $\varphi^{-1}(H')$ is defined even if the inverse function φ^{-1} does not exist, that is, even if φ is not bijective. In the case φ^{-1} *does* exist, the image of H' under φ^{-1}, which we are denoting $\varphi^{-1}(H')$, coincides with the preimage of H' under φ, which we are also denoting $\varphi^{-1}(H')$, so no confusion can arise.

11.4.1 Theorem.

(i) *If $H \leq G$, then $\varphi(H) \leq G'$.*

(ii) *If $H' \leq G'$, then $\varphi^{-1}(H') \leq G$.*

Proof. (i) Let $H \leq G$. (Must show that $\varphi(H) \leq G'$.) We use the Subgroup Theorem (5.1.2).

($e' \in \varphi(H)$?) Since $e \in H$, we have $e' = \varphi(e) \in \varphi(H)$ by Theorem 11.3.1.

($x', y' \in \varphi(H) \Rightarrow x'y' \in \varphi(H)$?) Let $x', y' \in \varphi(H)$. We have $x' = \varphi(x)$ and $y' = \varphi(y)$ for some $x, y \in H$. Then $xy \in H$, so that

$$x'y' = \varphi(x)\varphi(y) = \varphi(xy) \in \varphi(H).$$

($x' \in \varphi(H) \Rightarrow (x')^{-1} \in \varphi(H)$?) Let $x' \in \varphi(H)$. We have $x' = \varphi(x)$ for some $x \in H$. Then $x^{-1} \in H$, so that

$$(x')^{-1} = \varphi(x)^{-1} = \varphi(x^{-1}) \in H,$$

where we have used Theorem 11.3.1.

By the Subgroup Theorem, $\varphi(H) \leq G'$.

(ii) Exercise 11–5. □

The next theorem says that normality of a subgroup is preserved under a homomorphic image *provided* the homomorphism is surjective, and that it is preserved under a homomorphic preimage in general.

11.4.2 Theorem.

(i) *If $N \lhd G$ and φ is surjective, then $\varphi(N) \lhd G'$.*

(ii) *If $N' \lhd G'$, then $\varphi^{-1}(N') \lhd G$.*

Proof. (i) Exercise 11–6.

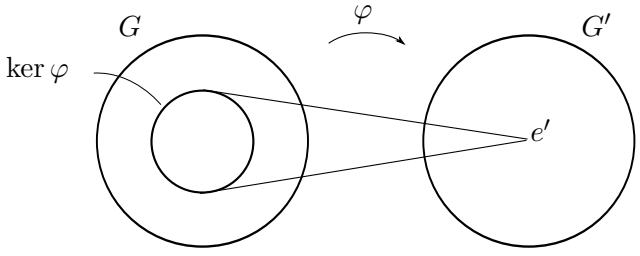
(ii) Let $N' \lhd G'$. (Must show that $\varphi^{-1}(N') \lhd G$.) By the preceding theorem $\varphi^{-1}(N') \leq G$ so we need only check the normality condition. Let $n \in \varphi^{-1}(N')$ and let $g \in G$. We need to show that $g^{-1}ng \in \varphi^{-1}(N')$, which is to say $\varphi(g^{-1}ng) \in N'$. We have

$$\varphi(g^{-1}ng) = \varphi(g)^{-1}\varphi(n)\varphi(g) \in N'.$$

(The equality uses Theorem 11.3.1. Since $n \in \varphi^{-1}(N')$, we have $\varphi(n) \in N'$, so by normality of N', $\varphi(g)^{-1}\varphi(n)\varphi(g) \in N'$ as well.) So $g^{-1}ng \in \varphi^{-1}(N')$. We conclude that $\varphi(N') \lhd G$. □

The **kernel** of the homomorphism $\varphi : G \to G'$ is defined by

$$\ker \varphi := \{x \in G \mid \varphi(x) = e'\}.$$



We have $\ker\varphi = \varphi^{-1}(\{e'\})$ and, since $\{e'\}$ is a normal subgroup of G', it follows from the previous theorem that

$$\ker\varphi \lhd G.$$

11.4.3 Example Fix $n \in \mathbf{N}$. Find the kernel of the reduction modulo n homomorphism $\varphi : \mathbf{Z} \to \mathbf{Z}_n$ (see Example 11.2.2).

Solution The reduction modulo n homomorphism sends an integer to its remainder upon division by n. Since 0 plays the role of the identity element of $\mathbf{Z}_n$, we seek the set of all integers for which $\varphi(x) = 0$, that is, the set of all integers x having remainder 0 upon division by n. This is precisely the set of multiples of n. Therefore, $\ker\varphi = n\mathbf{Z}$. □

11.5 Kernel and injectivity

If a function is a homomorphism and the question of whether it is injective arises, one could use the definition of injectivity to check, but the following theorem gives a condition that is generally easier to apply.

11.5.1 Theorem. *A group homomorphism $\varphi : G \to G'$ is injective if and only if* $\ker\varphi = \{e\}$.

Proof. Let $\varphi : G \to G'$ be a group homomorphism.

($\Rightarrow$) Assume that φ is injective. (Must show that $\ker\varphi = \{e\}$.)

($\subseteq$) Let $x \in \ker\varphi$. Then $\varphi(x) = e'$. But also, $\varphi(e) = e'$ by Theorem 11.3.1. So $\varphi(x) = e' = \varphi(e)$. Since φ is injective, we conclude that $x = e \in \{e\}$.

($\supseteq$) Since $\ker\varphi$ is a subgroup of G (see Section 11.4), it contains the identity element e. Hence, $\{e\} \subseteq \ker\varphi$.

We conclude that $\ker\varphi = \{e\}$.

($\Leftarrow$) Assume that $\ker\varphi = \{e\}$. (Must show that φ is injective.) Let $x, y \in G$ and assume that $\varphi(x) = \varphi(y)$. Then

$$\varphi(xy^{-1}) = \varphi(x)\varphi(y)^{-1} = \varphi(x)\varphi(x)^{-1} = e'$$

so $xy^{-1} \in \ker\varphi = \{e\}$. Hence, $xy^{-1} = e$, implying $x = y$. We conclude that φ is injective. □

In order to apply the theorem to show that a homomorphism is injective, it is enough to take an arbitrary element of the kernel and show that it must be the identity (for this shows that $\ker\varphi \subseteq \{e\}$ and the other inclusion is automatic since $\ker\varphi$ is a subgroup).

11.5.2 Example Let G be a group, let $a \in G$ with $\text{ord}(a) = \infty$, and let $\varphi : \mathbf{Z} \to G$ be given by $\varphi(n) = a^n$. Prove that φ is injective.

Solution Recall that saying $\text{ord}(a) = \infty$ is saying that there is no *positive* integer n such that $a^n = e$. If n is a negative integer and $a^n = e$, then $a^{-n} = (a^n)^{-1} = e^{-1} = e$. Therefore, saying $\text{ord}(a) = \infty$ is the same as saying that for any integer n, we have $a^n = e$ only if $n = 0$.

