

INTRODUCTION TO GROUPS AND GEOMETRIES



David W. Lyons
Lebanon Valley College

Lebanon Valley College
Introduction to Groups and Geometries

David W. Lyons

This text is disseminated via the Open Education Resource (OER) LibreTexts Project (<https://LibreTexts.org>) and like the thousands of other texts available within this powerful platform, it is freely available for reading, printing, and "consuming."

The LibreTexts mission is to bring together students, faculty, and scholars in a collaborative effort to provide an accessible, and comprehensive platform that empowers our community to develop, curate, adapt, and adopt openly licensed resources and technologies; through these efforts we can reduce the financial burden born from traditional educational resource costs, ensuring education is more accessible for students and communities worldwide.

Most, but not all, pages in the library have licenses that may allow individuals to make changes, save, and print this book. Carefully consult the applicable license(s) before pursuing such effects. Instructors can adopt existing LibreTexts texts or Remix them to quickly build course-specific resources to meet the needs of their students. Unlike traditional textbooks, LibreTexts' web based origins allow powerful integration of advanced features and new technologies to support learning.



LibreTexts is the adaptable, user-friendly non-profit open education resource platform that educators trust for creating, customizing, and sharing accessible, interactive textbooks, adaptive homework, and ancillary materials. We collaborate with individuals and organizations to champion open education initiatives, support institutional publishing programs, drive curriculum development projects, and more.

The LibreTexts libraries are Powered by [NICE CXone Expert](#) and was supported by the Department of Education Open Textbook Pilot Project, the California Education Learning Lab, the UC Davis Office of the Provost, the UC Davis Library, the California State University Affordable Learning Solutions Program, and Merlot. This material is based upon work supported by the National Science Foundation under Grant No. 1246120, 1525057, and 1413739.

Any opinions, findings, and conclusions or recommendations expressed in this material are those of the author(s) and do not necessarily reflect the views of the National Science Foundation nor the US Department of Education.

Have questions or comments? For information about adoptions or adaptations contact info@LibreTexts.org or visit our main website at <https://LibreTexts.org>.

This text was compiled on 04/01/2026

TABLE OF CONTENTS

Licensing

1: Preliminaries

- 1.1: Complex Numbers
- 1.2: Quaternions
- 1.3: Stereographic Projection
- 1.4: Equivalence Relations

2: Groups

- 2.1: Examples of groups
- 2.2: Definition of a group
- 2.3: Subgroups and Cosets
- 2.4: Group Homomorphisms
- 2.5: Group Actions
- 2.6: Additional exercises

3: Geometries

- 3.1: Geometries and Models
- 3.2: Möbius Geometry
- 3.3: Hyperbolic geometry
- 3.4: Elliptic geometry
- 3.5: Projective Geometry
- 3.6: Additional exercises

Index

Detailed Licensing

Licensing

A detailed breakdown of this resource's licensing can be found in [Back Matter/Detailed Licensing](#).

CHAPTER OVERVIEW

1: Preliminaries

- [1.1: Complex Numbers](#)
- [1.2: Quaternions](#)
- [1.3: Stereographic Projection](#)
- [1.4: Equivalence Relations](#)

This page titled [1: Preliminaries](#) is shared under a [CC BY-NC-SA 4.0](#) license and was authored, remixed, and/or curated by [David W. Lyons](#) via [source content](#) that was edited to the style and standards of the LibreTexts platform.

1.1: Complex Numbers

The complex numbers were originally invented to solve problems in algebra. It was later recognized that the algebra of complex numbers provides an elegant set of tools for geometry in the plane. This section presents the basics of the algebra and geometry of the complex numbers.

Elements in the set of complex numbers $\mathbb{C}$ are in one-to-one correspondence with points in the 2-dimensional real plane $\mathbb{R}^2$ (where $\mathbb{R}$ denotes the set of real numbers). We will write $z \leftrightarrow (x, y)$ to denote that the complex number z corresponds to the ordered pair (x, y) of real numbers.

Real and imaginary parts

Given a complex number z corresponding to the point (x, y) in $\mathbb{R}^2$, we say that x is the **real part** of z and that y is the **imaginary part** of z , denoted $\operatorname{Re}(z) = x$ and $\operatorname{Im}(z) = y$. The set $\mathbb{C}$ contains the set $\mathbb{R}$ as a subset. The real number x , which is also the complex number x , corresponds to the ordered pair $(x, 0)$. A complex number that corresponds to an ordered pair $(0, y)$ is called (**pure**) **imaginary**. The complex number i corresponds to the ordered pair $(0, 1)$. Here is a summary so far.

$$\begin{aligned} z &\leftrightarrow (\operatorname{Re}(z), \operatorname{Im}(z)) \\ x \in \mathbb{R} &\leftrightarrow (x, 0) \\ i &\leftrightarrow (0, 1) \end{aligned}$$

Modulus and argument

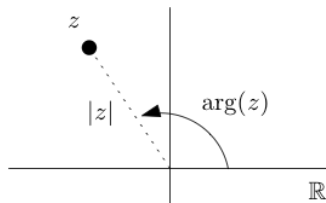


Figure 1.1.1. Norm and argument of a complex number are polar coordinates.

Given a complex number $z \leftrightarrow (x, y)$, let (r, θ) be polar coordinates for the point (x, y) such that $r \geq 0$ and θ is measured in radians. The **modulus** or **norm** of z , denoted $|z|$, is defined to be the polar coordinate $r = \sqrt{x^2 + y^2}$ and the **argument** of z , denoted $\arg(z)$, is the polar coordinate θ , that is, the oriented angle made by the real vector (x, y) with the positive real axis. In other words, $(|z|, \arg z)$ are polar coordinates for the point (x, y) . See Figure 1.1.1. Here is a summary.

Norm and argument.

$$z \leftrightarrow (x, y) = (|z| \cos(\arg z), |z| \sin(\arg z)) \quad (1.1.1)$$

Addition and multiplication of complex numbers

Given complex numbers $z \leftrightarrow (x, y)$ and $z' \leftrightarrow (x', y')$, the sum $z + z'$ is defined by the following.

Complex addition.

$$z + z' \leftrightarrow (x + x', y + y') \quad (1.1.2)$$

In other words, complex addition corresponds to real vector addition. See Figure 1.1.2.

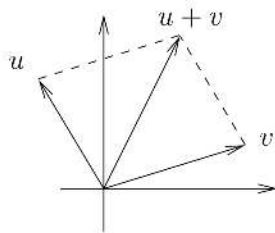


Figure 1.1.2. Complex addition is vector addition

The product zz' is defined as follows.

Complex multiplication.

$$|zz'| = |z||z'| \quad (1.1.3)$$

$$\arg(zz') = \arg z + \arg z' \quad (1.1.4)$$

The interaction between complex addition and multiplication is expressed by the following relationship, which holds for any complex z, u, v . See Figure 1.1.3.

Distributive law.

$$z(u + v) = zu + zv \quad (1.1.5)$$

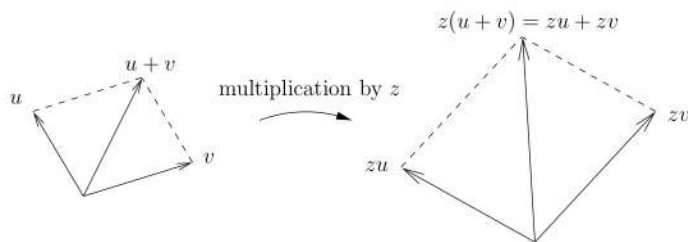


Figure 1.1.3. The distributive law: multiplication by z rotates the vectors u, v , and $u + v$ by angle $\arg z$ and scales by the factor $|z|$.

Below are a number of relationships arising from the definitions of complex addition and multiplication. Let a, b, c, d be real numbers and let z, u, v be complex numbers. The following relationships hold. ¹

$$a + ib \leftrightarrow (a, b) \quad (1.1.6)$$

$$a + b \text{ (complex sum)} = a + b \text{ (real sum)} \quad (1.1.7)$$

$$ab \text{ (complex product)} = ab \text{ (real product)} \quad (1.1.8)$$

$$|a| \text{ (complex norm)} = |a| \text{ (real absolute value)} \quad (1.1.9)$$

$$1z = z1 = z \quad (1.1.10)$$

$$i^2 = -1 \quad (1.1.11)$$

$$(a + ib) + (c + id) = (a + c) + i(b + d) \quad (1.1.12)$$

$$(a + ib)(c + id) = (ac - bd) + i(ad + bc) \quad (1.1.13)$$

The complex exponential function

The Taylor series for the real function $y = e^x$ is

$$e^x = 1 + x + \frac{x^2}{2} + \frac{x^3}{3!} + \dots$$

Convergence for sequences and series of complex numbers can be defined in a way that naturally extends the definitions for real numbers. It turns out that the complex power series

$$1 + z + \frac{z^2}{2} + \frac{z^3}{3!} + \dots$$

converges for every *complex* number z , so we define the *complex* exponential function by

$$e^z = 1 + z + \frac{z^2}{2} + \frac{z^3}{3!} + \cdots.$$

The complex exponential obeys familiar laws of the real exponential. For z, w in $\mathbb{C}$, we have

$$\begin{aligned} e^z e^w &= e^{z+w} \\ e^0 &= 1 \end{aligned}$$

A key property of the complex exponential is the following, called **Euler's formula**.

Euler's formula.

$$e^{it} = \cos t + i \sin t \quad (\text{for } t \text{ real}) \quad (1.1.14)$$

For z with $r = |z|$ and $t = \arg(z)$, the expression $z = re^{it}$ is called the **polar form** for z . By contrast, we call $z = x + iy$ the **rectangular form** (or the **Cartesian form**) for z . **Figure 1.1.4** shows a summary of the geometric content of the rectangular and polar forms for a complex number z .

Here is how complex multiplication looks in polar form. For $z = re^{i\theta}$, $w = se^{i\phi}$, we have

$$zw = (re^{i\theta})(se^{i\phi}) = rse^{i(\theta+\phi)}. \quad (1.1.15)$$

From this it is easy to see that for $r \neq 0$, we have

$$(re^{i\theta}) \left(\frac{1}{r} e^{-i\theta} \right) = 1.$$

For $z = re^{i\theta}$ with $r \neq 0$, we call $\frac{1}{r} e^{-i\theta}$ the **multiplicative inverse** of z , denoted $1/z$ or z^{-1} .

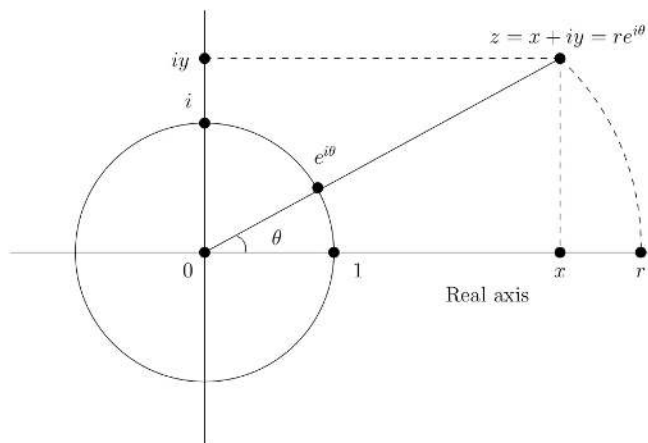


Figure 1.1.4. Rectangular and polar forms for a complex number z

Conjugation

The **conjugate** of the complex number $z = x + iy = re^{i\theta}$, denoted $\bar{z}$ or z^* , is defined to be $z^* = x - iy = re^{-i\theta}$. Geometrically, z^* is the reflection of z across the real axis (the x -axis) in $\mathbb{R}^2$. Here are some relations involving conjugates.

$$\operatorname{Re}(z) = \frac{z + z^*}{2} \quad (1.1.16)$$

$$\operatorname{Im}(z) = \frac{z - z^*}{2i} \quad (1.1.17)$$

$$|z|^2 = zz^* \quad (1.1.18)$$

$$2 \arg z = \frac{z}{z^*} \quad (\text{for } z \neq 0) \quad (1.1.19)$$

$$\frac{1}{z} = \frac{z^*}{zz^*} = \frac{z^*}{|z|^2} \quad (\text{for } z \neq 0) \quad (1.1.20)$$

$$(zw)^* = z^*w^* \quad (1.1.21)$$

Circles and lines

Let C be the circle of radius $r > 0$ and with center $a \in \mathbb{C}$. A point z lies on C if and only if the distance from z to a equals r . In mathematical symbols, C is the set of solutions z for the following equation.

$$|z - a| = r \quad (1.1.22)$$

The real line $\mathbb{R}$ is the set of solutions z of the equation $\operatorname{Im}(z) = 0$. More generally, let L be a line that contains the point $p \in \mathbb{C}$ and makes an angle θ with the real axis (set $\theta = 0$ if L is parallel to the real axis). If $z \in L$, then $e^{-i\theta}(z - p)$ is real, so $\operatorname{Im}(e^{-i\theta}(z - p)) = 0$. See Figure 1.1.5. Conversely, if $e^{-i\theta}(z - p)$ is real, then z lies on L . Multiplying by a positive constant k , and setting $a = ke^{-i\theta}$ and $b = -ke^{-i\theta}p$, we conclude that the line L is the set of solutions to the following equation.

$$\operatorname{Im}(az + b) = 0 \quad (1.1.23)$$

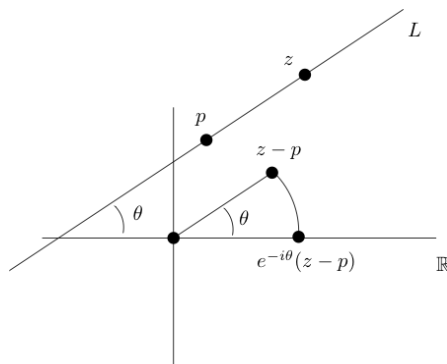


Figure 1.1.5. A line in the complex plane.

Exercises

? Exercise 1

What is the difference between polar coordinates and polar form? What is the difference between rectangular coordinates and rectangular form? Write formulas for converting from polar to rectangular coordinates and vice-versa.

Solution

Let z be a complex number, let $x = \operatorname{Re}(z)$, $y = \operatorname{Im}(z)$, $r = |z|$ and $\theta = \arg(z)$. The pair (r, θ) is called the polar coordinates for z , while the expression $re^{i\theta}$ is called the polar form for z . The pair (x, y) is called the rectangular coordinates for z , while the expression $x + iy$ is called the rectangular form for z .