By Example 11.2.3, φ is a homomorphism, so we can apply the previous theorem. Let $n \in \ker\varphi$. Then $e = \varphi(n) = a^n$. Since $\text{ord}(a) = \infty$, it follows that $n = 0$. By the previous theorem (and the remark following it), we conclude that φ is injective. □

11.6 Canonical epimorphism

Let G be a group and let N be a normal subgroup of G. Define $\pi : G \to G/N$ by

$$\pi(a) = aN.$$

11.6.1 Theorem. *Let $\pi : G \to G/N$ be defined as above.*

(i) *π is an epimorphism,*

(ii) $\ker\pi = N$.

Proof. (i) We need to show that π is a homomorphism and that it is surjective.

(π homomorphism?) For $a, b \in G$, we have

$$\pi(ab) = abN = aNbN = \pi(a)\pi(b),$$

so π is a homomorphism.

(π surjective?) Let $y \in G/N$. Then $y = aN$ for some $a \in G$. We have

$$\pi(a) = aN = y,$$

so we conclude that π is surjective. This finishes the proof that π is an epimorphism.

(ii) We prove that each set is contained in the other.

($\subseteq$) Let $a \in \ker \pi$. (Must show that $a \in N$.) Since $eN = N$ plays the role of the identity element of G/N, we have

$$N = \pi(a) = aN.$$

By Corollary 8.3.2, we get $a \in N$.

($\supseteq$) Let $n \in N$. (Must show that $n \in \ker \pi$.) We have

$$\pi(n) = nN = N,$$

using Corollary 8.3.2. Therefore, $n \in \ker \pi$.

We conclude that $\ker \pi = N$. □

The function $\pi : G \to G/N$ defined above is the **canonical epimorphism**.

In a sense, kernels and normal subgroups are one in the same. More specifically, the kernel of a homomorphism is a normal subgroup (see Section 11.4), and conversely, a normal subgroup is a kernel, namely the kernel of the corresponding canonical epimorphism (by the previous theorem).

11 – Exercises

11–1 Let $\varphi : G \to G'$ and $\psi : G' \to G''$ be two group homomorphisms. Prove that the composition $\psi \circ \varphi : G \to G''$ is a homomorphism.

11–2 Let G be a group and let $\varphi : G \to G$ be the function given by $\varphi(x) = x^{-1}$. Prove that φ is a homomorphism if and only if G is abelian.

11–3 Let $a, b \in \mathbf{R}$ with $a \leq b$. Denote by $\mathbf{C}_{[a,b]}$ the set of continuous real-valued functions on the interval $[a, b]$. Then $\mathbf{C}_{[a,b]}$ is a group under function addition. Define $\varphi : \mathbf{C}_{[a,b]} \to \mathbf{C}_{[a,b]}$ by

$$(\varphi(f))(x) = \int_a^x f(t)\, dt.$$

Prove that φ is a homomorphism.

11–4 Let G_1 and G_2 be groups. The direct product of G_1 and G_2 is the group

$$G_1 \times G_2 := \{(x_1, x_2) \mid x_1 \in G_1 \text{ and } x_2 \in G_2\}$$

with componentwise multiplication. Define $\varphi : G_1 \times G_2 \to G_1$ by $\varphi((x_1, x_2)) = x_1$.

(a) Prove that φ is an epimorphism.

(b) Find the kernel of φ (and prove your claim).

11–5 Let $\varphi : G \to G'$ be a group homomorphism and let $H' \leq G'$. Prove that $\varphi^{-1}(H') \leq G$.

11–6 Let $\varphi : G \to G'$ be a group homomorphism and let $N \lhd G$.

(a) Prove that if φ is surjective, then $\varphi(N) \lhd G'$.

(b) Give an example to show that if φ is not surjective, then it is possible to have $\varphi(N) \not\lhd G'$.

11–7

(a) Let $\varphi : G \to G'$ be a group homomorphism and let a' be a fixed element of G'. Prove that if a is an element of G satisfying $\varphi(a) = a'$, then the set of all elements x of G satisfying $\varphi(x) = a'$ is the coset aN, where $N = \ker \varphi$.

(b) Let $r, s \in \mathbf{R}$. Prove that every solution y to the linear differential equation $y' + ry = s$ is of the form $y = y_p + y_0$, where y_p is a particular solution and y_0 is a solution to the corresponding homogeneous equation $y' + ry = 0$. (This is an important theorem in the theory of differential equations.)

(Hint: Consider the function $\varphi : \mathbf{D_R} \to \mathbf{F_R}$ given by $\varphi(y) = y' + ry$, where $\mathbf{D_R}$ is the additive group of differentiable functions on $\mathbf{R}$. Use part (a).)

12 Isomorphism theorems

12.1 First Isomorphism Theorem

The following theorem is the most fundamental theorem of group theory. Before stating it, we remind the reader of the relevant definitions: If $\varphi : G \to G'$ is a group homomorphism, then

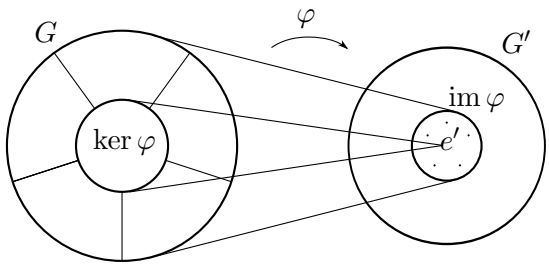
$$\ker \varphi := \{x \in G \mid \varphi(x) = e'\},$$

$$\operatorname{im} \varphi := \{\varphi(x) \mid x \in G\}.$$

12.1.1 Theorem (First Isomorphism Theorem). *Let $\varphi : G \to G'$ be a group homomorphism. We have*

$$G/\ker \varphi \cong \operatorname{im} \varphi.$$

The proof is given below, but first here is a diagram that can be used to visualize what the theorem says:



In this picture, there are 6 cosets of the kernel, so $G/\ker \varphi$ has 6 elements. Also, the image of φ has 6 elements. So both sides in the statement of the theorem have 6 elements. The theorem says that these groups are isomorphic.

Proof. First, it has been observed that $\ker \varphi$ is a normal subgroup of G (see Section 11.4), so the quotient group $G/\ker \varphi$ is defined.

To simplify notation, put $N = \ker \varphi$, so the claim becomes $G/N \cong \operatorname{im} \varphi$. We will prove this claim by exhibiting an isomorphism from G/N to $\operatorname{im} \varphi$.

Define $\bar{\varphi} : G/N \to \operatorname{im}\varphi$ by

$$\bar{\varphi}(aN) = \varphi(a).$$

For an input aN, the corresponding output is $\varphi(a)$, which is an element of $\operatorname{im}\varphi$, so $\bar{\varphi}$ is well defined in the sense that it maps into the indicated codomain. We are concerned about another issue of well-definedness, though. If aN is an input, this same coset might also be written bN. In this case, we need to show that the corresponding outputs, namely $\varphi(a)$ and $\varphi(b)$, are the same.

($\bar{\varphi}$ well defined?) Let $a, b \in G$ and assume that $aN = bN$. (Must show that $\varphi(a) = \varphi(b)$.) By Theorem 8.3.1, we have $a^{-1}b \in N = \ker\varphi$. Therefore,

$$e' = \varphi(a^{-1}b) = \varphi(a)^{-1}\varphi(b).$$

Multiplying both sides by $\varphi(a)$ yields $\varphi(a) = \varphi(b)$, as desired.