To convert from polar to rectangular, use the equations $x = r \cos \theta$, $y = r \sin \theta$ (show sketches to explain these formulas). To convert from rectangular to polar, use $r = \sqrt{x^2 + y^2}$ and $\tan \theta = y/x$. For the last equation, you must use judgment when $x = 0$ to decide whether θ should be $\pi/2$ or $-\pi/2$. You must also use judgment when calculating $\theta = \arctan(y/x)$. The standard codomain for arctan is the interval $(-\pi/2, \pi/2)$, so you need to use $\theta = \arctan(y/x) + \pi$ for $x < 0$.

? Exercise 2

Express each of the following in rectangular and polar form.

a. $3(2 - i) + 6(1 + i)$

b. $(2e^{i\pi/6})(3e^{-i\pi/3})$

c. $(2 + 3i)(4 - i)$

d. $(1 + i)^3$

Answer

a. $12 + 3i = \sqrt{153} e^{i \arctan(1/4)}$

b. $6e^{-i\pi/6} = 3\sqrt{3} - 3i$

c. $11 + 10i = \sqrt{221} e^{i \arctan(10/11)}$

d. $-2 + 2i = 2\sqrt{2} e^{i3\pi/4}$

? Exercise 3

Prove the following property of norm.

The triangle inequality.

For any two complex numbers z, w , we have

$$\| |z + w| \leq |z| + |w|. \|$$

Solution

The simplest approach is geometric: Sketch the parallelogram for vector addition and use the fact that the length of any side of a triangle is less than the sum of the lengths of the other two sides.

Here is one route to an algebraic proof: Let $z = a + bi$, $w = c + di$. Manipulate the triangle inequality (start by squaring both sides) to obtain

$$\| 2abcd \leq b^2c^2 + a^2d^2. \|$$

This is the same as the clearly true statement

$$0 \leq b^2c^2 + a^2d^2 - 2abcd = (bc - ad)^2.$$

Conclude by observing that all steps of the derivation are reversible.

? Exercise 4

Prove (1.1.18).

Solution

Let $z = re^{i\theta}$. Then $\bar{z} = re^{-i\theta}$, and we have

$$\begin{aligned} z\bar{z} &= re^{i\theta} re^{-i\theta} \\ &= r^2 e^0 \\ &= r^2 = |z|^2. \end{aligned}$$

? Exercise 5

Let p and q be complex numbers. Prove that the distance (ordinary distance between points in the plane) between p and q is $|p - q|$.

Hint

Use rectangular form.

Solution

Let $p = a + ib$ and $q = c + id$. We have

$$\begin{aligned} |p - q| &= |(a + ib) - (c + id)| \\ &= |(a - c) + i(b - d)| \\ &= \sqrt{(a - c)^2 + (b - d)^2}. \end{aligned}$$

The latter expression is the distance from p to q , so we are done.

? Exercise 6

Express each of the following in rectangular and polar form.

- $\frac{2 + i}{3 - i}$
- $\frac{1 + 2i}{1 - 2i}$
- $\frac{2e^{i\pi/4}}{3e^{-i\pi/2}}$

Answer

- $\frac{1}{2} + \frac{1}{2}i = \frac{\sqrt{2}}{2}e^{i\pi/4}$
- $-\frac{3}{5} + \frac{4}{5}i = e^{i(\arctan(-4/3)+\pi)}$
- $\frac{2}{3}e^{i3\pi/4} = -\frac{\sqrt{2}}{3} + \frac{\sqrt{2}}{3}i$

? Exercise 7

Verify the formulas (1.1.16) and (1.1.17).

Solution

Let $z = x + iy$. Then we have

- $\frac{z + \bar{z}}{2} = \frac{2x}{2} = x = \operatorname{Re}(z)$, and
- $\frac{z - \bar{z}}{2i} = \frac{2iy}{2i} = y = \operatorname{Im}(z)$.

? Exercise 8

Given a nonzero complex number z , explain why z has exactly two square roots, and explain how to find them.

Solution

Since squaring a number squares the norm and doubles the argument, a square root can be found by taking the square root of the norm and dividing the argument by two. That is, for $z = re^{i\theta}$, a square root of z is $\sqrt{r}e^{i\theta/2}$. Another square root of z is

the negative of that expression. Any other square root of z would have to have norm $\sqrt{|z|}$ and argument $\theta/2$ plus or minus an integer multiple of π , so these must be all the square roots of z .

? Exercise 9

Find all complex solutions of the following equations.

a. $z^2 + 3z + 5 = 0$

b. $(z - i)(z + i) = 1$

c. $\frac{2z + i}{-z + 3i} = z$

Answer

a. $-\frac{3}{2} \pm i \frac{\sqrt{11}}{2}$

b. 0

c. $(1/2)[(-2 \pm 281^{1/4} \cos \varphi) + i(3 \pm 281^{1/4} \sin \varphi)]$, where

$\varphi = (\arctan(16/5) + \pi)/2$

? Exercise 10

Use the fact that $e^{ia}e^{ib} = e^{i(a+b)}$ together with Euler's formula $e^{i\theta} = \cos \theta + i \sin \theta$ to derive the trigonometric angle sum formulas below.

$$\begin{aligned}\cos(a + b) &= \cos a \cos b - \sin a \sin b \\ \sin(a + b) &= \cos a \sin b + \sin a \cos b\end{aligned}$$

Solution

Using Euler's formula for the first equality below, and then using complex multiplication for the second equality, we have

$$\begin{aligned}e^{ia}e^{ib} &= (\cos a + i \sin a)(\cos b + i \sin b) \\ &= (\cos a \cos b - \sin a \sin b) + i(\cos a \sin b + \sin a \cos b).\end{aligned}\tag{*}$$

On the other hand, Euler's formula also gives

$$e^{i(a+b)} = \cos(a + b) + i \sin(a + b).\tag{**}$$

Equating real and imaginary parts of (*) and (**) gives the desired trigonometric identities.

? Exercise 11

Circles and lines.

a. For a real variable x and a real constant a , *completing the square* refers to rewriting the expression $x^2 - 2ax$ as follows.

$$x^2 - 2ax = x^2 - 2ax + a^2 - a^2 = (x - a)^2 - a^2.$$

A complex version of completing the square for a complex variable z and a complex constant a is the following.

$$|z|^2 - 2\operatorname{Re}(za^*) = |z - a|^2 - |a|^2\tag{1.1.24}$$

Write a derivation to justify this. Then use completing the square to find the center and radius of the circle given by the equation $|z|^2 - iz + iz^* - 5 = 0$.

b. Write an alternative proof for the general form for the equation of a line (1.1.23), as follows. Let $a = u + iv$, $b = r + is$, $z = x + iy$. Find the equation of the line $\operatorname{Im}(az + b) = 0$ in terms of the real variables x, y and real constants u, v, r, s . Explain why it is

necessary that $a \neq 0$.

? Exercise 12

Complex numbers as 2×2 real matrices.

Let $\mathcal{M}_{\mathbb{C}}$ denote the set of 2×2 matrices of the form $\begin{bmatrix} a & b \\ -b & a \end{bmatrix}$ with $a, b \in \mathbb{R}$. Given a complex number z with Cartesian form $z = a + bi$, let $M(z)$ denote the matrix in $\begin{bmatrix} a & b \\ -b & a \end{bmatrix}$ in $\mathcal{M}_{\mathbb{C}}$. Conversely, given a matrix $M \in \mathcal{M}_{\mathbb{C}}$ with top left entry a and top right entry b , let $C(M)$ denote the complex number $a + bi$. It is clear that the mappings $z \rightarrow M(z)$ and $M \rightarrow C(M)$ are inverses to one another, and establish a one-to-one correspondence $\mathbb{C} \leftrightarrow \mathcal{M}_{\mathbb{C}}$.

a. Show that $\mathcal{M}_{\mathbb{C}}$ is closed under addition and multiplication. That is, suppose that M, N are elements of $\mathcal{M}_{\mathbb{C}}$. Show that $M + N$ and MN are also elements of $\mathcal{M}_{\mathbb{C}}$.

b. Show that complex addition and multiplication are "mirrored" in $\mathcal{M}_{\mathbb{C}}$. That is, show that $C(M(z) + M(w)) = z + w$ and $C(M(z)M(w)) = zw$ for all $z, w \in \mathbb{C}$.

This page titled [1.1: Complex Numbers](#) is shared under a [CC BY-NC-SA 4.0](#) license and was authored, remixed, and/or curated by [David W. Lyons](#) via [source content](#) that was edited to the style and standards of the LibreTexts platform.

1.2: Quaternions

The quaternions, discovered by William Rowan Hamilton in 1843, were invented to capture the algebra of rotations of 3-dimensional real space, extending the way that the complex numbers capture the algebra of rotations of 2-dimensional real space.

Elements in the set of quaternions $\mathbb{H}$ are in one-to-one correspondence with points in 4-dimensional real space $\mathbb{R}^4$. We will write $r \leftrightarrow (t, x, y, z)$ to denote that the quaternion r corresponds to the 4-tuple (t, x, y, z) of real numbers.

Cartesian form and pure quaternions

The quaternions i, j, k are defined as follows.

$$i \leftrightarrow (0, 1, 0, 0) \quad (1.2.1)$$

$$j \leftrightarrow (0, 0, 1, 0) \quad (1.2.2)$$

$$k \leftrightarrow (0, 0, 0, 1) \quad (1.2.3)$$

The expression $r = a + bi + cj + dk$ is called the **Cartesian form** of the quaternion that corresponds to the vector (a, b, c, d) in $\mathbb{R}^4$. A quaternion of the form $a = a + 0i + 0j + 0k \leftrightarrow (a, 0, 0, 0)$ is called a **scalar** quaternion or a **real** quaternion. A quaternion of the form $xi + yj + zk \leftrightarrow (0, x, y, z)$ is called a **pure** quaternion or an **imaginary** quaternion. For a quaternion $r = a + bi + cj + dk$, we call the real quaternion a the **scalar part** or **real part** of r , and we call the quaternion $xi + yj + zk$ the **vector part** or the **imaginary part** of r . To reflect the natural correspondence of the pure quaternion $xi + yj + zk$ with the vector (x, y, z) in $\mathbb{R}^3$ we will write $\mathbb{R}_{\mathbb{H}}^3$ to denote the space of pure quaternions.

Correspondence with complex matrices

Analogous to the way that the complex numbers $\mathbb{C}$ can be realized as the set $\mathcal{M}_{\mathbb{C}}$ of 2×2 real matrices (see [Exercise 1.1.7.12](#)), the quaternions can be realized by a set of 2×2 complex matrices, as follows. Let $\mathcal{M}_{\mathbb{H}}$ denote the set of 2×2 complex matrices of the form $\begin{bmatrix} u & v \\ -v^* & u^* \end{bmatrix}$. Given a quaternion $r = a + bi + cj + dk$, let u, v be the complex numbers $u = a + bi$ and $v = c + di$, and let $M(r)$ denote the 2×2 matrix in $\mathcal{M}_{\mathbb{H}}$ given by

$$M(r) = \begin{bmatrix} u & v \\ -v^* & u^* \end{bmatrix}.$$

Conversely, given a matrix $M \in \mathcal{M}_{\mathbb{H}}$, with top left entry $a + bi$ and top right entry $c + di$, let $Q(M)$ denote the quaternion $r = a + bi + cj + dk$. It is clear that the mappings $r \rightarrow M(r)$ and $M \rightarrow Q(M)$ are inverses to one another, and establish a one-to-one correspondence $\mathbb{H} \leftrightarrow \mathcal{M}_{\mathbb{H}}$.

 **Proposition 1.2.1.** $\mathcal{M}_{\mathbb{H}}$ is closed under addition and multiplication.

Let M, N be elements of $\mathcal{M}_{\mathbb{H}}$. Then the sum $M + N$ and the product MN are also elements of $\mathcal{M}_{\mathbb{H}}$.

Checkpoint 1.2.2.

Prove **Proposition 1.2.1**.

Addition and multiplication

By virtue of **Proposition 1.2.1**, we can define addition and multiplication of quaternions r, s as follows.

$$r + s = Q(M(r) + M(s)) \quad (1.2.4)$$

$$rs = Q(M(r)M(s)) \quad (1.2.5)$$

Because matrix algebra has associative and distributive laws, these carry over to quaternions. Note that quaternion multiplication is not commutative! However, for any real quaternion a , we have $M(a) = aId$, so $M(a)$ commutes with all matrices, and therefore a commutes with all quaternions. To summarize, let q, r, s be quaternions and let a be a real quaternion. We have the following.

$$q(rs) = (qr)s \quad (\text{associative law of multiplication}) \quad (1.2.6)$$

$$q(r + s) = qr + qs \quad (\text{distributive law}) \quad (1.2.7)$$

$$ar = ra \quad (\text{real quaternions commute with all quaternions}) \quad (1.2.8)$$

In practice, it is not necessary to convert quaternions to matrices in order to add and multiply. Quaternion addition and multiplication in Cartesian form is analogous to complex multiplication, using the following basic multiplication rules.

$$i^2 = j^2 = k^2 = -1 \quad (1.2.9)$$

$$ij = -ji = k, \quad jk = -kj = i, \quad ki = -ik = j \quad (1.2.10)$$

Checkpoint 1.2.3.

Verify (1.2.9) and (1.2.10).

For $r = a + bi + cj + dk$ and $r' = a' + b'i + c'j + d'k$, we have

$$r + r' = (a + a') + (b + b')i + (c + c')j + (d + d')k. \quad (1.2.11)$$

Multiplication looks like this.

$$\begin{aligned} rr' &= (a + bi + cj + dk)(a' + b'i + c'j + d'k) \\ &= aa' + bb'i^2 + cc'j^2 + dd'k^2 \\ &\quad + ab'i + ba'i + cd'jk + dc'kj \\ &\quad + ac'j + ca'j + bd'ik + db'ki \\ &\quad + ad'k + da'k + bc'ij + cb'ji \\ &= (aa' - bb' - cc' - dd') \\ &\quad + (ab' + ba' + cd' - dc')i \\ &\quad + (ac' + ca' - bd' + db')j \\ &\quad + (ad' + da' + bc' - cb')k \end{aligned} \quad (1.2.12)$$

If u, v are pure quaternions, (1.2.12) can be written more compactly in terms of the dot and cross products for vectors in $\mathbb{R}^3$.

$$uv = -(u \cdot v) + u \times v \quad (\text{for pure quaternions } u, v) \quad (1.2.13)$$

Checkpoint 1.2.4.

Verify (1.2.13).

Conjugate, modulus, and polar form

The **conjugate** of a quaternion $r = a + bi + cj + dk$ is $r^* = a - bi - cj - dk$, and the **modulus** of r is $|r| = \sqrt{a^2 + b^2 + c^2 + d^2}$. The **unit quaternions**, denoted $U(\mathbb{H})$, is the set of quaternions with modulus 1.¹

Analogous to complex numbers, quaternions can be expressed in *polar form*. Given a nonzero quaternion r , the quaternion $r' = \frac{r}{|r|}$ is a unit quaternion, say $r' = a + bi + cj + dk$. If $|a| < 1$, let $u = \frac{1}{\sqrt{1-a^2}}(bi + cj + dk)$ be the unit pure quaternion obtained by normalizing the pure quaternion $bi + cj + dk$. Let $\theta = \arccos a$. The expression

$$r = |r|(\cos \theta + u \sin \theta) \quad (1.2.14)$$

is called the **polar form** of r .