($\bar{\varphi}$ homomorphism?) For $aN, bN \in G/N$, we have

$$\bar{\varphi}(aNbN) = \bar{\varphi}(abN) = \varphi(ab) = \varphi(a)\varphi(b) = \bar{\varphi}(aN)\bar{\varphi}(bN),$$

so $\bar{\varphi}$ is a homomorphism.

($\bar{\varphi}$ injective?) By Theorem 11.5.1 (and the remark following it), it is enough to show that the kernel of $\bar{\varphi}$ contains only the identity element of G/N, namely N. Let $aN \in \ker\bar{\varphi}$. Then

$$\varphi(a) = \bar{\varphi}(aN) = e',$$

so $a \in \ker\varphi = N$. Therefore, $aN = N$ and it follows that $\bar{\varphi}$ is injective.

($\bar{\varphi}$ surjective?) Let $y \in \operatorname{im}\varphi$. Then $y = \varphi(a)$ for some $a \in G$. We have $aN \in G/N$ and

$$\bar{\varphi}(aN) = \varphi(a) = y,$$

so it follows that $\bar{\varphi}$ is surjective.

We have shown that $\bar{\varphi} : G/N \to \operatorname{im}\varphi$ is a homomorphism and that it is bijective. Therefore it is an isomorphism. We conclude that $G/\ker\varphi = G/N \cong \operatorname{im}\varphi$. □

The First Isomorphism Theorem can be used to show that two groups are isomorphic when one of the groups is a quotient group. The next example illustrates the technique.

12.1.2 Example Prove that $\mathbf{Z}/n\mathbf{Z} \cong \mathbf{Z}_n$ $(n \in \mathbf{N})$.

Solution In order to use the First Isomorphism Theorem, we need to find a homomorphism $\varphi : \mathbf{Z} \to \mathbf{Z}_n$ having kernel $n\mathbf{Z}$ and image $\mathbf{Z}_n$. Showing $\operatorname{im}\varphi = \mathbf{Z}_n$ amounts to showing that φ is surjective.

Define $\varphi : \mathbf{Z} \to \mathbf{Z}_n$ to be reduction modulo n, that is, the function defined by letting $\varphi(x)$ be the remainder of x upon division by n.

(φ homomorphism?) This was shown in Example 11.2.2.

($\ker\varphi = n\mathbf{Z}$?) This was shown in Example 11.4.3.

(φ surjective?) Let $x \in \mathbf{Z}_n = \{0, 1, 2, \ldots, n-1\}$. Since $0 \leq x < n$, the remainder of x upon division by n is just x itself. Therefore, $\varphi(x) = x$. This shows that φ is surjective.

By the First Isomorphism Theorem,

$$\mathbf{Z}/n\mathbf{Z} = \mathbf{Z}/\ker\varphi \cong \operatorname{im}\varphi = \mathbf{Z}_n.$$

□

12.1.3 Example Let $n \in \mathbf{N}$. By Exercise 9–2, $\mathrm{SL}_n(\mathbf{R}) \lhd \mathrm{GL}_n(\mathbf{R})$. Prove that $\mathrm{GL}_n(\mathbf{R})/\mathrm{SL}_n(\mathbf{R}) \cong \mathbf{R}^\times$, where $\mathbf{R}^\times$ is the group of nonzero real numbers under multiplication.

Solution Since one of the groups in the desired isomorphism is a quotient, we try to apply the First Isomorphism Theorem. We need an epimorphism $\varphi : \mathrm{GL}_n(\mathbf{R}) \to \mathbf{R}^\times$ with kernel $\mathrm{SL}_n(\mathbf{R})$.

Let $\varphi : \mathrm{GL}_n(\mathbf{R}) \to \mathbf{R}^\times$ be the determinant function given by $\varphi(A) = \det A$. By Example 11.2.1, φ is a homomorphism.

($\ker\varphi = \mathrm{SL}_n(\mathbf{R})$?) We can prove both inclusions at the same time. For $A \in \mathrm{GL}_n(\mathbf{R})$, we have

$$\begin{aligned} A \in \ker\varphi &\Leftrightarrow \varphi(A) = 1 \\ &\Leftrightarrow \det A = 1 \\ &\Leftrightarrow A \in \mathrm{SL}_n(\mathbf{R}). \end{aligned}$$

Therefore, $\ker\varphi = \mathrm{SL}_n(\mathbf{R})$.

(φ surjective?) Let $x \in \mathbf{R}^\times$. Put

$$A = \begin{bmatrix} x & 0 & 0 & \cdots & 0 & 0 \\ 0 & 1 & 0 & \cdots & 0 & 0 \\ 0 & 0 & 1 & \cdots & 0 & 0 \\ \vdots & \vdots & \vdots & \ddots & \vdots & \vdots \\ 0 & 0 & 0 & \cdots & 1 & 0 \\ 0 & 0 & 0 & \cdots & 0 & 1 \end{bmatrix}.$$

Then $\det A = x \neq 0$, so $A \in \mathrm{GL}_n(\mathbf{R})$ and $\varphi(A) = \det A = x$. Therefore, φ is surjective.

By the First Isomorphism Theorem,

$$\mathrm{GL}_n(\mathbf{R})/\operatorname{SL}_n(\mathbf{R}) = \mathrm{GL}_n(\mathbf{R})/\ker\varphi \cong \operatorname{im}\varphi = \mathbf{R}^\times.$$

□

It is instructive to verify the First Isomorphism Theorem in the two extreme cases where the kernel of the homomorphism $\varphi : G \to G'$ is all of G on the one hand, and where it is the trivial subgroup on the other:

- Assume that $\ker\varphi = G$. This implies that φ maps every element of G to the identity element e' of G', so that $\operatorname{im}\varphi = \{e'\}$. Therefore, the First Isomorphism Theorem says that

  $$G/G = G/\ker\varphi \cong \operatorname{im}\varphi = \{e'\}.$$

  Since G/G is the trivial group (see Section 10.3) and $\{e'\}$ is as well, this is just saying that the trivial group is isomorphic to the trivial group, which is in agreement with what we know.

- Assume that $\ker\varphi = \{e\}$. Then the First Isomorphism Theorem says that

  $$G/\{e\} = G/\ker\varphi \cong \operatorname{im}\varphi.$$

  Now $G/\{e\}$ is isomorphic to G in a natural way (see Section 10.3), so we get $G \cong \operatorname{im}\varphi$.

  We can verify this another way: Since $\ker\varphi = \{e\}$, the homomorphism φ is injective (see Section 11.5) and therefore it defines an isomorphism from G to $\operatorname{im}\varphi$, which also implies that $G \cong \operatorname{im}\varphi$.

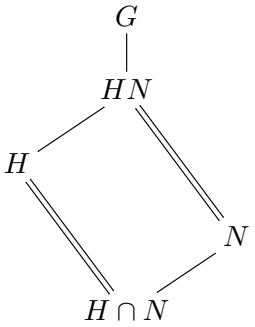
12.2 Second Isomorphism Theorem

Let G be a group and let H and N be subgroups of G with N normal.