Checkpoint 1.2.5.

Fill in the remaining details on polar form for quaternions. What happens if $r = 0$? What happens if $|a| = 1$?

Continuing the analogy with complex numbers, we have the following, for all quaternions r, s .

$$(rs)^* = s^*r^* \quad (1.2.15)$$

$$|rs| = |r||s| \quad (1.2.16)$$

$$|r|^2 = rr^*. \quad (1.2.17)$$

Checkpoint 1.2.6.

Verify the three equations above.

Quaternions as rotations of $\mathbb{R}_{\mathbb{H}}^3$

Let r be a unit quaternion and let v be a pure quaternion. Let $R_r(v)$ denote the quaternion $R_r(v) = rvr^*$. It is easy to check that $(R_r(v))^* = -R_r(v)$. From this we conclude that rvr^* is a pure quaternion.

Checkpoint 1.2.7.

Explain how "we conclude" that $R_r(v)$ is pure when r is a unit quaternion and v is a pure quaternion.

It is easy to see that R_r is a linear map from the real vector space of unit quaternions to itself. That means that the following properties hold for all pure quaternions v, w and all real scalars α .

$$R_r(v + w) = R_r(v) + R_r(w) \quad (1.2.18)$$

$$R_r(\alpha v) = \alpha R_r(v) \quad (1.2.19)$$

Checkpoint 1.2.8.

Show the details to prove that R_r is linear.

We conclude with the main result of this section that shows how rotations of 3-dimensional real space are encoded in the algebra of quaternions.

Proposition 1.2.9. Quaternions and rotations of $\mathbb{R}_{\mathbb{H}}^3$

Let $r = \cos \theta + u \sin \theta$ be a unit quaternion in polar form, and let R_r be the linear transformation of the space of pure quaternions given by $v \rightarrow rvr^*$. The action of R_r is a rotation by 2θ radians about the axis given by the unit vector u .

Proof

See Exercise 1.2.6.2.

Exercises

? Exercise 1

Let r be a pure, unit quaternion. Use (1.2.13) to show that the map $\mathbb{R}_{\mathbb{H}}^3 \rightarrow \mathbb{R}_{\mathbb{H}}^3$ given by $u \rightarrow rur$ is the reflection across the plane normal to r . That is, show that $ru r = u - 2(u \cdot r)r$. See Figure 1.2.10.

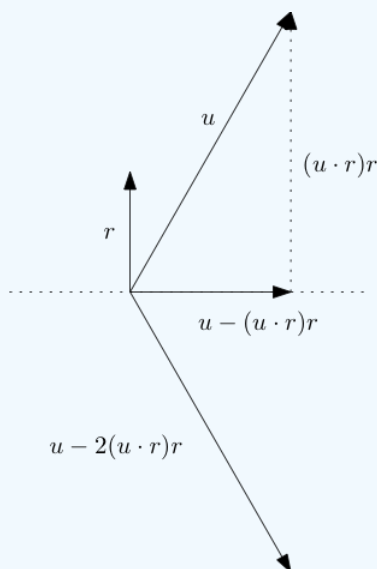


Figure 1.2.10. The reflection of $u \in \mathbb{R}_{\mathbb{H}}^3$ across the plane normal to $r \in \mathbb{R}_{\mathbb{H}}^3$.

? Exercise 2

Prove [Proposition 1.2.9](#) using the following outline. Let $r = \cos \theta + u \sin \theta$ be the polar form for a unit quaternion r .

- Show that $R_r(u) = u$.
- Let v be any pure unit quaternion orthogonal to u , and let $w = u \times v$, so that the triple u, v, w forms a right-handed coordinate system for $\mathbb{R}^3$. Show that

$$R_r(v) = \cos(2\theta)v + \sin(2\theta)w$$

(use equation (1.2.13)) and explain how this proves the Proposition.

? Exercise 1.2.1

Show that the following hold for all $r, s \in U(\mathbb{H})$.

- $R_r \circ R_s = R_{rs}$.
- $(R_r)^{-1} = R_{r^*}$.

This page titled [1.2: Quaternions](#) is shared under a [CC BY-NC-SA 4.0](#) license and was authored, remixed, and/or curated by [David W. Lyons](#) via [source content](#) that was edited to the style and standards of the LibreTexts platform.

1.3: Stereographic Projection

Stereographic projection $S^1 \rightarrow \hat{\mathbb{R}}$

Let S^1 denote the unit circle in the x, y -plane.

$$S^1 = \{(x, y) \in \mathbb{R}^2: x^2 + y^2 = 1\} \quad (1.3.1)$$

Let $N = (0, 1)$ denote the "north pole" (that is, the point at the "top" of the unit circle). Given a point $P = (x, y) \neq N$ on the unit circle, let $s(P)$ denote the intersection of the line $\overline{NP}$ with the x -axis. See **Figure 1.3.1**. The map $s: S^1 \setminus \{N\} \rightarrow \mathbb{R}$ given by this rule is called **stereographic projection**. Using similar triangles, it is easy to see that $s(x, y) = \frac{x}{1-y}$.

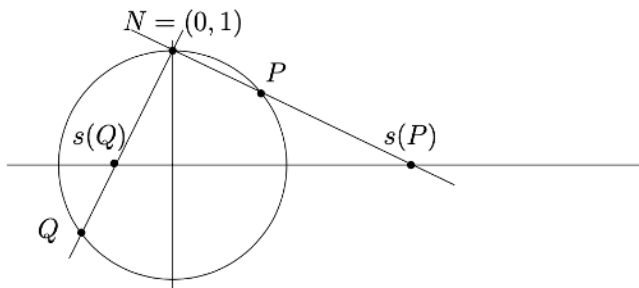


Figure 1.3.1. Stereographic projection

Checkpoint 1.3.2.

Draw the relevant similar triangles and verify the formula $s(x, y) = \frac{x}{1-y}$.

We extend stereographic projection to the entire unit circle as follows. We call the set

$$\hat{\mathbb{R}} = \mathbb{R} \cup \{\infty\} \quad (1.3.2)$$

the **extended real numbers**, where " ∞ " is an element that is not a real number. Now we define stereographic projection $s: S^1 \rightarrow \hat{\mathbb{R}}$ by

$$s(x, y) = \begin{cases} \frac{x}{1-y} & y \neq 1 \\ \infty & y = 1 \end{cases} \quad (1.3.3)$$

Stereographic projection $S^2 \rightarrow \hat{\mathbb{C}}$

The definitions in the previous subsection extend naturally to higher dimensions. Here are the details for the main case of interest.

Let S^2 denote the unit sphere in $\mathbb{R}^3$.

$$S^2 = \{(a, b, c) \in \mathbb{R}^3: a^2 + b^2 + c^2 = 1\} \quad (1.3.4)$$

Let $N = (0, 0, 1)$ denote the "north pole" (that is, the point at the "top" of the sphere, where the positive z -axis is "up"). Given a point $P = (a, b, c) \neq N$ on the unit sphere, let $s(P)$ denote the intersection of the line $\overline{NP}$ with the x, y -plane, which we identify with the complex plane $\mathbb{C}$. See **Figure 1.3.3**. The map $s: S^2 \setminus \{N\} \rightarrow \mathbb{C}$ given by this rule is called **stereographic projection**. Using similar triangles, it is easy to see that $s(a, b, c) = \frac{a+ib}{1-c}$.

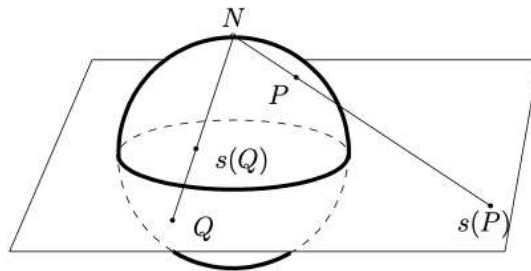


Figure 1.3.3. Stereographic projection

We extend stereographic projection to the entire unit sphere as follows. We call the set

$$\hat{\mathbb{C}} = \mathbb{C} \cup \{\infty\} \quad (1.3.5)$$

the **extended complex numbers**, where " ∞ " is an element that is not a complex number. Now we define stereographic projection $s: S^2 \rightarrow \hat{\mathbb{C}}$ by

$$s(a, b, c) = \begin{cases} \frac{a+ib}{1-c} & c \neq 1 \\ \infty & c = 1 \end{cases}. \quad (1.3.6)$$

Exercises

Formulas for inverse stereographic projection.

It is intuitively clear that stereographic projection is a bijection. Make this rigorous by finding a formula for the inverse.

? Exercise 1

For $s: S^1 \rightarrow \hat{\mathbb{R}}$, find a formula for $s^{-1}: \hat{\mathbb{R}} \rightarrow S^1$. Find $s^{-1}(3)$.

Answer

$$s^{-1}(r) = \begin{cases} \left(\frac{2r}{r^2+1}, \frac{r^2-1}{r^2+1} \right) & \text{if } r \neq \infty \\ (0, 1) & \text{if } r = \infty \end{cases}$$

$$s^{-1}(3) = (3/5, 4/5)$$

? Exercise 2

For $s: S^2 \rightarrow \hat{\mathbb{C}}$, find a formula for $s^{-1}: \hat{\mathbb{C}} \rightarrow S^2$. Find $s^{-1}(3+i)$.

Answer

$$s^{-1}(z) = \begin{cases} \left(\frac{2\operatorname{Re}(z)}{|z|^2+1}, \frac{2\operatorname{Im}(z)}{|z|^2+1}, \frac{|z|^2-1}{|z|^2+1} \right) & \text{if } z \neq \infty \\ (0, 0, 1) & \text{if } z = \infty \end{cases}$$

$$s^{-1}(3+i) = (6/11, 2/11, 9/11)$$

Conjugate transformations.

Let $\mu: X \rightarrow Y$ be a bijective map. We say that maps $f: X \rightarrow X$ and $g: Y \rightarrow Y$ are **conjugate transformations** (with respect to the bijection μ) if $f = \mu^{-1} \circ g \circ \mu$.

? Exercise 3

Show that the maps $S^1 \rightarrow S^1$ given by $(x, y) \rightarrow (x, -y)$ and $\hat{\mathbb{R}} \rightarrow \hat{\mathbb{R}}$ given by $x \rightarrow 1/x$ are conjugate transformations with respect to stereographic projection

? Exercise 4

Show that the map $R_{Z,\theta}: S^2 \rightarrow S^2$ given by $(a, b, c) \rightarrow (a \cos \theta - b \sin \theta, a \sin \theta + b \cos \theta, c)$ (a rotation about the z -axis by angle θ) and the map $T_{Z,\theta}: \hat{\mathbb{C}} \rightarrow \hat{\mathbb{C}}$ given by $z \rightarrow e^{i\theta} z$ are conjugate transformations with respect to stereographic projection.

? Exercise 5

Show that the map $R_{X,\pi}: S^2 \rightarrow S^2$ given by $(a, b, c) \rightarrow (a, -b, -c)$ (rotation about the x -axis by π radians) and the map $T_{X,\pi}: \hat{\mathbb{C}} \rightarrow \hat{\mathbb{C}}$ given by $z \rightarrow 1/z$ are conjugate transformations with respect to stereographic projection.

? Exercise 6

Show that the map $R_{X,\pi/2}: S^2 \rightarrow S^2$ given by $(a, b, c) \rightarrow (a, -c, b)$ (rotation about the x -axis by $\pi/2$ radians) and the map $T_{X,\pi/2}: \hat{\mathbb{C}} \rightarrow \hat{\mathbb{C}}$ given by $z \rightarrow \frac{z+i}{iz+1}$ are conjugate transformations with respect to stereographic projection.

7. Projections of endpoints of diameters.

Show that $s(a, b, c)(s(-a, -b, -c))^* = -1$ for any point (a, b, c) in S^2 with $|c| \neq 1$. Conversely, suppose that $zw^* = -1$ for some $z, w \in \mathbb{C}$. Show that .

This page titled [1.3: Stereographic Projection](#) is shared under a [CC BY-NC-SA 4.0](#) license and was authored, remixed, and/or curated by [David W. Lyons](#) via [source content](#) that was edited to the style and standards of the LibreTexts platform.

1.4: Equivalence Relations

Definitions

A relation on a set X is a subset of $X \times X$. Given a relation $R \subseteq X \times X$, we write $x \sim_R y$, or just $x \sim y$ if R is understood by context, to denote that $(x, y) \in R$. A relation is **reflexive** if $x \sim x$ for every x in X . A relation is **symmetric** if $x \sim y$ implies $y \sim x$. A relation is **transitive** if $x \sim y$ and $y \sim z$ together imply that $x \sim z$. A relation is called an **equivalence relation** if it is reflexive, symmetric, and transitive. Given an equivalence relation on X and an element $x \in X$, we write $[x]$ to denote the set

$$[x] = \{y \in X : x \sim y\}, \quad (1.4.1)$$

called the **equivalence class** of the element x . The set of equivalence classes is denoted $X/\sim$, that is,

$$X/\sim = \{[x] : x \in X\}. \quad (1.4.2)$$

A **partition** of a set X is a collection of nonempty disjoint sets whose union is X .

Facts

Fact 1.4.1. Equivalence relations and partitions.

Let X be a set. Equivalence relations on X and partitions of X are in one-to-one correspondence, as follows. Given an equivalence relation $\sim$ on X , the collection

$$X/\sim = \{[x] : x \in X\}$$

is a partition of X . Conversely, given a partition $\mathcal{P}$ of X , the relation $\sim_{\mathcal{P}}$ defined by

$$x \sim_{\mathcal{P}} y \Leftrightarrow x, y \text{ lie in the same element of } \mathcal{P}$$

is an equivalence relation. These correspondences are inverse to one another. That is, $\sim = \sim_{(X/\sim)}$ and $X/(\sim_{\mathcal{P}}) = \mathcal{P}$.

Fact 1.4.2. Construction of functions on sets of equivalence classes.

Let $\sim$ be an equivalence relation on a set X , let $\pi : X \rightarrow X/\sim$ denote the map given by $x \rightarrow [x]$, and let $f : X \rightarrow Y$ be a function. There exists a map $\bar{f} : X/\sim \rightarrow Y$ such that $(\bar{f} \circ \pi)(x) = f(x)$ for all $x \in X$ if and only if f is constant on equivalence classes (that is, if and only if $[x \sim y \Rightarrow f(x) = f(y)]$).