By Exercise 9–6, HN is a subgroup of G. It contains N as a normal subgroup so the quotient group HN/N is defined.

Also, $H \cap N$ is a subgroup of H and it is normal, so the quotient group $H/H \cap N$ is defined. (The fact that $H \cap N$ is normal in H can be checked directly, but the proof of the following theorem will show that $H \cap N$ is the kernel of a homomorphism and this will imply that it is normal.)

Here is the relevant subgroup diagram:

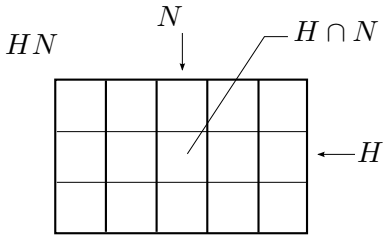


The following theorem says that the two quotient groups corresponding to the two doubled line segments are isomorphic.

12.2.1 Theorem (Second Isomorphism Theorem). *Let G be a group and let H and N be subgroups of G with N normal.*

$$H/H \cap N \cong HN/N.$$

The proof is given below, but first here is a diagram that can be used to visualize what the theorem says:



In this picture, H is the middle horizontal band and N is the middle vertical band. The 5 vertical bands are the cosets of N in HN, so HN/N has 5 elements. On the other hand, the 5 middle squares are the cosets of $H \cap N$ in H, so $H/H \cap N$ has 5 elements. So both sides in the statement of the theorem have 5 elements. The theorem says that these groups are isomorphic. (The encompassing group G is not pictured.)

Proof. Our aim is to use the First Isomorphism Theorem, so we need to find a homomorphism $\varphi : H \to HN/N$ such that $\ker \varphi = H \cap N$ and $\operatorname{im} \varphi = HN/N$ (and this latter means that φ should be surjective).

Define $\varphi : H \to HN/N$ by $\varphi(h) = hN$. Then φ is a homomorphism (it is simply the restriction to H of the canonical epimorphism $\pi : G \to G/N$).

($\ker \varphi = H \cap N$?) We will prove both inclusions at the same time. For $h \in H$ we have

$$\begin{aligned} h \in \ker \varphi \quad &\Leftrightarrow \quad \varphi(h) = N \\ &\Leftrightarrow \quad hN = N \\ &\Leftrightarrow \quad h \in H \cap N, \end{aligned}$$

so $\ker \varphi = H \cap N$.

(φ surjective?) Let $x \in HN/N$. Then $x = hnN = hN$ for some $h \in H$ and $n \in N$, and we have $\varphi(h) = hN = x$, so φ is surjective.

By the First Isomorphism Theorem,

$$H/(H \cap N) = H/\ker \varphi \cong \operatorname{im} \varphi = HN/N,$$

and the proof is complete. □

Because of the diagram above, this theorem is sometimes called the "Diamond Theorem."

12.2.2 Example Let G_1 and G_2 be groups and set $G = G_1 \times G_2$. Define $N = \{(e_1, x_2) \,|\, x_2 \in G_2\}$. Then $N \lhd G$ (since, for instance, N is the kernel of the homomorphism in Exercise 11–4). Use the Second Isomorphism Theorem to prove that $G/N \cong G_1$.

Solution Put $H = \{(x_1, e_2) \,|\, x_1 \in G_1\}$. Then H is a (normal) subgroup of G (for essentially the same reason that N is).

We claim that $G = HN$. The inclusion ($\supseteq$) is immediate, and if $x = (x_1, x_2) \in G$, then

$$x = (x_1, x_2) = (x_1, e_2)(e_1, x_2) \in HN,$$

which gives the inclusion ($\subseteq$).

We also have $H \cap N = \{(e_1, e_2)\}$. So, by the Second Isomorphism Theorem, we get

$$G/N = HN/N \cong H/H \cap N = H/\{(e_1, e_2)\} \cong H.$$

Finally $H \cong G_1$ (the map $\varphi : H \to G_1$ given by $\varphi((x_1, e_2)) = x_1$ is an isomorphism), so we conclude that $G/N \cong G_1$. □

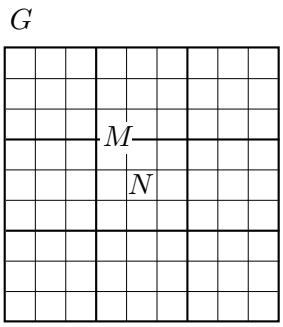
12.3 Third Isomorphism Theorem

Let G be a group and let M and N be normal subgroups of G with $M \supseteq N$. Then M/N is a normal subgroup of G/N (this can be verified directly, but it is also a consequence of the following proof), so the quotient group $(G/N)/(M/N)$ is defined.

12.3.1 Theorem (Third Isomorphism Theorem). *Let G be a group and let M and N be normal subgroups of G with $M \supseteq N$.*

$$(G/N)/(M/N) \cong G/M.$$

The proof is given below, but first here is a diagram that can be used to visualize what the theorem says:



In this picture, G/N consists of the 81 small squares and M/N consists of the 9 inner most small squares, so $(G/N)/(M/N)$ has 9 elements. On

the other hand, G/M consists of the 9 large squares. So both sides in the statement of the theorem have 9 elements. The theorem says that these groups are isomorphic.

Proof. We intend to use the First Isomorphism Theorem, so we need to find a homomorphism $\varphi : G/N \to G/M$ such that $\ker \varphi = M/N$ and $\operatorname{im} \varphi = G/M$ (and this latter means that φ should be surjective).

Define $\varphi : G/N \to G/M$ by $\varphi(aN) = aM$.

(φ well defined?) Let $a, b \in G$ and assume that $aN = bN$. Then $a^{-1}b \in N \subseteq M$ so that $aM = bM$. It follows that φ is well defined.

(φ homomorphism?) For $aN, bN \in G/N$, we have

$$\varphi(aNbN) = \varphi(abN) = abM = aMbM = \varphi(aN)\varphi(bN),$$

so φ is a homomorphism.

($\ker \varphi = M/N$?) We can prove both inclusions at the same time. For $aN \in G/N$, we have

$$\begin{aligned} aN \in \ker \varphi &\Leftrightarrow \varphi(aN) = M \\ &\Leftrightarrow aM = M \\ &\Leftrightarrow a \in M \qquad \text{(Corollary 8.3.2)} \\ &\Leftrightarrow aN \in M/N. \end{aligned}$$

Hence, $\ker \varphi = M/N$. (This shows, in particular, that $M/N \lhd G/N$ as claimed before the statement of the theorem.)

(φ surjective?) Let $aM \in G/M$. Then $aN \in G/N$ and $\varphi(aN) = aM$. Therefore, φ is surjective.

By the First Isomorphism Theorem,

$$(G/N)/(M/N) = (G/N)/\ker \varphi \cong \operatorname{im} \varphi = G/M.$$

□

12 – Exercises

12–1 Let G_1 and G_2 be groups and put $G = G_1 \times G_2$. Use the First Isomorphism Theorem to prove that $G/N \cong G_1$, where $N = \{(e_1, x_2) \mid x_2 \in G_2\}$.

HINT: Exercise 11–4.

12–2 Prove the Second Isomorphism Theorem by using the First Isomorphism Theorem with HN/N playing the role of the quotient $G/\ker\varphi$.

HINT: There is a natural way to define a homomorphism, but it needs to be shown that the homomorphism is well defined.

12–3 To what familiar group is $(\mathbf{Z}/6\mathbf{Z})/(2\mathbf{Z}/6\mathbf{Z})$ isomorphic? Explain.

12–4 Prove the Third Isomorphism Theorem by using the First Isomorphism Theorem with G/M playing the role of the quotient $G/\ker\varphi$.

13 Simple group

13.1 Definition

A group G is **simple** if the following hold:

(i) $|G| > 1$ (that is, G is not the trivial group),

(ii) the only normal subgroups of G are $\{e\}$ and G.

The next theorem provides several examples of simple groups, namely $\mathbf{Z}_p$ for any prime number p.

13.1.1 Theorem. *Let $n \in \mathbf{N}$. The group $\mathbf{Z}_n$ is simple if and only if n is prime.*

Proof. ($\Rightarrow$) We prove the contrapositive. Assume that n is not prime. (Must show that $\mathbf{Z}_n$ is not simple.) If $n = 1$, then $|\mathbf{Z}_n| = 1$ and $\mathbf{Z}_n$ is not simple since it fails property (i). Therefore, we may assume $n > 1$. Since n is not prime, there is a factorization $n = dd'$ with d and d' integers neither of which are 1 or n. By Exercise 6–1, $\mathbf{Z}_n$ has a subgroup H of order d. Since d is neither 1 nor n it follows that H is neither $\{e\}$ nor $\mathbf{Z}_n$. Moreover, H is normal since $\mathbf{Z}_n$ is abelian. Therefore, $\mathbf{Z}_n$ is not simple since it fails property (ii).

($\Leftarrow$) Assume that n is prime. (Must show that $\mathbf{Z}_n$ is simple.) Since n is prime, we have $|\mathbf{Z}_n| = n > 1$, so $\mathbf{Z}_n$ satisfies property (i). Let N be an arbitrary normal subgroup of $\mathbf{Z}_n$. By Corollary 8.9.1, the order of N divides the order of $\mathbf{Z}_n$, which is n. But n is prime, so the order of N must be either 1, in which case $N = \{e\}$, or n, in which case $N = \mathbf{Z}_n$. Therefore, $\mathbf{Z}_n$ satisfies property (ii). We conclude that $\mathbf{Z}_n$ is simple. □

13.1.2 Theorem. *The alternating group A_n is simple for $n \geq 5$.*

Proof. Omitted. (The proof is not difficult, but neither is it elegant since it requires a check of several cases.) □

(The groups A_n with $n < 5$ are not simple.)

This theorem has important consequences for solutions of polynomial equations. The general 2nd degree polynomial equation $ax^2 + bx + c = 0$ has solutions given by the quadratic formula:

$$x = \frac{-b \pm \sqrt{b^2 - 4ac}}{2a}.$$

There is an analogous, but more complicated, formula for the solutions to the general 3rd degree polynomial equation $ax^3 + bx^2 + cx + d = 0$. Likewise for the general 4th degree polynomial equation.

For about 280 years, mathematicians searched for an analog of the quadratic formula for the solutions to the general 5th degree polynomial equation. The search came to a disappointing end when in 1824 the mathematician Abel (at age twenty-two) showed that all such efforts were in vain; he proved that no such formula could possibly exist. His proof showed essentially that the existence of such a formula would imply that the alternating group A_5 was not simple, contrary to the above theorem. Later, Galois showed, using the above theorem, that there does not exist an analog of the quadratic formula for the solutions to the general polynomial equations of degrees greater than five as well.

13.2 Maximal normal subgroup

Let G be a group. A **maximal normal subgroup** of G is a normal subgroup M of G satisfying the following properties:

(i) $M \neq G$,

(ii) if $N \lhd G$ and $N \supsetneq M$, then $N = G$.

So a normal subgroup M of G is a maximal normal subgroup if it does not equal G and the only normal subgroup of G properly containing M is G itself.

13.2.1 Theorem. *A normal subgroup M of G is a maximal normal subgroup of G if and only if G/M is simple.*

Proof. Let M be a normal subgroup of G.

($\Rightarrow$) Assume that M is a maximal normal subgroup of G. (Must show that G/M is simple.) First, $M \neq G$, so $|G/M| > 1$ and property (i) in the

definition of simple group is satisfied. Now for property (ii). Let N' be a normal subgroup of G/M and assume that $N' \neq \{M\}$. (Must show that $N' = G/M$.) By our assumption, there exists $aM \in N'$ with $aM \neq M$, so that $a \notin M$ by Corollary 8.3.2. Let $\pi : G \to G/M$ be the canonical epimorphism. By Theorem 11.4.2, $N := \pi^{-1}(N') \lhd G$ and by Theorem 11.6.1, $M = \ker \pi = \pi^{-1}(\{M\}) \subseteq \pi^{-1}(N') = N$. Since $\pi(a) = aM \in N'$, we have $a \in \pi^{-1}(N') = N$. But we have seen that $a \notin M$. Therefore, $N \supsetneqq M$. Our assumption that M is maximal now yields $N = G$. Since π is surjective, we get $G/M = \pi(G) = \pi(N) \subseteq N'$ which forces $N' = G/M$. Thus, G/M is simple.

($\Leftarrow$) Assume that G/M is simple. (Must show that M is a maximal normal subgroup of G.) By our assumption, G/M is not trivial, so $M \neq G$, which shows that M satisfies property (i) in the definition of maximal normal subgroup. Now for property (ii). Let $N \lhd G$ and assume that $N \supsetneqq M$. (Must show that $N = G$.) Again, let $\pi : G \to G/M$ be the canonical epimorphism. By Exercise 11–6, $\pi(N) \lhd G/M$. Now $\pi(N) \neq \{M\}$, since otherwise we would have $N \subseteq \ker \pi = M$. Since G/M is simple, we conclude that $\pi(N) = G/M$, that is $N/M = G/M$.

We are trying to show that $N = G$. The inclusion ($\subseteq$) is immediate, so we just need to check the other inclusion. Let $g \in G$. Then $g \in gM = nM$ for some $n \in N$. Therefore, $g = nm$ for some $m \in M$. But M is contained in N, so $m \in N$ implying $g \in N$. This shows that $G \subseteq N$ and so $N = G$. This concludes the proof that M is a maximal normal subgroup of G. □

13.3 Composition factors

Consider the diagram

$$\begin{array}{c} \mathbf{Z}_6 \\ \Big| \; \mathbf{Z}_3 \\ \langle 3 \rangle \\ \Big| \; \mathbf{Z}_2 \\ \{0\} \end{array}$$

The indication $\mathbf{Z}_3$ says that the quotient group $\mathbf{Z}_6/\langle 3 \rangle$ is isomorphic to $\mathbf{Z}_3$. (Reason: $\langle 3 \rangle = \{0, 3\}$, so the quotient group has order $|\mathbf{Z}_6|/|\langle 3 \rangle| = 6/2 = 3$ by Lagrange's theorem and therefore must be isomorphic to $\mathbf{Z}_3$ by Corollary

8.9.2 and Theorem 6.4.1.) Similarly, the indication $\mathbf{Z}_2$ says that the quotient group $\langle 3\rangle/\{0\}$ is isomorphic to $\mathbf{Z}_2$.