Note on terminology: when a function f is constant on equivalence classes, we say that the associated function $\bar{f}$ is **well-defined**.

Fact 1.4.3. Construction of equivalence relations and partitions from functions.

Given a function $f : X \rightarrow Y$, there is a natural equivalence relation $\sim_f$ on X given by $x \sim_f y$ if and only if $f(x) = f(y)$. The corresponding set of equivalence classes is $X/\sim_f = \{f^{-1}(y) : y \in f(X)\}$. Furthermore, the function $X/\sim_f \rightarrow f(X)$ given by $[x] \rightarrow f(x)$ is a one-to-one correspondence.

Important example: the integers modulo an integer n

Let n be a positive integer. Let $\sim_n$ be the relation on the integers $\mathbb{Z}$ given by

$$x \sim_n y \Leftrightarrow n \mid (x - y)$$

(recall that the symbols " $a \mid b$ " for integers a, b , pronounced " a divides b ", means $b = ka$ for some integer k). It is easy to show that $\sim_n$ is an equivalence relation, and that the equivalence classes are precisely the set

$$\mathbb{Z}/\sim_n = \{[0], [1], [2], \dots, [n-1]\}.$$

Checkpoint 1.4.4.

1. Verify that the relation $\sim_n$ is indeed an equivalence relation.

2. Verify that the equivalence classes of the equivalence relation $\sim_n$ are indeed $\{[0], [1], [2], \dots, [n-1]\}$. Hint: Use the **division algorithm**, which says that for any $x \in \mathbb{Z}$, there are unique integers q, r , with r in the range $0 \leq r \leq n-1$, such that $x = qn + r$.

This set of equivalence classes is fundamental and pervasive in mathematics. Instead of writing $\mathbb{Z}/\sim_n$, the universally used notation is $\mathbb{Z}_n$. Instead of writing $x \sim_n y$, the universally used notation is $x = y \pmod n$ (or sometimes $x \equiv y \pmod n$).

A useful tool: commutative diagrams

A **directed graph** (or digraph) is a set V of vertices and a set $E \subset V \times V$ of directed edges. We draw pictures of digraphs by drawing an arrow pointing from a vertex v to a vertex w whenever $(v, w) \in E$. See Figure 1.4.5.

A **path** in a directed graph is a sequence of vertices $v_0, v_1, \dots, v_n$ such that $(v_{i-1}, v_i) \in E$ for $1 \leq i \leq n$. The vertex v_0 is called the **initial vertex** and v_n is called the **final vertex** of the path $v_0, v_1, \dots, v_n$.

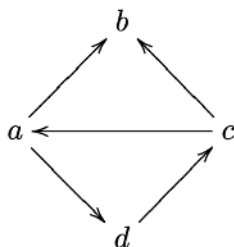


Figure 1.4.5. Example of a directed graph with vertex set $V = \{a, b, c, d\}$ and edge set $E = \{(a, b), (b, c), (c, a), (a, d), (d, c)\}$. The vertex sequences c, b and c, a, b are both paths from c to b .

A **commutative diagram** is a directed graph with two properties.

1. Vertices are labeled by sets and directed edges are labeled by functions between those sets. That is, the directed edge $f = (X, Y)$ denotes a function $f: X \rightarrow Y$.
2. Whenever there are two paths from an initial vertex X to a final vertex Y , the composition of functions along one path is equal to the composition of functions along the other path. That is, if $X_0, X_1, \dots, X_n$ is a path with edges $f_i: X_{i-1} \rightarrow X_i$ for $1 \leq i \leq n$ and $X_0 = Y_0, Y_1, Y_2, \dots, Y_m = X_n$ is a path with edges $g_i: Y_{i-1} \rightarrow Y_i$ for $1 \leq i \leq m$, then

$$f_n \circ f_{n-1} \circ \dots \circ f_1 = g_m \circ g_{m-1} \circ \dots \circ g_1.$$

Figure 1.4.6 shows a commutative diagram that goes with **Fact 1.4.2**.

Figure 1.4.7 shows a commutative diagram that illustrates the definition of conjugate transformations.

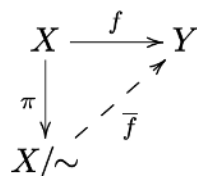


Figure 1.4.6. A commutative diagram showing the relationship $\bar{f} \circ \pi = f$ in **Fact 1.4.2**.

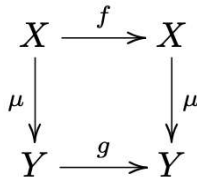


Figure 1.4.7. A commutative diagram illustrating the definition of conjugate transformations f, g given in Exercise Group 1.3.3.3–6.

Exercises

The integers modulo n . Let n be a positive integer.

? Exercise 1

Let ω be the complex number $\omega = e^{2\pi i/n}$, and let $f: \mathbb{Z} \rightarrow \mathbb{C}$ be given by $m \rightarrow \omega^m$. Show that the equivalence relation $\sim_f$ given by Fact 1.4.3 is the same as $\sim_n$.

? Exercise 2

Show that the operation of addition on $\mathbb{Z}_n$ given by

$$[x] + [y] := [x + y]$$

is **well-defined**. This means showing that if $[x] = [x']$ and $[y] = [y']$, then $[x + y] = [x' + y']$.

? Exercise 3

Show that the operation of multiplication on $\mathbb{Z}_n$ given by

$$[x] \cdot [y] := [xy]$$

is well-defined.

? Exercise 4

Alternative construction of $\mathbb{Z}_n$ Another standard definition of the set $\mathbb{Z}_n$, together with its operations of addition and multiplication, is the following. Given an integer a , we write $a \text{ MOD } n$ to denote the **remainder** obtained when dividing a by n (the integer $a \text{ MOD } n$ is the same as the integer r in the statement of the division algorithm given in Checkpoint 1.4.4). Now define $\mathbb{Z}_n$ to be the set

$$\mathbb{Z}_n = \{0, 1, 2, \dots, n-1\},$$

define the addition operation $+_n$ on $\mathbb{Z}_n$ by

$$x +_n y = (x + y) \text{ MOD } n$$

and define the multiplication operation $\cdot_n$ on $\mathbb{Z}_n$ by

$$x \cdot_n y = (xy) \text{ MOD } n.$$

Show that this version of $\mathbb{Z}_n$ is equivalent to the version developed in Exercise 1.4.5.2 and Exercise 1.4.5.3.

? Exercise 5

Commutative diagram examples.

1. Draw a commutative diagram that illustrates the results of **Exercise 1.3.3.5**.
2. The **distributive law** for $\mathbb{Z}_n$ says that

$$[x]([y] + [z]) = [x][y] + [x][z]$$

for all $[x], [y], [z] \in \mathbb{Z}_n$. Label the maps in the commutative diagram below to express the distributive law.

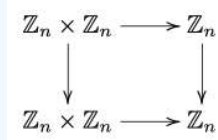


Figure 1.4.8.

? Exercise 6

Prove **Fact 1.4.1**.

? Exercise 7

Prove **Fact 1.4.2**.

? Exercise 8

Prove **Fact 1.4.3**.

This page titled [1.4: Equivalence Relations](#) is shared under a [CC BY-NC-SA 4.0](#) license and was authored, remixed, and/or curated by [David W. Lyons](#) via [source content](#) that was edited to the style and standards of the LibreTexts platform.

CHAPTER OVERVIEW

2: Groups

- [2.1: Examples of groups](#)
- [2.2: Definition of a group](#)
- [2.3: Subgroups and Cosets](#)
- [2.4: Group Homomorphisms](#)
- [2.5: Group Actions](#)
- [2.6: Additional exercises](#)

This page titled [2: Groups](#) is shared under a [CC BY-NC-SA 4.0](#) license and was authored, remixed, and/or curated by [David W. Lyons](#) via [source content](#) that was edited to the style and standards of the LibreTexts platform.

2.1: Examples of groups

Groups are one of the most basic algebraic objects, yet have structure rich enough to be widely useful in all branches of mathematics and its applications. A group is a set G with a binary operation $G \times G \rightarrow G$ that has a short list of specific properties. Before we give the complete definition of a group in the next section (see **Definition 2.2.1**), this section introduces examples of some important and useful groups.

Permutations

A **permutation** of a set X is a bijection from X to itself, that is, a function that is both one-to-one and onto. Given two permutations α, β of a set X , we write $\alpha\beta$ to denote the composition of functions $\alpha \circ \beta$.

Definition 2.1.1.

Let X be a set and let $\text{Perm}(X)$ denote the set of all permutations of X . The **group of permutations of X** is the set $G = \text{Perm}(X)$ together with the binary operation $G \times G \rightarrow G$ given by function composition, that is, $(\alpha, \beta) \rightarrow \alpha \circ \beta$. For the special case $X = \{1, 2, \dots, n\}$ for some integer $n \geq 1$, the group $\text{Perm}(X)$ is called the **symmetric group**, and is denoted S_n .

Checkpoint 2.1.2.

A permutation σ of $X = \{1, 2, \dots, n\}$ can be specified by a list of values $[\sigma(1), \sigma(2), \dots, \sigma(n)]$.¹ For example, the list $[3, 1, 2]$ specifies the permutation $\sigma: \{1, 2, 3\} \rightarrow \{1, 2, 3\}$ given by

$$\sigma(1) = 3, \sigma(2) = 1, \sigma(3) = 2.$$

Let $\tau = [2, 1, 3]$. Find $\sigma\tau$, $\tau\sigma$, and $\sigma^2 = \sigma\sigma$.

Answer

$$\sigma\tau = [1, 3, 2], \tau\sigma = [3, 2, 1], \sigma^2 = [2, 3, 1]$$

Symmetries of regular polygons

Informally and intuitively, we say that regular polygons have rotational and mirror symmetries. Specifically, the rotational symmetries are rotations about the center O of the polygon, clockwise or counterclockwise, by some angle $\angle POP'$, where P, P' are any two vertices. The mirror symmetries of the polygon are reflections across lines of the form $\overline{OP}$ or $\overline{OM}$, where P is any vertex and M is the midpoint of any edge of the polygon. See **Figure 2.1.3**.

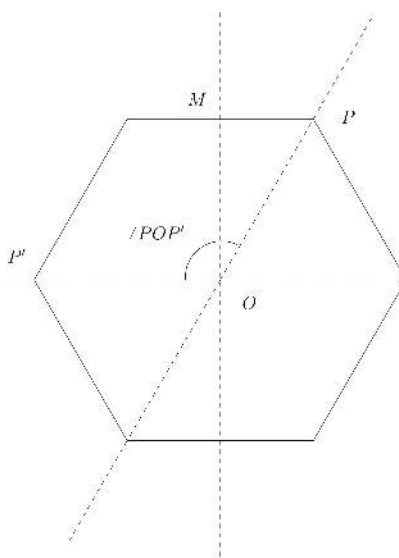


Figure 2.1.3. Symmetries of a regular n -gon

Here are some standard notations for rotations and reflections in the plane. See **Figure 2.1.4**.

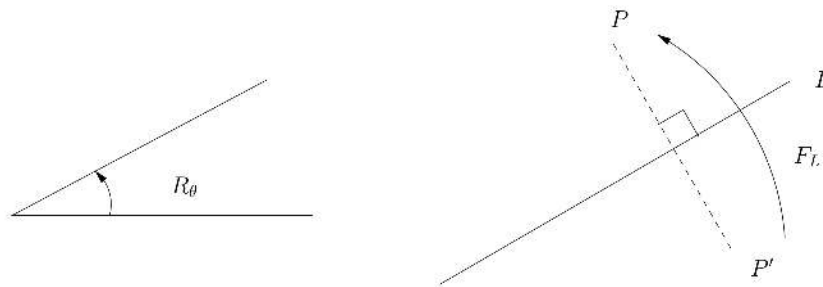


Figure 2.1.4. Rotations and reflections in the plane

Rotations in the plane.

Fix a center point O . We write R_θ to denote the rotation by angle θ about the point O . Angle units can be revolutions or degrees or radians, whatever is most convenient. We observe the usual convention that positive values of θ denote counterclockwise rotations and negative values of θ denote clockwise rotations.

Reflections in the plane.

We write F_L to denote the reflection across the line L . This means that $P' = F_L(P)$ if and only if $\overline{PP'} \perp L$ and the distance from P to L is the same as the distance from P' to L .

Given symmetries A, B , we write AB to denote the composition $A \circ B$. For example, for the symmetries of the equilateral triangle, with angles in degrees, and with $L = \overline{OP}$ for some vertex P , we have $R_{240}R_{120} = R_0$ and $F_L R_{120} = R_{-120} F_L$.

Definition 2.1.5.

The **dihedral group**, denoted D_n is the set of rotation and reflection symmetries of the regular n -gon together with the binary operation of function composition.

Checkpoint 2.1.6.

Let X be the square centered at the origin in the x, y -plane with vertices at $(\pm 1, \pm 1)$. The square X has lines of symmetry H, V, D, D' (horizontal, vertical, diagonal, and another diagonal) where H, V denote the x, y axes, respectively, and D, D' denote the lines $y = -x, y = x$, respectively. See **Figure 2.1.7**.

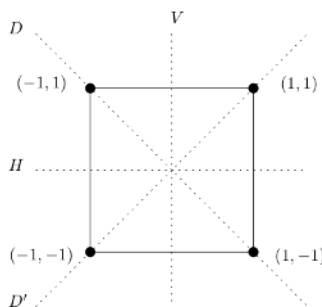


Figure 2.1.7. Lines of symmetry for the square.

The symmetries of the square X are

$$D_4 = \{R_0, R_{1/4}, R_{1/2}, R_{3/4}, F_H, F_V, F_D, F_{D'}\}$$

where the rotation angles units are revolutions. Find the following.

1. $R_{1/4}R_{1/2}$
2. $R_{1/4}F_H$

3. $F_H R_{1/4}$
4. $F_H F_D$
5. $F_D F_H$
6. $(F_D R_{1/2})^2 = F_D R_{1/2} F_D R_{1/2}$
7. $(F_D R_{1/2})^3$

Answer

1. $R_{3/4}$
2. $F_{D'}$
3. F_D
4. $R_{1/4}$
5. $R_{3/4}$
6. R_0
7. $F_{D'}$

The norm 1 complex numbers

Definition 2.1.8.

The **circle group**, denoted S^1 , is the set

$$S^1 = \{z \in \mathbb{C}: |z| = 1\}$$

of norm 1 complex numbers together with the binary operation $S^1 \times S^1 \rightarrow S^1$ given by complex multiplication, that is, $(z, w) \rightarrow zw$.

Checkpoint 2.1.9.

Show that if z, w are elements of S^1 , then their product zw is also in S^1 .

The n -th roots of unity

Let $n \geq 1$ be an integer. The set

$$C_n = \{z \in \mathbb{C}: z^n = 1\}$$

is called the set of (**complex**) **n -th roots of unity**.