We say that $\mathbf{Z}_6$ has "composition factors $\mathbf{Z}_3$ and $\mathbf{Z}_2$." This example motivates the following definitions.

Let G be a group. A **composition series** of G is a sequence $(G_0, G_1, \ldots, G_r)$ of subgroups of G satisfying the following:

(i) $G_0 = G$.

(ii) $G_r = \{e\}$.

(iii) $G_{i+1} \lhd G_i$ for all $0 \leq i < r$

(iv) G_i/G_{i+1} is simple for all $0 \leq i < r$.

The simple factors G_i/G_{i+1} are the **composition factors** of the series.

Here is the picture for the case $r = 3$:

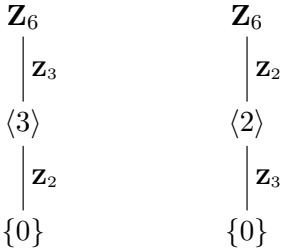
$$
\begin{array}{ccc}
G & = & G_0 \\
 & & \Big| \quad G_0/G_1, \text{ simple} \\
 & & G_1 \\
 & & \Big| \quad G_1/G_2, \text{ simple} \\
 & & G_2 \\
 & & \Big| \quad G_2/G_3, \text{ simple} \\
\{e\} & = & G_3
\end{array}
$$

13.3.1 Theorem. *If G is finite and nontrivial, then G has a composition series.*

Proof. Assume that G is finite and nontrivial. Put $G_0 = G$. Consider the set S of all proper normal subgroups of G_0. Since G_0 is nontrivial, S contains the trivial subgroup $\{e\}$ and is therefore nonempty. Since G_0 is finite, S has only finitely many elements, so we can choose $G_1 \in S$ such that G_1 is not contained in any other element of S. Then G_1 is a maximal normal subgroup of G_0, which implies that G_0/G_1 is simple by Theorem 13.2.1. If $G_1 = \{e\}$, then (G_0, G_1) is a composition series of G. Otherwise, we can use the argument above with G_0 replaced by G_1 to find a normal

subgroup G_2 of G_1 such that G_1/G_2 is simple. Continuing in this fashion we get $G_0, G_1, G_2, \ldots$ and since the orders of these subgroups are strictly decreasing, we must have $G_r = \{e\}$ for some r. This gives a composition series $(G_0, G_1, G_2, \ldots, G_r)$ of G. □

A group can have more than one composition series. For instance, $\mathbf{Z}_6$ has the following:



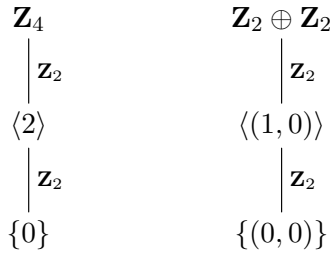
Note that in each case the composition factors, $\mathbf{Z}_3$, $\mathbf{Z}_2$, are the same. This illustrates the following theorem.

13.3.2 Theorem (Jordan-Hölder). *Any two composition series of G have the same composition factors.*

Proof. Omitted. □

We define the **composition factors** of a finite group to be the composition factors of any composition series of the group. This notion is well defined by the last two theorems. The example above shows that $\mathbf{Z}_6$ has composition factors $\mathbf{Z}_3$, $\mathbf{Z}_2$.

The composition factors of a group can be regarded as the group's building blocks (or atoms). It is possible for two nonisomorphic groups to have the same building blocks. For instance, here are composition series for the groups $\mathbf{Z}_4$ and $\mathbf{Z}_2 \oplus \mathbf{Z}_2$, showing that both groups have composition factors $\mathbf{Z}_2$, $\mathbf{Z}_2$:



Yet $\mathbf{Z}_4$ is not isomorphic to $\mathbf{Z}_2 \oplus \mathbf{Z}_2$ since, for instance, the first is cyclic and the second is not (see Theorem 6.5.2). One imagines that the building blocks are stacked differently to form the two groups.

The two main problems in finite group theory are the following:

- Classify the finite simple groups,
- Determine all the ways finite simple groups can be stacked to form other groups.

The first of these means "Find a list of finite simple groups such that every finite simple group is isomorphic to one in the list." (Using the analogy of finite simple groups as atoms, we could view such a list as a sort of periodic table for groups.) In fact, this classification of finite simple groups has been completed (see Section 13.4).

Progress has been made on the second problem, but the feeling is that it is far from being solved. It is the purview of a field of study called "homological algebra."

13.4 Classification of finite simple groups

In the previous section, the finite simple groups were described as the building blocks of which all finite groups are comprised. This makes their classification of particular interest. This classification was completed in 2004.

13.4.1 Theorem. *Every finite simple group is isomorphic to one of the following:*

(i) $\mathbf{Z}_p$ *with* p *prime,*

(ii) A_n *with* $n \geq 5$*,*

(iii) *a finite simple group of Lie type,*

(iv) *a sporadic group, of which there are* 26*.*

(The finite simple groups of Lie type are certain groups of matrices, or variations of such. The 26 sporadic groups are certain simple groups that are not isomorphic to any of the groups in (i−iii). The largest of these sporadic groups is the "Monster group." It has order approximately 8×10^{53}.)

The original proof of this theorem is over $10,000$ pages in length consisting of numerous journal articles contributed by about one hundred mathematicians.

13 – Exercises

13–1 Find the composition factors of the symmetric group S_5. (Support your claim.)

13–2 Find the composition factors of the dihedral group D_4. (Support your claim.)

14 Finite abelian groups

The problem of classifying all finite groups is seemingly intractable (see Section 13.3), but it turns out that adding the assumption of commutativity of the binary operation leaves a much simpler problem.

In fact, the classification of finite *abelian* groups has been known for some time. The theorem says that every finite abelian group is isomorphic to a direct sum of cyclic groups, each having prime power order. (It is customary to use additive notation when referring to an arbitrary abelian group, which is why the theorem uses the term "direct sum" instead of "direct product.")

A more detailed statement of the theorem is given below.

14.1 Fundamental theorem

In the direct sum

$$\mathbf{Z}_{2^1} \oplus \mathbf{Z}_{2^3} \oplus \mathbf{Z}_{3^2} \oplus \mathbf{Z}_{3^4} \oplus \mathbf{Z}_{3^5} \oplus \mathbf{Z}_{5^1} \oplus \mathbf{Z}_{5^8}$$

note that the subscripts

$$2^1, 2^3, 3^2, 3^4, 3^5, 5^1, 5^8$$

are all powers of primes with the different primes increasing from left to right and with the exponents for each prime nondecreasing from left to right.

The main theorem says that every nontrivial finite abelian group is isomorphic to a unique direct sum in such a form.

14.1.1 Theorem (Fundamental theorem of finite abelian groups). *Let G be a nontrivial finite abelian group. There exist unique prime numbers $p_1 < p_2 < \cdots < p_m$ and for each $1 \le i \le m$ unique positive integers $n_{i,1} \le n_{i,2} \le \cdots \le n_{i,r_i}$ such that*

$$\begin{aligned} G \cong\ & \mathbf{Z}_{p_1^{n_{1,1}}} \oplus \cdots \oplus \mathbf{Z}_{p_1^{n_{1,r_1}}} \\ & \oplus \mathbf{Z}_{p_2^{n_{2,1}}} \oplus \cdots \oplus \mathbf{Z}_{p_2^{n_{2,r_2}}} \\ & \vdots \\ & \oplus \mathbf{Z}_{p_m^{n_{m,1}}} \oplus \cdots \oplus \mathbf{Z}_{p_m^{n_{m,r_m}}}. \end{aligned}$$

Proof. Omitted. □

The right-hand side is completely determined by the subscripts. These numbers are the **elementary divisors** of the group G. For instance, if

$$G \cong \mathbf{Z}_{2^3} \oplus \mathbf{Z}_{3^1} \oplus \mathbf{Z}_{3^2} \oplus \mathbf{Z}_{7^3} \oplus \mathbf{Z}_{7^8},$$

then G has elementary divisors 2^3, 3^1, 3^2, 7^3, 7^8.

Note that the order of the group G is the product of its elementary divisors.

14.2 Examples

The following are examples of direct sums that meet the criteria of the theorem:

- $\mathbf{Z}_{2^1} \oplus \mathbf{Z}_{2^3} \oplus \mathbf{Z}_{3^2} \oplus \mathbf{Z}_{5^3} \oplus \mathbf{Z}_{5^6}$,
- $\mathbf{Z}_{3^5} \oplus \mathbf{Z}_{7^2} \oplus \mathbf{Z}_{7^4} \oplus \mathbf{Z}_{19^3} \oplus \mathbf{Z}_{19^8}$,
- $\mathbf{Z}_{7^2}$.

(The last example shows that the direct sum is allowed to have only one summand.)

And here are examples of direct sums that do not meet the criteria:

- $\mathbf{Z}_{2^1} \oplus \mathbf{Z}_{4^3} \oplus \mathbf{Z}_{7^2} \oplus \mathbf{Z}_{7^6}$ (4 is not prime)
- $\mathbf{Z}_{3^2} \oplus \mathbf{Z}_{7^1} \oplus \mathbf{Z}_{5^4}$ (distinct primes are not increasing)
- $\mathbf{Z}_{2^3} \oplus \mathbf{Z}_{2^4} \oplus \mathbf{Z}_{5^6} \oplus \mathbf{Z}_{5^3}$ (exponents of 5 are not nondecreasing)

14.2.1 Example Write a list of groups having the property that every abelian group of order 360 is isomorphic to precisely one member of the list.

Solution We have $360 = 2^3 3^2 5$. Here are the different ways to write the prime powers that appear:

$$2^3,\ 2^1 2^2,\ 2^1 2^1 2^1, \qquad 3^2,\ 3^1 3^1, \qquad 5^1.$$

Therefore, according to Theorem 14.1.1, the desired list of groups is

$$\begin{aligned}
&\mathbf{Z}_{2^3} \oplus \mathbf{Z}_{3^2} \oplus \mathbf{Z}_{5^1} \\
&\mathbf{Z}_{2^3} \oplus \mathbf{Z}_{3^1} \oplus \mathbf{Z}_{3^1} \oplus \mathbf{Z}_{5^1} \\
&\mathbf{Z}_{2^1} \oplus \mathbf{Z}_{2^2} \oplus \mathbf{Z}_{3^2} \oplus \mathbf{Z}_{5^1} \\
&\mathbf{Z}_{2^1} \oplus \mathbf{Z}_{2^2} \oplus \mathbf{Z}_{3^1} \oplus \mathbf{Z}_{3^1} \oplus \mathbf{Z}_{5^1} \\
&\mathbf{Z}_{2^1} \oplus \mathbf{Z}_{2^1} \oplus \mathbf{Z}_{2^1} \oplus \mathbf{Z}_{3^2} \oplus \mathbf{Z}_{5^1} \\
&\mathbf{Z}_{2^1} \oplus \mathbf{Z}_{2^1} \oplus \mathbf{Z}_{2^1} \oplus \mathbf{Z}_{3^1} \oplus \mathbf{Z}_{3^1} \oplus \mathbf{Z}_{5^1}.
\end{aligned}$$

□

A Writing proofs

A.1 Strings of relations

In a string of relations, the main news value should appear at the ends of the string and all of the intermediate steps should be easily verifiable.

- *If* $r > 2$*, then* $r^2 + r - 6 = (r + 3)(r - 2) > 0$ $(r \in \mathbf{R})$.

  The point being made is that if r is greater than 2, then $r^2 + r - 6$ is positive. The equality $r^2+r-6 = (r+3)(r-2)$ is verified by multiplying out the right hand side; the inequality $(r + 3)(r - 2) > 0$ follows from the fact that both factors are positive under the assumption $r > 2$.

- $(2 + 3)^2 = 5^2 = 25 \neq 13 = 4 + 9 = 2^2 + 3^2$.

  This says that $(2 + 3)^2 \neq 2^2 + 3^2$.

- $\frac{1}{2} + \frac{2}{3} - \frac{1}{4} = \frac{6}{12} + \frac{8}{12} - \frac{3}{12} = \frac{11}{12} \notin \mathbf{Z}$.

  This says that $\frac{1}{2} + \frac{2}{3} - \frac{1}{4}$ is not an integer. It is confusing to the reader if this point is made by writing $\frac{11}{12} = \frac{6}{12} + \frac{8}{12} - \frac{3}{12} = \frac{1}{2} + \frac{2}{3} - \frac{1}{4} \notin \mathbf{Z}$. In working from left to right, he can easily check each step except for the last, $\frac{1}{2} + \frac{2}{3} - \frac{1}{4} \notin \mathbf{Z}$. For this, he has to work backwards to see that $\frac{1}{2} + \frac{2}{3} - \frac{1}{4}$ equals $\frac{11}{12}$ which is not an integer.

A.2 If P, then Q.

To prove a statement of the form "If P, then Q" (which is the same as "P implies Q"), assume that P is true and show that Q is true.

- *Let* $a, b, c \in \mathbf{R}$*. If* $a < b$ *and* $c < 0$*, then* $ca > cb$*.*

  Proof: Assume that $a < b$ and $c < 0$. Since $a < b$, we have $a - b < 0$. Therefore, $ca - cb = c(a - b) > 0$. Hence, $ca > cb$, as desired. □

A.3 P if and only if Q

A statement of the form "P if and only if Q" is a combination of the two statements "If P, then Q" and "If Q, then P," so it is often written with a double implication symbol: "$P \Leftrightarrow Q$." To prove such a statement, take each implication separately and proceed as in A.2.

- *For $r \in \mathbf{R}$, $r^2 - 2r = -1$ if and only if $r = 1$.*

  Proof: Let $r \in \mathbf{R}$.