Checkpoint 2.1.10.

1. Let $\omega = e^{i2\pi/n}$. Show that ω^k is in C_n for all integers k .
2. Show that, if z is an element of C_n , then $z = \omega^k$ for some integer k .
3. Show that the set C_n consists of precisely the n elements

$$\{\omega^0, \omega^1, \omega^2, \dots, \omega^{n-1}\}.$$

Definition 2.1.11.

The set $C_n = \{\omega^0, \omega^1, \omega^2, \dots, \omega^{n-1}\}$, together with the operation of complex multiplication, is called the **group of n -th roots of unity**.

Integers

Definition 2.1.12.

The set $\mathbb{Z}$ of integers, together with the operation of addition, is called the **group of integers**. Similarly, the set $\mathbb{Z}_n$ of integers modulo n (where n is some integer $n \geq 1$), together with the operation of addition modulo n , is called the **group of integers mod n** .

Invertible matrices

Let $n \geq 1$ be an integer. We write $GL(n, \mathbb{R})$ to denote the set of $n \times n$ invertible matrices with real entries. We write $GL(n, \mathbb{C})$ to denote the set of $n \times n$ invertible matrices with complex entries.

Definition 2.1.13.

The set $GL(n, \mathbb{R})$ (respectively, $GL(n, \mathbb{C})$), together with the binary operation of matrix multiplication, is called the **group of $n \times n$ real (respectively, complex) invertible matrices**, or also the **general linear group**.

Nonzero elements in a field

Let $\mathbb{F}$ be a field, such as the rational numbers $\mathbb{Q}$, the real numbers $\mathbb{R}$, or the complex numbers $\mathbb{C}$. We write $\mathbb{F}^*$ to denote the set of nonzero elements in $\mathbb{F}$.

Definition 2.1.14.

Let $\mathbb{F}$ be a field. The set $\mathbb{F}^*$, together with the binary operation of multiplication, is called the **group of nonzero elements** in the field $\mathbb{F}$.

Unit quaternions

Definition 2.1.15.

The set $U(\mathbb{H})$ of quaternions of norm 1 (defined in Subsection 1.2.4), together with the binary operation of quaternion multiplication, is called the **group of unit quaternions**.

Exercises

Exercise 1

Matrices for the dihedral group D_4 . Let H denote the x -axis in the x, y -plane. The map $F_H: \mathbb{R}^2 \rightarrow \mathbb{R}^2$ is a linear map whose matrix is $\begin{bmatrix} 1 & 0 \\ 0 & -1 \end{bmatrix}$. The map $R_{1/4}: \mathbb{R}^2 \rightarrow \mathbb{R}^2$ is a linear map whose matrix is $\begin{bmatrix} 0 & -1 \\ 1 & 0 \end{bmatrix}$. Find the matrices for the remaining elements of the dihedral group D_4 as specified in **Checkpoint 2.1.6**.

Exercise 2

Complex number operations for the dihedral group D_4 . Let H denote the real line $\mathbb{R}$ in the complex plane $\mathbb{C}$. The map $F_H: \mathbb{C} \rightarrow \mathbb{C}$ is complex conjugation $z \rightarrow z^*$. The map $R_{1/4}: \mathbb{C} \rightarrow \mathbb{C}$ is the map $z \rightarrow e^{i\pi/2}z = iz$. Find the maps $\mathbb{C} \rightarrow \mathbb{C}$ for the remaining elements of the dihedral group D_4 as specified in **Checkpoint 2.1.6**.

Exercise 3

Recall that a binary operation $(x, y) \rightarrow x * y$ is *commutative* if $x * y = y * x$ for all possible values of x, y .

1. Which of the group operations in the examples in this section are commutative? Which are not?
2. Show that S_n is *not* commutative for $n > 2$.

? Exercise 4

One of the properties of a group is the existence of an *identity* element. This is a group element e with the property that $eg = ge = g$ for every g in G . Find an identity element for each of the groups in the examples in this section.

? Exercise 5

One of the properties of a group is the existence of an *inverse* element for every element in the group. This means that for every g in a group G , there is an element h with the property that $gh = hg = e$, where e is the identity element of the group. Find inverses for the following list of group elements.

1. $[4, 2, 1, 3]$ in S_4
2. R_{120} in D_6 (where 120 is in degrees)
3. $\frac{1}{\sqrt{2}}(-1 + i)$ in S^1
4. 7 in $\mathbb{Z}$
5. 7 in $\mathbb{Z}_9$
6. $\begin{bmatrix} 1 & 2 \\ 2 & 1 \end{bmatrix}$ in $GL(2, \mathbb{R})$
7. $r = a + bi + cj + dk$ in $U(\mathbb{H})$

This page titled [2.1: Examples of groups](#) is shared under a [CC BY-NC-SA 4.0](#) license and was authored, remixed, and/or curated by [David W. Lyons](#) via [source content](#) that was edited to the style and standards of the LibreTexts platform.

2.2: Definition of a group

We will use the notation $\ast: S \times S \rightarrow S$ to denote a binary operation on a set S that sends the pair (x, y) to $x \ast y$. Recall that a binary operation $\ast$ is *associative* means that $x \ast (y \ast z) = (x \ast y) \ast z$ for all $x, y, z \in S$.

Definition 2.2.1. Group.

A **group** is a set G , together with a binary operation $\ast: G \times G \rightarrow G$ with the following properties.

- The operation $\ast$ is associative.
- There exists an element e in G , called an **identity** element, such that $e \ast g = g \ast e = g$ for all $g \in G$.
- For every $g \in G$, there exists an element $h \in G$, called an **inverse** element for g , such that $g \ast h = h \ast g = e$.

Proposition 2.2.2. Immediate consequences of the definition of group.

Let G be a group. The element e in the second property of **Definition 2.2.1** is unique. Given $g \in G$, the element h in the third property of **Definition 2.2.1** is unique.

Proof.

See **Exercise 2.2.2.1** and **Exercise 2.2.2.2**.

Definition 2.2.3. Multiplicative notation.

Let G be a group. By **Proposition 2.2.2**, we may speak of an identity element as **the** identity element for G . Given $g \in G$, we may refer to an inverse element for g as **the** inverse of g , and we write g^{-1} to denote this element. In practice, we often omit the operator $\ast$, and simply write gh to denote $g \ast h$. We adopt the convention that g^0 is the identity element. For $k \geq 1$, we write g^k to denote $\underbrace{g \ast g \ast \cdots \ast g}_{k \text{ factors}}$ and we write g^{-k} to denote $(g^k)^{-1}$. This set of notational conventions is called **multiplicative notation**.

Definition 2.2.4. Abelian group, additive notation.

In general, group operations are not commutative.¹ A group with a commutative operation is called **Abelian**.

For some Abelian groups, such as the group of integers, the group operation is called **addition**, and we write $a + b$ instead of using the multiplicative notation $a \ast b$. We write 0 to denote the identity element, we write $-a$ to denote the inverse of a , and we write ka to denote $\underbrace{a + a + \cdots + a}_{k \text{ summands}}$ for positive integers k . This set of notational conventions is called **additive notation**.

Definition 2.2.5. Order of a group.

The number of elements in a finite group is called the **order** of the group. A group with infinitely many elements is said to be of **infinite order**. We write $|G|$ to denote the order of the group G .

Definition 2.2.6. The trivial group.

A group with a single element (which is necessarily the identity element) is called a **trivial group**. In multiplicative notation, one might write $\{1\}$, and in additive notation, one might write $\{0\}$, to denote a trivial group.

Exercises

? Exercise 1

Uniqueness of the identity element.

Let G be a group. Suppose that e, e' both satisfy the second property of the **Definition 2.2.1**, that is, suppose $e * x = x * e = e' * x = x * e' = x$ for all $x \in G$. Show that $e = e'$.

? Exercise 2

Uniqueness of inverse elements.

Let G be a group with identity element e . Let $g \in G$ and suppose that $g * h = h * g = g * h' = h' * g = e$. Show that $h = h'$.

? Exercise 3

The cancellation law.

Suppose that $gx = hx$ for some elements g, h, x in a group G . Show that $g = h$. [Note that the same proof, mutatis mutandis, shows that if $xg = xh$, then $g = h$.

? Exercise 4

4. The "socks and shoes" property.

Let g, h be elements of a group G . Show that $(gh)^{-1} = h^{-1}g^{-1}$.

? Exercise 5

5. Product Groups.

Given two groups G, H with group operations $*_G, *_H$, the Cartesian product $G \times H$ is a group with the operation $*_{G \times H}$ given by

$$(g, h) *_{G \times H} (g', h') = (g *_G g', h *_H h').$$

Show that this operation satisfies the definition of a group.

? Exercise 6

6. Cyclic groups.

A group G is called *cyclic* if there exists an element g in G , called a **generator**, such that the sequence

$$(g^k)_{k \in \mathbb{Z}} = (\dots, g^{-3}, g^{-2}, g^{-1}, g^0, g^1, g^2, g^3, \dots)$$

contains all of the elements in G .

1. The group of integers is cyclic. Find all of the generators.
2. The group $\mathbb{Z}_8$ is cyclic. Find all of the generators.
3. The group $\mathbb{Z}_2 \times \mathbb{Z}_3$ is cyclic. Find all of the generators.
4. Show that the group $\mathbb{Z}_2 \times \mathbb{Z}_2$ is *not* cyclic.
5. Let m, n be positive integers. Show that the group $\mathbb{Z}_m \times \mathbb{Z}_n$ is cyclic if and only if m, n are relatively prime, that is, if the greatest common divisor of m, n is 1.

Hint

For the last part, observe that $(a, b) \in \mathbb{Z}_m \times \mathbb{Z}_n$ is a generator if and only if every entry in the sequence

$$(a, b), (2a, 2b), (3a, 3b), \dots, (mna, mnb)$$

is distinct (say why!). Let L be the least common multiple of n, m . If m, n are relatively prime, then $L = mn$, and if m, n are not relatively prime, then $L < mn$ (say why!). Use this observation to prove the statement in the exercise.

? Exercise 7

Cyclic permutations.

Let n be a positive integer and k be an integer in the range $1 \leq k \leq n$. A permutation $\pi \in S_n$ (see **Definition 2.1.1**) is called a **k -cycle** if there is a k -element set $A = \{a_1, a_2, \dots, a_k\} \subseteq \{1, 2, \dots, n\}$ such that $\pi(a_i) = a_{i+1}$ for $1 \leq i \leq k-1$ and $\pi(a_k) = a_1$, and $\pi(j) = j$ for $j \notin A$. We use **cycle notation** $(a_1 a_2 \dots a_k)$ to denote the k -cycle that acts as

$$a_1 \rightarrow a_2 \rightarrow a_3 \rightarrow \dots \rightarrow a_k \rightarrow a_1$$

on the distinct positive integers $a_1, a_2, \dots, a_k$. For example, the element $\pi = [1, 4, 2, 3] = (2, 4, 3)$ is a 3-cycle in S_4 because π acts on the set $A = \{2, 3, 4\}$ by

$$2 \rightarrow 4 \rightarrow 3 \rightarrow 2$$

and π acts on $A^c = \{1\}$ as the identity. Note cycle notation is not unique. For example, we have $(2, 4, 3) = (4, 3, 2) = (3, 2, 4)$ in S_4 . Cycles of any length (any positive integer) are called **cyclic** permutations. A 2-cycle is called a **transposition**.

1. Find all of the cyclic permutations in S_3 . Find their inverses.
2. Find all of the cyclic permutations in S_4 .

? Exercise 8

Cycles $(a_1 a_2 \dots a_k)$ and $(b_1 b_2 \dots b_\ell)$ are called **disjoint** if the sets $\{a_1, a_2, \dots, a_k\}$ and $\{b_1, b_2, \dots, b_\ell\}$ are disjoint, that is, if $a_i \neq b_j$ for all i, j . Show that every permutation in S_n is a product of disjoint cycles.

? Exercise 9

Show that every permutation in S_n can be written as a product of transpositions.

? Exercise 10

Parity of a permutation.

1. Suppose that the identity permutation e in S_n is written as a product of transpositions

$$e = \tau_1 \tau_2 \dots \tau_r.$$

Show that r is even.

2. Suppose that σ in S_n is written in two ways as a product of transpositions.

$$\sigma = (a_1 b_1)(a_2 b_2) \dots (a_s b_s) = (c_1 d_1)(c_2 d_2) \dots (c_t d_t)$$

Show that s, t are either both even or both odd. The common evenness or oddness of s, t is called the **parity** of the permutation σ .

3. Show that the parity of a k -cycle is even if k is odd, and the parity of a k -cycle is odd if k is even.

Hint

- a. Consider the two rightmost transpositions $\tau_{r-1} \tau_r$. They have one of the following forms, where a, b, c, d are distinct.

$$(ab)(ab), (ac)(ab), (bc)(ab), (cd)(ab)$$

The first allows you to reduce the transposition count by two by cancelling. The remaining three can be rewritten.

$$(ab)(bc), (ac)(cb), (ab)(cd)$$

Notice that the index of the rightmost transposition in which the symbol a occurs has been reduced by 1 (from r to $r - 1$). Finish this reasoning with an inductive argument.

? Exercise 11

Cayley tables.

The **Cayley table** for a finite group G is a two-dimensional array with rows and columns labeled by the elements of the group, and with entry gh in position with row label g and column label h . Partial Cayley tables for S_3 (Figure 2.2.7) and D_4 (Figure 2.2.8) are given below.

	e	(23)	(13)	(12)	(123)	(132)
e				(12)		
(23)						
(13)		(132)				
(12)					(23)	
(123)						
(132)						

Figure 2.2.7. (Partial) Cayley table for S_3 . The symbol e denotes the identity permutation.

	F_V	F_H	F_D	$F_{D'}$	$R_{1/4}$	$R_{1/2}$	$R_{3/4}$	R_0
F_V		$R_{1/2}$						
F_H				F_D				
F_D						$F_{D'}$		
$F_{D'}$								
$R_{1/4}$								
$R_{1/2}$								
$R_{3/4}$								
R_0								

Figure 2.2.8. (Partial) Cayley table for D_4 . (See Checkpoint 2.1.6 for notation for the elements of D_4 .)

1. Fill in the remaining entries in the Cayley tables for S_3 and D_4 .
2. Prove that the Cayley table for any group is a **Latin square**. This means that every element of the group appears exactly once in each row and in each column.

Answer 1

	e	(23)	(13)	(12)	(123)	(132)
e	e	(23)	(13)	(12)	(123)	(132)
(23)	(23)	e	(123)	(132)	(13)	(12)
(13)	(13)	(132)	e	(123)	(12)	(23)
(12)	(12)	(123)	(132)	e	(23)	(13)
(123)	(123)	(12)	(23)	(13)	(132)	e
(132)	(132)	(13)	(12)	(23)	e	(123)

Answer 2

	F_V	F_H	F_D	$F_{D'}$	$R_{1/4}$	$R_{1/2}$	$R_{3/4}$	R_0
F_V	R_0	$R_{1/2}$	$R_{3/4}$	$R_{1/4}$	$F_{D'}$	F_H	F_D	F_V
F_H	$R_{1/2}$	R_0	$R_{1/4}$	$R_{3/4}$	F_D	F_V	$F_{D'}$	F_H
F_D	$R_{1/4}$	$R_{3/4}$	R_0	$R_{1/2}$	F_V	$F_{D'}$	F_H	F_D
$F_{D'}$	$R_{3/4}$	$R_{1/4}$	$R_{1/2}$	R_0	F_H	F_D	F_V	$F_{D'}$
$R_{1/4}$	F_D	$F_{D'}$	F_H	F_V	$R_{1/2}$	$R_{3/4}$	R_0	$R_{1/4}$
$R_{1/2}$	F_H	F_V	$F_{D'}$	F_D	$R_{3/4}$	R_0	$R_{1/4}$	$R_{1/2}$
$R_{3/4}$	$F_{D'}$	F_D	F_V	F_H	R_0	$R_{1/4}$	$R_{1/2}$	$R_{3/4}$
R_0	F_V	F_H	F_D	$F_{D'}$	$R_{1/4}$	$R_{1/2}$	$R_{3/4}$	R_0

This page titled [2.2: Definition of a group](#) is shared under a [CC BY-NC-SA 4.0](#) license and was authored, remixed, and/or curated by [David W. Lyons](#) via [source content](#) that was edited to the style and standards of the LibreTexts platform.

2.3: Subgroups and Cosets

Definition 2.3.1. Subgroups and cosets.

A subset H of a group G is called a **subgroup** of G if H itself is a group under the group operation of G restricted to H . We write $H \leq G$ to indicate that H is a subgroup of G . A **(left) coset** of a subgroup H of G is a set of the form

$$gH := \{gh : h \in H\}.$$

The set of all cosets of H is denoted G/H .

$$G/H := \{gH : g \in G\}$$

Checkpoint 2.3.2.

Consider D_4 as described in Checkpoint 2.1.6.

$$D_4 = \{R_0, R_{1/4}, R_{1/2}, R_{3/4}, F_H, F_V, F_D, F_{D'}\}$$

1. Is the subset $\{R_0, R_{1/4}, R_{1/2}, R_{3/4}\}$ of rotations a subgroup of D_4 ? Why or why not?
2. Is the subset $\{F_H, F_V, F_D, F_{D'}\}$ of reflections a subgroup of D_4 ? Why or why not?

Answer

Yes. The composition of any two rotations is a rotation, and every rotation has an inverse that is also a rotation. No. Just observe that $F_H^2 = R_0$ is not a reflection. The group operation on D_4 does not restrict properly to the subset of reflections.

Checkpoint 2.3.3.

Find G/H for $G = S_3$, $H = \{e, (12)\}$.

Answer

$$\begin{aligned} G/H &= \{eH, (12)H, (13)H, (23)H, (123)H, (132)H\} \\ &= \{\{e, (12)\}, \{(12), e\}, \{(13), (123)\}, \{(23), (132)\}, \{(13), (123)\}, \{(132), (23)\}\} \\ &= \{H, \{(13), (123)\}, \{(23), (132)\}\} \end{aligned}$$

Proposition 2.3.4. Subgroup tests.

Let H be a subset of a group G . The following are equivalent.

1. H is a subgroup of G
2. **(2-step subgroup test)** H is nonempty, ab is in H for every a, b in H (H is closed under the group operation), and a^{-1} is in H for every a in H (H is closed under group inversion)
3. **(1-step subgroup test)** H is nonempty and ab^{-1} is in H for every a, b in H

Proof.

See Exercise 2.3.2.1.

Proposition 2.3.5. Subgroup generated by a set of elements.

Let S be a nonempty subset of a group G , and let $S^{-1}S^{-1}$ denote the set $S^{-1} = \{s^{-1} : s \in S\}$ of inverses of elements in S . We write $\langle S \rangle$ to denote the set of all elements of G of the form

$$s_1 s_2 \cdots s_k$$

where k is a positive integer and each s_i is in $S \cup S^{-1}$ for $1 \leq i \leq k$. The set $\langle S \rangle$ is a subgroup of G , called the **subgroup generated by the set S** , and the elements of S are called the **generators** of $\langle S \rangle$.

Comment on notational convention: If $S = \{s_1, s_2, \dots, s_k\}$ is finite, we write $\langle s_1, s_2, \dots, s_k \rangle$ for $\langle S \rangle$, instead of the more cumbersome $\langle \{s_1, s_2, \dots, s_k\} \rangle$.

 Observation 2.3.6.

If G is a cyclic group with generator g , then $G = \langle g \rangle$.

Checkpoint 2.3.7.

Show that $\langle S \rangle$ is indeed a subgroup of G . How would this fail if S were empty?

Checkpoint 2.3.8.

1. Find $\langle F_H, F_V \rangle \subseteq D_4$.
2. Find $\langle 6, 8 \rangle \subseteq \mathbb{Z}$.

Answer

1. $\langle F_H, F_V \rangle = \{R_0, R_{1/2}, F_H, F_V\}$
2. $\langle 6, 8 \rangle = \langle 2 \rangle = 2\mathbb{Z}$

 Proposition 2.3.9. Cosets as equivalence classes.

Let G be a group and let H be a subgroup of G . Let $\sim_H$ be the relation on G defined by $x \sim_H y$ if and only if $x^{-1}y \in H$. The relation $\sim_H$ is an equivalence relation on G , and the equivalence classes are the cosets of H , that is, we have $G/\sim_H = G/H$.

Proof.

See **Exercise 2.3.2.7**

 Corollary 2.3.10. Cosets as a partition.

Let G be a group and let H be a subgroup of G . The set G/H of cosets of H form a partition of G .

Exercises

 Exercise 1.

Prove **Proposition 2.3.4**.

 Exercise 2.

Find all the subgroups of S_3 .

Answer

In the "list of values" permutation notation of **Checkpoint 2.1.2**, the subgroups of S_3 are $\{[1, 2, 3]\}$, $\{[1, 2, 3], [2, 1, 3]\}$, $\{[1, 2, 3], [1, 3, 2]\}$, $\{[1, 2, 3], [3, 2, 1]\}$, and S_3 . In cycle notation, the subgroups of S_3 (in the same order) are $\{e\}$, $\{e, (12)\}$, $\{e, (23)\}$, $\{e, (13)\}$, $\{e, (123), (132)\}$, S_3 .

 Exercise 3.

Find all the cosets of the subgroup $\{R_0, R_{1/2}\}$ of D_4 .

? Exercise 4.

Subgroups of $\mathbb{Z}$ and $\mathbb{Z}_n$.

1. Let H be a subgroup of $\mathbb{Z}$. Show that either $H = \{0\}$ or $H = \langle d \rangle$, where d is the smallest positive element in H .
2. Let H be a subgroup of $\mathbb{Z}_n$. Show that either $H = \{0\}$ or $H = \langle d \rangle$, where d is the smallest positive element in H .
3. Let $n_1, n_2, \dots, n_r$ be positive integers. Show that

$$\langle n_1, n_2, \dots, n_r \rangle = \langle \gcd(n_1, n_2, \dots, n_r) \rangle$$

Consequence of this exercise: The greatest common divisor $\gcd(a, b)$ of integers a, b is the smallest positive integer of the form $sa + tb$ over all integers s, t . Two integers a, b are relatively prime if and only if there exist integers s, t such that $sa + tb = 1$.

? Exercise 5.

Centralizers, Center of a group.

The **centralizer** of an element a in a group G , denoted $C(a)$, is the set

$$C(a) = \{g \in G : ag = ga\}.$$

The **center** of a group G , denoted $Z(G)$, is the set

$$Z(G) = \{g \in G : ag = ga \quad \forall a \in G\}.$$

1. Show that the centralizer $C(a)$ of any element a in a group G is a subgroup of G .
2. Show that the center $Z(G)$ of a group G is a subgroup of G .

? Exercise 6.

The order of a group element.

Let g be an element of a group G . The **order** of g , denoted $|g|$, is the smallest positive integer n such that $g^n = e$, if such an integer exists. If there is no positive integer n such that $g^n = e$, then g is said to have *infinite* order. Show that, if the order of g is finite, say $|g| = n$, then

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

Consequence of this exercise: If G is cyclic with generator g , then $|G| = |g|$.

? Exercise 7.

Cosets of a subgroup partition the group, Lagrange's Theorem.

1. Prove **Proposition 2.3.9**.
2. Now suppose that a group G is finite. Show that all of the cosets of a subgroup H have the same size.
3. Prove the following.

Lagrange's Theorem.

If G is a finite group and H is a subgroup, then the order of H divides the order of G .

Hint

For part (b), let aH, bH be cosets. Show that the function $aH \rightarrow bH$ given by $x \rightarrow ba^{-1}x$ is a bijection.

? Exercise 8.

Consequences of Lagrange's Theorem.

1. Show that the order of any element of a finite group divides the order of the group.
2. Let G be a finite group, and let $g \in G$. Show that $g^{|G|} = e$.
3. Show that a group of prime order is cyclic.

This page titled [2.3: Subgroups and Cosets](#) is shared under a [CC BY-NC-SA 4.0](#) license and was authored, remixed, and/or curated by [David W. Lyons](#) via [source content](#) that was edited to the style and standards of the LibreTexts platform.

2.4: Group Homomorphisms

Definition 2.4.1. Group homomorphism.

Let G, H be groups.

A map $\phi: G \rightarrow H$ is called a **homomorphism** if

$$\phi(xy) = \phi(x)\phi(y)$$

for all x, y in G . A homomorphism that is both injective (one-to-one) and surjective (onto) is called an **isomorphism** of groups.

If $\phi: G \rightarrow H$ is an isomorphism, we say that G is **isomorphic** to H , and we write $G \approx H$.

Checkpoint 2.4.2.

Show that each of the following are homomorphisms.

- $GL(n, \mathbb{R}) \rightarrow \mathbb{R}^*$ given by $M \rightarrow \det M$
- $\mathbb{Z} \rightarrow \mathbb{Z}$ given by $x \rightarrow mx$, some fixed $m \in \mathbb{Z}$
- $G \rightarrow G$, G any group, given by $x \rightarrow axa^{-1}$, some fixed $a \in G$
- $\mathbb{C}^* \rightarrow \mathbb{C}^*$ given by $z \rightarrow z^2$

Show that each of the following are not homomorphisms. In each case, demonstrate what fails.

- $\mathbb{Z} \rightarrow \mathbb{Z}$ given by $x \rightarrow x + 3$
- $\mathbb{Z} \rightarrow \mathbb{Z}$ given by $x \rightarrow x^2$
- $D_4 \rightarrow D_4$ given by $g \rightarrow g^2$

Definition 2.4.3. Kernel of a group homomorphism.

Let $\phi: G \rightarrow H$ be a group homomorphism, and let e_H be the identity element for H . We write $\ker(\phi)$ to denote the set

$$\ker(\phi) := \phi^{-1}(e_H) = \{g \in G: \phi(g) = e_H\},$$

called the **kernel** of ϕ .

Checkpoint 2.4.4.

Find the kernel of each of the following homomorphisms.

- $\mathbb{C}^* \rightarrow \mathbb{C}^*$ given by $z \rightarrow z^n$
- $\mathbb{Z}_8 \rightarrow \mathbb{Z}_8$ given by $x \rightarrow 6x \pmod{8}$
- $G \rightarrow G$, G any group, given by $x \rightarrow axa^{-1}$, some fixed $a \in G$

Answer

1. C_n
2. $\langle 4 \rangle = \{0, 4\}$
3. $\{x \in G: axa^{-1} = e\} = C(a)$

Proposition 2.4.5. Basic properties of homomorphisms.

Let $\phi: G \rightarrow H$ be a homomorphism of groups. Let e_G, e_H denote the identity elements of G, H , respectively. We have the following.

1. (identity goes to identity) $\phi(e_G) = e_H$
2. (inverses go to inverses) $\phi(g^{-1}) = (\phi(g))^{-1}$ for all $g \in G$
3. $\ker(\phi)$ is a subgroup of G
4. $\phi(G)$ is a subgroup of H

5. (preimage sets are cosets of the kernel) $\phi(x) = y$ if and only if $\phi^{-1}(y) = x \ker(\phi)$
6. $\phi(a) = \phi(b)$ if and only if $a \ker(\phi) = b \ker(\phi)$
7. ϕ is one-to-one if and only if $\ker(\phi) = \{e_G\}$

Proof.

See **Exercise Group 2.4.2.1–3.**

 **Proposition 2.4.6.** G/K is a group if and only if K is a kernel.

Let K be a subgroup of a group G . The set G/K of cosets of K forms a group, called a **quotient group** (or **factor group**), under the operation

$$(xK)(yK) = xyK \quad (2.4.1)$$

if and only if K is the kernel of a homomorphism $G \rightarrow G'$ for some group G' .

Proof.

See **Exercise 2.4.2.5.**

Here is a corollary of **Proposition 2.4.6** and its proof.

 **Corollary 2.4.7. (First Isomorphism Theorem).**

Let $\phi: G \rightarrow H$ be a homomorphism of groups. Then $G/\ker(\phi)$ is isomorphic to $\phi(G)$ via the map $g\ker(\phi) \rightarrow \phi(g)$.

 **Definition 2.4.8. Normal subgroup.**

A subgroup H of a group G is called **normal** if $ghg^{-1} \in H$ for every $g \in G, h \in H$. We write $H \trianglelefteq G$ to indicate that H is a normal subgroup of G .

 **Proposition 2.4.9. Characterization of normal subgroups.**

Let K be a subgroup of a group G . The following are equivalent.

1. K is the kernel of some group homomorphism $\phi: G \rightarrow H$
2. G/K is a group with multiplication given by Equation (2.4.1)
3. K is a normal subgroup of G

Exercises

? Exercise 1

Basic properties of homomorphism. Prove **Proposition 2.4.5.**

Prove Properties 1 and 2.

Prove Properties 3 and 4.

Prove Properties 5, 6, and 7.

Hint

Use **Fact 1.4.3.**

? Exercise 2

Show that the inverse of an isomorphism is an isomorphism.

? Exercise 3

Prove **Proposition 2.4.6**.

? Exercise 4

Let n, a be relatively prime positive integers. Show that the map $\mathbb{Z}_n \rightarrow \mathbb{Z}_n$ given by $x \rightarrow ax$ is an isomorphism.