  ($\Rightarrow$) Assume $r^2 - 2r = -1$. Then $(r-1)^2 = r^2 - 2r + 1 = 0$, which implies $r - 1 = 0$. Hence, $r = 1$.

  ($\Leftarrow$) Assume $r = 1$. Then $r^2 - 2r = 1^2 - 2(1) = -1$. □

It is common to use ($\Rightarrow$) and ($\Leftarrow$) as above to introduce the particular implication being proved. Incidentally, you should convince yourself that ($\Leftarrow$) corresponds to the statement "P if Q" while ($\Rightarrow$) corresponds to the statement "P only if Q."

A.4 Counterexample

To show that a statement involving "for every" is false, provide a single, explicit counterexample.

- *For every positive real number r, we have $r^3 > r^2$.*

  This statement is false, for if $r = \frac{1}{2}$, then $r^3 = \frac{1}{8} \not> \frac{1}{4} = r^2$.

I could also have said that the statement is false, for if r is any real number less than 1, then $r^3 - r^2 = r^2(r-1) < 0$, whence $r^3 < r^2$. However, the explicit counterexample above is preferable to this argument in that it is easier to understand and it says just what needs to be said.

A.5 Showing "there exists"

To prove a statement involving "there exists," just exhibit a single such object and show that it satisfies the stated property.

- *There exists an $r \in \mathbf{R}$ satisfying $r^2 + r - 12 = 0$.*

  Proof: Let $r = 3$. Then, $r^2 + r - 12 = 3^2 + 3 - 12 = 0$.

Note that I did not tell the reader how I came up with an r that works. There is no obligation to reveal the thought process that leads to the insight. In fact, doing so risks confusing the reader since it is unexpected. Also, I did not include that $r = -4$ also works since exhibiting a single r sufficed.

A.6 Showing "for every"

To prove a statement involving "for every," start with an arbitrary such object and show that it satisfies the given property.

- *For every $r \in \mathbf{R}$ with $r \geq 3$, we have $r^2 - 2r + 1 \geq 4$.*

  Proof: Let $r \in \mathbf{R}$ with $r \geq 3$. Then $r^2 - 2r + 1 = (r-1)^2 \geq (3-1)^2 = 4$. □

The first sentence of the proof means "Let r denote an arbitrary (i.e., any old) real number greater than or equal to 3."

A.7 Proof by contradiction

There is a method for proving a statement called "Proof by contradiction" which is sometimes useful. To use this method, one assumes that the given statement is false and then proceeds to derive a contradiction. The contradiction signals the presence somewhere of an invalid step. Therefore, provided all the other steps are valid, one can conclude that the initial assumption was not correct, which is to say that the given statement is in fact true.

- *There are infinitely many prime numbers.* (A *prime number* is an integer greater than 1 that is evenly divisible by no positive integers except 1 and itself (e.g., 2, 3, 5, 7, 11, ...).)

  Proof: Suppose the statement is false. In other words, suppose there are only finitely many primes. We may enumerate them: $p_1, p_2, \ldots, p_n$. Consider the number $s := p_1 p_2 \cdots p_n + 1$. Now s is an integer greater than 1, so it must be divisible by some prime, say p_i. This means that $s = p_i m$ for some integer m. But then, $1 = s - p_1 p_2 \cdots p_n = p_i(m - p_1 p_2 \cdots \hat{p_i} \cdots p_n)$ where the symbol $\hat{p_i}$ means "delete p_i." The expression in the parentheses is just some integer and, since it is not possible to multiply the prime p_i by another integer and get 1, this is an obvious contradiction. Hence, our original assumption is wrong, that is, there are infinitely many prime numbers. □

This is essentially Euclid's famous proof of the infinitude of primes.

A.8 Contrapositive

A statement of the form "If P, then Q" is logically equivalent to the statement "If not Q, then not P" meaning that the first statement is true if and only if the second statement is true (you should be able to convince yourself that this is the case). This second statement is called the *contrapositive* of the first. Sometimes, proving the contrapositive of a statement is easier than proving the statement itself.

- *If* $r \neq s$, *then* $2r + 3 \neq 2s + 3$ $(r, s \in \mathbf{R})$.

  Proof: We prove the contrapositive: If $2r + 3 = 2s + 3$, then $r = s$. Assume $2r + 3 = 2s + 3$. Subtracting 3 from both sides and dividing through by 2 gives $r = s$, as desired. □

Occasionally, people give a proof by contradiction (see A.7) of a statement that can be established more directly by proving its contrapositive. For example, to prove the above statement by contradiction, we would start off assuming that there exist $r, s \in \mathbf{R}$ such that $r \neq s$ and $2r + 3 = 2s + 3$. Then, as above, we would obtain $r = s$, contradicting that $r \neq s$. This proof is valid, but it is not as direct as the first proof. When a proof by contradiction ends up contradicting one of the initial assumptions, as in this case, it can usually be recast using the contrapositive. (Note that this was not the case in the example worked for A.7.)

A.9 Negation

In order to formulate the contrapositives of statements or to give proofs by contradiction, one needs to be able to negate statements. Usually, this is easy; for instance, the negative of $a = b$ is $a \neq b$. However, more complicated statements require some thought. Logicians have formal rules that can be used to accurately negate extremely complex statements, but since most statements occurring in mathematics have very simple logical structures, mathematicians tend not to use the formulas relying instead on their own reasoning. Statements involving "for every" sometimes cause problems, so here is an example.

- $ab = ba$ *for every* $a, b \in G$.

  The negative is "There exist $a, b \in G$ such that $ab \neq ba$" (not "$ab \neq ba$ for every $a, b \in G$").

A.10 Variable scope

The "scope" of a variable in a proof refers to the portion of the proof that starts where the variable is introduced and ends where the variable no longer has meaning.

Generally, if a variable x is introduced with "If $x\ldots$" or "For every $x\ldots$," then that variable (and every variable that depends on it), ceases to have meaning at the end of the sentence. Such a variable x is said to have "local scope."

On the other hand, a variable x introduced using "Let $x\ldots$" or "There exists $x\ldots$" has meaning all the way to the end of the proof. Such a variable is said to have "global scope."

- If n is an even integer, then $n = 2m$ for some integer m. Therefore, $m = n/2$.

  (Incorrect. Due to the conditional "If ..." the variable n has no meaning past the first sentence. Since m depends on this n, it too has no meaning past the first sentence.)

- Let n be an even integer. Then $n = 2m$ for some integer m. Therefore, $m = n/2$.

  (Correct. The phrase "Let n be an even integer" fixes an arbitrary even integer, and from that point on n refers to that fixed even integer. The m in the next sentence is chosen to satisfy $n = 2m$, so it too continues to have meaning from that point on.)

- For every odd integer n, the integer $n+1$ is even. Therefore, $n+1 = 2m$ for some $m \in \mathbf{Z}$.

  (Incorrect. Due to the quantifier "For every," n ceases to have meaning past the first sentence.)

- Let n be an odd integer. Then $n + 1$ is even, so $n + 1 = 2m$ for some integer m. Therefore, $m = (n + 1)/2$.

  (Correct. Both n and m have the indicated meaning to the end of the proof, unless the meaning is overwritten by a new statement, such as "Let n be an even integer.")