Hint

Use the fact that $\gcd(m, n)$ is the least positive integer of the form $sm + tn$ over all integers s, t (see **Exercise 2.3.2.4**). Use this to solve $ax = 1 \pmod{n}$ when a, n are relatively prime.

? Exercise 5

Another construction of $\mathbb{Z}_n$.

Let $n \geq 1$ be an integer and let $\omega = e^{i2\pi/n}$. Let $\phi: \mathbb{Z} \rightarrow S^1$ be given by $k \rightarrow \omega^k$.

1. Show that the image of ϕ is the group C_n of n th roots of unity.
2. Show that ϕ is a homomorphism, and that the kernel of ϕ is the set $n\mathbb{Z} = \{nk: k \in \mathbb{Z}\}$.
3. Conclude that $\mathbb{Z}/(n\mathbb{Z})$ is isomorphic to the group of n -th roots of unity.

? Exercise 6: Isomorphic images of generators are generators

Let S be a subset of a group G . Let $\phi: G \rightarrow H$ be an isomorphism of groups, and let $\phi(S) = \{\phi(s): s \in S\}$. Show that $\phi(\langle S \rangle) = \langle \phi(S) \rangle$.

? Exercise 7: Conjugation

Let G be a group, let a be an element of G , and let $C_a: G \rightarrow G$ be given by $C_a(g) = aga^{-1}$. The map C_a is called **conjugation** by the element a and the elements g, aga^{-1} are said to be **conjugate** to one another.

1. Show that C_a is an isomorphism of G with itself.
2. Show that "is conjugate to" is an equivalence relation. That is, consider the relation on G given by $x \sim y$ if $y = C_a(x)$ for some a . Show that this is an equivalence relation.

? Exercise 8: Isomorphism induces an equivalence relation

Prove that "is isomorphic to" is an equivalence relation on groups. That is, consider the relation $\approx$ on the set of all groups, given by $G \approx H$ if there exists a group isomorphism $\phi: G \rightarrow H$. Show that this is an equivalence relation.

Characterization of normal subgroups.

Prove **Proposition 2.4.9**. That **Item 1** is equivalent to **Item 2** is established by **Proposition 2.4.6**.

? Exercise 9

Show that **Item 1** implies **Item 3**.

? Exercise 10

Show that **Item 3** implies **Item 2**. The messy part of this proof is to show that multiplication of cosets is well-defined. This means you start by supposing that $xK = x'K$ and $yK = y'K$, then show that $xyK = x'y'K$.

? Exercise 11: Further characterizations of normal subgroups

Show that **Item 3** is equivalent to the following conditions.

1. $gKg^{-1} = K$ for all $g \in G$
2. $gK = Kg$ for all $g \in G$

? Exercise 12: Automorphisms

Let G be a group. An **automorphism** of G is an isomorphism from G to itself. The set of all automorphisms of G is denoted $\text{Aut}(G)$.

1. Show that $\text{Aut}(G)$ is a group under the operation of function composition.
2. Show that

$$\text{Inn}(G) := \{C_g : g \in G\}$$

is a subgroup of $\text{Aut}(G)$. (The group $\text{Inn}(G)$ is called the group of **inner automorphisms** of G .)

3. Find an example of an automorphism of a group that is not an inner automorphism.

This page titled [2.4: Group Homomorphisms](#) is shared under a [CC BY-NC-SA 4.0](#) license and was authored, remixed, and/or curated by [David W. Lyons](#) via [source content](#) that was edited to the style and standards of the LibreTexts platform.

2.5: Group Actions

Definition 2.5.1. Group action, orbit, stabilizer.

Let G be a group and let X be a set. An **action** of the group G on the set X is a group homomorphism

$$\phi: G \rightarrow \text{Perm}(X).$$

We say that the group G **acts** on the set X , and we call X a G -**space**. For $g \in G$ and $x \in X$, we write gx to denote $(\phi(g))(x)$.¹ We write $\text{Orb}(x)$ to denote the set

$$\text{Orb}(x) = \{gx: g \in G\},$$

called the **orbit** of x , and we write $\text{Stab}(x)$ to denote the set

$$\text{Stab}(x) = \{g \in G: gx = x\},$$

called the **stabilizer** or **isotropy** subgroup² of x . A group action is **transitive** if there is only one orbit. A group action is **faithful** if the map $G \rightarrow \text{Perm}(X)$ has a trivial kernel.

Checkpoint 2.5.2.

Find the indicated orbits and stabilizers for each of the following group actions.

- D_4 acts on the square $X = \{(x, y) \in \mathbb{R}^2: -1 \leq x, y \leq 1\}$ by rotations and reflections. What is the orbit of $(1, 1)$? What is the orbit of $(1, 0)$? What is the stabilizer of $(1, 1)$? What is the stabilizer of $(1, 0)$?
- The circle group S^1 (see **Subsection 2.1.3**) acts on the two-sphere S^2 by rotation about the z -axis. Given an element $e^{i\alpha}$ in S^1 a point (θ, ϕ) in S^2 (in spherical coordinates), the action is given by

$$e^{i\alpha} \cdot (\theta, \phi) = (\theta, \phi + \alpha).$$

What is the orbit of $(\pi/4, \pi/6)$? What is the orbit of the north pole $(0, 0)$? What is the stabilizer of $(\pi/4, \pi/6)$? What is the stabilizer of the north pole?

- Any group G acts on itself by *conjugation*, that is, by $(\phi(g))(x) = gxg^{-1} = C_g(x)$ (see **Exercise 2.4.2.9**). Describe the orbit and stabilizer of a group element x .

Answer

- $\text{Orb}((1, 1)) = \{(1, 1), (1, -1), (-1, 1), (-1, -1)\}$, $\text{Orb}((1, 0)) = \{(1, 0), (-1, 0), (0, 1), (0, -1)\}$, $\text{Stab}((1, 1)) = \{R_0, F_D\}$, $\text{Stab}((1, 0)) = \{R_0, F_H\}$
- $\text{Orb}(\pi/4, \pi/6)$ is the horizontal circle on S^2 with "latitude" $\pi/4$, $\text{Orb}(0, 0) = \{(0, 0)\}$, $\text{Stab}(\pi/4, \pi/6) = \{1\}$, $\text{Stab}(0, 0) = S^1$
- $\text{Orb}(x) = \{gxg^{-1}: g \in G\}$, $\text{Stab}(x) = C(x)$ (the centralizer of x)

Checkpoint 2.5.3.

Show that the stabilizer of an element x in a G -space X is a subgroup of G .

Proposition 2.5.4: Orbits of a group action form a partition

Let group G act on set X . The collection of orbits is a partition of X . The corresponding equivalence relation $\sim_G$ on X is given by $x \sim_G y$ if and only if $y = gx$ for some $g \in G$. We write X/G to denote the set of orbits, which is the same as the set $X/\sim_G$ of equivalence classes.

$$X/G = \{\text{Orb}(x): x \in X\}$$

Checkpoint 2.5.5.

Describe X/G for each of the three group actions in **Checkpoint 2.5.2**.

Theorem 2.5.6: The Orbit-Stabilizer Theorem

Let G be a group acting on a set X , and let x be an element of X . There is a one-to-one correspondence

$$G/Stab(x) \leftrightarrow Orb(x)$$

given by

$$gStab(x) \leftrightarrow gx.$$

Proof.

See Exercise 2.5.3.5.

Exercises

? Exercise 1: Actions of a group on itself

Let G be a group. Here are two actions $G \rightarrow Perm(G)$ of G on itself. **Left multiplication** is given by

$$g \rightarrow L_g$$

where L_g is given by $L_g(h) = gh$. **Right inverse multiplication** is given by

$$g \rightarrow R_g$$

where R_g is given by $R_g(h) = hg^{-1}$. **Conjugation** is given by

$$g \rightarrow C_g$$

where C_g is given by $C_g(h) = ghg^{-1}$.

1. Show that, for $g \in G$, the maps L_g, R_g, C_g are elements of $Perm(G)$.
2. Show that each of these maps L, R, C is indeed a group action.
3. Show that the map L is injective, so that $G \approx L(G)$.

Consequence of this exercise: Every group is isomorphic to a subgroup of a permutation group.

? Exercise 2: Cosets, revisited

Let H be a subgroup of a group G , and consider the map

$$R: H \rightarrow Perm(G)$$

given by $h \rightarrow R_h$, where $R_h(g) = gh^{-1}$ (this is the restriction of right inverse multiplication action in Exercise 2.5.3.1 to H). Show that the orbits of this action of H on G are the same as the cosets of H . This shows that the two potentially different meanings of G/H (one is the set of cosets, the other is the set of orbits of the action of H on G via R), are in fact in agreement.

? Exercise 3: The natural action of a matrix group on a vector space

Let G be a group whose elements are $n \times n$ matrices with entries in a field $\mathbb{F}$ and with the group operation of matrix multiplication. The **natural action** $G \rightarrow Perm(X)$ of G on the vector space $X = \mathbb{F}^n$ is given by

$$g \rightarrow [v \rightarrow g \cdot v],$$

where the "dot" in the expression $g \cdot v$ is ordinary multiplication of a matrix times a column vector. Show that this is indeed a group action.

? Exercise 4

Prove **Proposition 2.5.4**.

? Exercise 5

Prove **Theorem 2.5.6**.

? Exercise 6: The projective linear group action on projective space

Let V be a vector space over a field $\mathbb{F}$ (in this course, the base field $\mathbb{F}$ is either the real numbers $\mathbb{R}$ or the complex numbers $\mathbb{C}$). The group $\mathbb{F}^*$ of nonzero elements in $\mathbb{F}$ acts on the set $V \setminus \{0\}$ of nonzero elements in V by scalar multiplication, that is, by the map $\alpha \rightarrow [v \rightarrow \alpha v]$. The set of orbits $(V \setminus \{0\})/\mathbb{F}^*$ is called the *projectivization* of V , or simply **projective space**, and is denoted $\mathbb{P}(V)$.

1. Let $\sim_{\text{proj}}$ denote the equivalence relation that defines the orbits $(V \setminus \{0\})/\mathbb{F}^*$. Verify that $\sim_{\text{proj}}$ is given by $x \sim_{\text{proj}} y$ if and only if $x = \alpha y$ for some $\alpha \in \mathbb{F}^*$.
2. Verify that the group $GL(V)$ (the group of invertible linear transformations of V) acts on $\mathbb{P}(V)$ by

$$g \cdot [v] = [g(v)] \quad (2.5.1)$$

for $g \in GL(V)$ and $v \in V \setminus \{0\}$.

3. Show that the kernel of the map $GL(V) \rightarrow \text{Perm}(\mathbb{P}(V))$ given by (2.5.1) is the subgroup $K = \{\alpha Id : \alpha \in \mathbb{F}^*\}$.
4. Conclude that the **projective linear group** $PGL(V) := GL(V)/K$ acts on $\mathbb{P}(V)$.
5. Show that $\mathbb{F}^*$ acts on $GL(V)$ by $\alpha \cdot T = \alpha T$, and that $PGL(V) \approx GL(V)/\mathbb{F}^*$.
6. Show that the map $\mathbb{P}(\mathbb{C}^2) \rightarrow S^2$ given by $[(\alpha, \beta)] \rightarrow s^{-1}(\alpha/\beta)$ if $\beta \neq 0$ and given by $[(\alpha, \beta)] \rightarrow (0, 0, 1)$ if $\beta = 0$ is well-defined and is a bijection.

This page titled [2.5: Group Actions](#) is shared under a [CC BY-NC-SA 4.0](#) license and was authored, remixed, and/or curated by [David W. Lyons](#) via [source content](#) that was edited to the style and standards of the LibreTexts platform.

2.6: Additional exercises

? Exercise 1

1. The group of units in $\mathbb{Z}_n$.

Let U_n denote the set of elements in $\mathbb{Z}_n$ that have multiplicative inverses, that is,

$$U_n = \{x \in \mathbb{Z}_n : \exists y, xy = 1 \pmod{n}\}.$$

1. Show that x is in U_n if and only if x is relatively prime to n .
2. Show that U_n with the binary operation of multiplication mod n is an Abelian group.
3. Show that U_n is isomorphic to $\text{Aut}(\mathbb{Z}_n)$ via $x \rightarrow [a \rightarrow ax]$.

Terminology: The group U_n is called the the group of (**multiplicative**) **units** in $\mathbb{Z}_n$. The function $n \rightarrow |U_n|$, important in number theory, is called the **Euler phi function**, written $\phi(n) = |U_n|$.

? Exercise 2

2. Fermat's Little Theorem.

For every integer x and every prime p , we have $x^p = x \pmod{p}$.

Hint

First, reduce $x \pmod{p}$, that is, write $x = qp + r$ with $0 \leq r \leq p - 1$. Now consider two cases. The case $r = 0$ is trivial. If $r \neq 0$, apply the fact $r^{|G|} = e$ (see [Exercise 2.3.2.8](#)) to the group $G = U_p$.

? Exercise 3

3. The alternating group.

1. Show that, for $n \geq 2$, half of the elements of S_n are even, and half are odd.
2. The set of even permutations in S_n is called the **alternating group**, denoted A_n . Show that A_n is indeed a subgroup of S_n .

? Exercise 4

4. The order of a permutation.

Let $\sigma \in S_n$ be written as a product of disjoint cycles. Show that the order σ is the least common multiple of the lengths of those disjoint cycles.

? Exercise 5

5. Semidirect product.

Let K, H be groups, and let $\phi: H \rightarrow \text{Aut}(K)$ be a homomorphism. The **semidirect product**, denoted $K \rtimes_{\phi} H$, or $K \rtimes H$ if ϕ is understood, is the set consisting of all pairs (k, h) with $k \in K, h \in H$ with the group multiplication operation $*$ given by

$$(k_1, h_1) * (k_2, h_2) = (k_1 \phi(h_1)(k_2), h_1 h_2).$$

Two examples demonstrate why this is a useful construction. The dihedral group D_n is (isomorphic to) the semidirect product $C_n \rtimes C_2$, where C_n is the cyclic group generated by the rotation $R_{1/n}$ (rotation by $1/n$ of a revolution) and C_2 is the two-element group generated by any reflection R_L in D_n . The map $\phi: C_2 \rightarrow \text{Aut}(C_n)$ is given by $R_L \rightarrow [R_{\theta} \rightarrow R_{-\theta}]$. The *Euclidean group* of congruence transformations of the plane is (isomorphic to) the group $\mathbb{R}^2 \rtimes O(2)$, where $(\mathbb{R}^2, +)$ is the additive group of 2×1 column vectors with real entries, and $O(2)$ is the group of 2×2 real orthogonal matrices. The map $\phi: O(2) \rightarrow \text{Aut}(\mathbb{R}^2)$ is given

by $g \rightarrow [v \rightarrow gv]$, that is to say, the natural action of $O(2)$ on $\mathbb{R}^2$. [The Euclidean group element (v, g) acts on the point $x \in \mathbb{R}^2$ by $x \rightarrow gx + v$.]

1. Do all the necessary details to show that $K \rtimes H$ is indeed a group.
2. (**Characterization of semidirect products**) Suppose that K, H are subgroups of a group G . Let $KH = \{kh: k \in K, h \in H\}$. Suppose that K is a normal subgroup of G , that $G = KH$, and that $K \cap H = \{e\}$. Show that $\phi: H \rightarrow \text{Aut}(K)$, given by $\phi(h)(k) = hkh^{-1}$, is a homomorphism. Show that $\psi: K \times_{\phi} H \rightarrow G$, given by $\psi(k, h) = kh$, is an isomorphism.
3. Show that $D_n \approx C_n \rtimes C_2$, as described above.
4. Show that the following requirement holds for the Euclidean group action. We have

$$[(v_1, g_1)(v_2, g_2)]x = (v_1, g_1)[(v_2, g_2)x],$$

for all $v_1, v_2, x \in \mathbb{R}^2$ and $g_1, g_2 \in O(2)$.

5. Suppose that $\phi: H \rightarrow \text{Aut}(K)$ is the trivial homomorphism (that is, $\phi(h)$ is the identity homomorphism on K , for all $h \in H$). Show that $K \times_{\phi} H \approx K \times H$ in this case.

? Exercise 6

6. Group action on functions on a G -space.

Suppose that a group G acts on a set X . Let $\mathcal{F}(X, Y)$ denote the set of functions

$$\mathcal{F}(X, Y) = \{f: X \rightarrow Y\}$$

from X to some set Y . Show that the formula

$$(g \cdot \alpha)(x) = \alpha(g^{-1} \cdot x)$$

defines an action of G on $\mathcal{F}(X, Y)$, where $g \in G$, $\alpha \in \mathcal{F}(X, Y)$, and $x \in X$.

This page titled [2.6: Additional exercises](#) is shared under a [CC BY-NC-SA 4.0](#) license and was authored, remixed, and/or curated by [David W. Lyons](#) via [source content](#) that was edited to the style and standards of the LibreTexts platform.

CHAPTER OVERVIEW

3: Geometries

[3.1: Geometries and Models](#)

[3.2: Möbius Geometry](#)

[3.3: Hyperbolic geometry](#)

[3.4: Elliptic geometry](#)

[3.5: Projective Geometry](#)

[3.6: Additional exercises](#)

This page titled [3: Geometries](#) is shared under a [CC BY-NC-SA 4.0](#) license and was authored, remixed, and/or curated by [David W. Lyons](#) via [source content](#) that was edited to the style and standards of the LibreTexts platform.

3.1: Geometries and Models

An integral part of the modern understanding of geometry is the concept of *congruence transformation*, or simply *symmetry*. The symmetries of a geometric space preserve inherent properties of figures, such as distance, angle, and area. In his 1872 work called the *Erlanger Programm*¹, Felix Klein unified the study of a wide variety of geometric spaces by overtly placing the group of congruence transformations as part of the structure of a geometry. The following is a version of Klein's definition of geometry.

Definition 3.1.1.

A **geometry** is a pair (X, G) , where X is a set, called the **(model) space**, and G is a group, called the group of **congruence transformations**, that acts on X . Subsets of X are called **figures**. Figures F, F' are called **congruent** if there is an element g in G such that $g(F) = F'$. We write $F \cong F'$ to denote that figures F, F' are congruent.

Note on terminology and notation: throughout this chapter on geometry, the term *transformation* will always mean a one-to-one and onto map of a space to itself. Given a geometry (X, G) with group action $\phi: G \rightarrow \text{Perm}(X)$, we will abuse notation and write $g: X \rightarrow X$ to denote the map $\phi(g): X \rightarrow X$ for an element g in G . It is common usage to say "the transformation g " to mean "the transformation $\phi(g)$ " of the space X .

Checkpoint 3.1.2.

Show that congruence is an equivalence relation on the set of figures in a geometry.

Examples of geometries

- **Planar Euclidean geometry.** The model space for planar Euclidean geometry is the plane $\mathbb{R}^2$. The group of congruence transformations consists of translations, rotations, reflections, and their compositions. Specifically, Euclidean congruences are functions of the form $v \rightarrow Rv + b$, where $v \in \mathbb{R}^2$, R is an element of the group of 2×2 orthogonal matrices, and $b \in \mathbb{R}^2$.
- **Spherical geometry.** The model space for spherical geometry is the sphere $S^2 = \{(x, y, z) \in \mathbb{R}^3: x^2 + y^2 + z^2 = 1\}$. The group of congruence transformations consists of rotations of the sphere and reflections across planes through the origin. Specifically, spherical congruences are functions of the form $v \rightarrow Rv$, where $v \in \mathbb{R}^3$, $|v| = 1$, and R is an element of the group of 3×3 orthogonal matrices.
- **Projective geometry.** The model space for a projective geometry is projective space $\mathbb{P}(V)$, where V is a vector space V (see Exercise 2.5.3.6 in the previous chapter). The group of congruence transformations is the projective linear group $PGL(V)$.

Planar geometries

Much of this chapter on geometry is devoted to a family of *planar* geometries whose model spaces are the extended complex plane $\hat{\mathbb{C}} = \mathbb{C} \cup \{\infty\}$ (described in section Section 1.3) and some of its subsets. One of the properties shared by the congruence transformations in all of these planar geometries is *conformality*, or angle preservation. To say that a transformation T is **conformal** means that if two curves C_1 and C_2 make an oriented angle θ at a point P of intersection, then the two image curves $T(C_1)$ and $T(C_2)$ also make the same oriented angle at the point $T(P)$ of intersection (the angle made by two curves is the angle made by their tangents at the point of intersection). See Figure 3.1.3. Exercise Group 3.1.4.2–5 examines the conformal properties of the four basic types of complex functions summarized in Table 3.1.4.

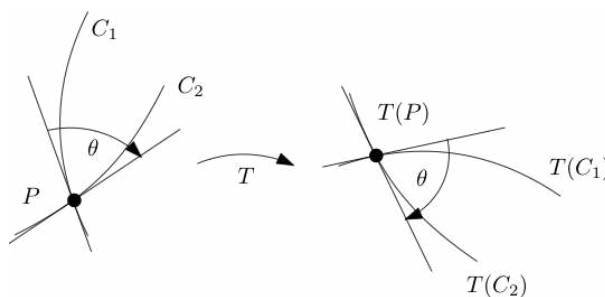


Figure 3.1.3. Conformal maps preserve oriented angles

Table 3.1.4. Basic planar geometric transformations

<i>homothety</i>	$z \rightarrow kz, k > 0$
<i>rotation</i>	$z \rightarrow e^{it}z, t \in \mathbb{R}$
<i>translation</i>	$z \rightarrow z + b, b \in \mathbb{C}$
<i>inversion</i>	$z \rightarrow \frac{1}{z}$

Subgeometries and equivalent geometries

Definition 3.1.5. Subgeometry.

We say that a geometry (X, G) is a **subgeometry** of a geometry (Y, H) if X is a subset of Y and G is a subgroup of H .

Definition 3.1.6. Equivalent geometries.

Geometries (X, G) and (Y, H) are **equivalent** if there is a bijective map $\mu: X \rightarrow Y$ such that every element of H has a conjugate transformation in G and every element of G has a conjugate transformation in H . In symbols:²

- for every $g \in G$, there is an $h \in H$ such that $\mu \circ g \circ \mu^{-1} = h$, and
- for every $h \in H$, there is a $g \in G$ such that $\mu^{-1} \circ h \circ \mu = g$.

Equivalent geometries are said to be **models** of the same geometry.

Note on terminology: the term "geometry" is used to refer to a specific model as in definition **Definition 3.1.1**, and also to refer to an equivalence class of geometries.³

Exercises

? Exercise 1: Warm up exercises with the three example geometries

1. Find the Euclidean congruence transformation that takes the triangle with vertices $(2, 0), (6, 0), (6, 3)$ to the triangle with vertices $(0, -1), (0, -5), (3, -1)$.
2. Find the spherical congruence that takes the three points $(0, 0, 1), (0, 0, -1), (1, 0, 0)$ to the three points $(1, 0, 0), (-1, 0, 0), (0, 1, 0)$ (in that order).
3. Find the projective transformation in $PGL(2, \mathbb{C})$ that takes the three points $[(1, 1)], [(0, 1)], [(1, 0)]$ in $\mathbb{P}(\mathbb{C}^2)$ to $[(a, 1)], [(b, 1)], [(c, 1)]$ (in that order).
4. Find formulas for the composition of two Euclidean transformations and the inverse of a Euclidean transformation.
5. Let $d(P, Q)$ denote the distance between points P, Q in Euclidean geometry, and let T be a Euclidean congruence transformation. Show that $d(T(P), T(Q)) = d(P, Q)$.

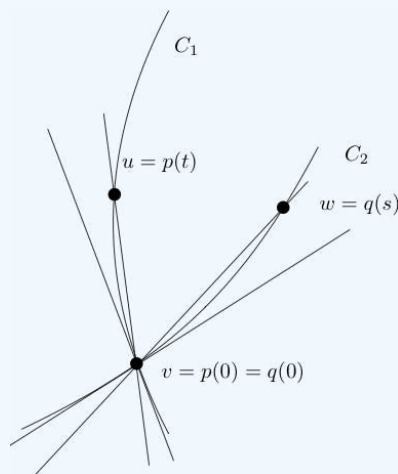


Figure 3.1.7. The angle between tangents to curves as a limit of secant approximations

? Exercise 2: Angles and Conformal Transformations

The complex plane comes with a built-in measure of oriented angle. If u is a positive real number, $v = 0$, and $w \neq 0$ is a complex number, the measure of the oriented angle $\angle uvw$ is $\arg w$. More generally, if u, v, w are three complex numbers with v distinct from u and w , the measure of the oriented angle $\angle uvw$ is

$$\arg \left(\frac{w - v}{u - v} \right). \quad (3.1.1)$$

2. Use the fact that rotations and translations are conformal to prove (3.1.1).

3. Use (3.1.1) to prove that homotheties are conformal.

4. Now suppose two curves C_1, C_2 intersect at v , let u be a point on C_1 and let w be a point on C_2 . If u and w are close to v , then $\angle uvw$ is a secant approximation of an angle made by the tangents to C_1, C_2 at v . See Figure 3.1.7. Now let $p(t), q(s)$ be parameterizations of C_1, C_2 , respectively, with $p(0) = q(0) = v$, and $p(t_1) = u, q(s_1) = w$ for some $t_1, s_1 > 0$. We can compute an angle made by the tangents to the curves by the following limit.

$$\lim_{s \rightarrow 0^+, t \rightarrow 0^+} \arg \left(\frac{q(s) - v}{p(t) - v} \right) \quad (3.1.2)$$

The value of limit (3.1.2) is sensitive to the direction of the curve parameterizations and the sided-ness of the limits $t \rightarrow 0^\pm$ or $s \rightarrow 0^\pm$. If the value of the limit (3.1.2) is θ for one set of choices for parameterizations and sided-ness, the limit for the other choices will be θ or $\theta \pm \pi$. For a given pair of parameterizations p, q , draw a sketch to illustrate the four possible cases $t \rightarrow 0^\pm, s \rightarrow 0^\pm$.

5. Use (3.1.1) and (3.1.2) to prove that inversion is conformal.

? Exercise 3: Equivalent Geometries

6. Show that the definition of equivalence of geometries actually defines an equivalence relation on geometries.

7. Let $\mathcal{E}_1$ denote the set of Euclidean congruence transformations given above in Subsection 3.1.1. Let $\mathcal{E}_2$ denote the set of complex functions that can be written as compositions of the following three types:

- $z \rightarrow e^{it}z$ for some $t \in \mathbb{R}$
- $z \rightarrow z + b$ for some $b \in \mathbb{C}$
- $z \rightarrow z^*$

Show that the geometries $(\mathbb{R}^2, \mathcal{E}_1)$ and $(\mathbb{C}, \mathcal{E}_2)$ are equivalent.

8. Suppose that $(X, \mathcal{G})$ and $(Y, \mathcal{H})$ are equivalent geometries. Is it necessarily the case that G and H are isomorphic groups? If yes, give a proof. If no, give a counterexample.

This page titled [3.1: Geometries and Models](#) is shared under a [CC BY-NC-SA 4.0](#) license and was authored, remixed, and/or curated by [David W. Lyons](#) via [source content](#) that was edited to the style and standards of the LibreTexts platform.

3.2: Möbius Geometry

Möbius geometry provides a unifying framework for studying planar geometries. In particular, the transformation groups of hyperbolic and elliptic geometries in the sections that follow are subgroups of the group of Möbius transformations.

Möbius transformations

A **Möbius transformation** (also called a **linear fractional transformation**) of the extended complex plane $\hat{\mathbb{C}}$ is a function of the form

$$f(z) = \frac{az + b}{cz + d} \quad (3.2.1)$$

where z is a complex variable, a, b, c, d are complex constants, and $ad - bc \neq 0$. To complete the definition, we make the assignments $f(-d/c) = \infty$ and $f(\infty) = a/c$ if $c \neq 0$. If $c = 0$, we assign $f(\infty) = \infty$.

Note on notational convention: It is customary to use capital letters such as S, T, U to denote Möbius transformations. It is also customary to omit the parentheses, and to write Tz instead of $T(z)$ to denote the value of a Möbius transformation.

Checkpoint 3.2.1.

Let $f(x) = (ax + b)/(cx + d)$ be a function of a *real* variable x with real constants a, b, c, d with $ad - bc \neq 0$ and $c \neq 0$.

1. Show that $\lim_{x \rightarrow -d/c} |f(x)| = \infty$.
2. Show that $\lim_{x \rightarrow \infty} f(x) = a/c$.

Checkpoint 3.2.2.

Show that the condition $ad - bc \neq 0$ is necessary and sufficient for invertibility. Find a formula for the inverse of $z \rightarrow (az + b)/(cz + d)$.

Checkpoint 3.2.3.

Show that the composition of two Möbius transformations is a Möbius transformation. Suggestion: First show that the composition has the form $z \rightarrow \frac{rz+s}{tz+u}$. Next, instead of a brute force calculation to check that $ru - ts \neq 0$, use **Checkpoint 3.2.2**.

Definition 3.2.4.

The set of all Möbius transformations forms a group $\mathbf{M}$, called the **Möbius group**, under the operation of function composition. **Möbius geometry** is the pair $(\hat{\mathbb{C}}, \mathbf{M})$.

There is a natural relationship between Möbius group operations and matrix group operations. The map $\mathcal{T}: GL(2, \mathbb{C}) \rightarrow \mathbf{M}$ be given by

$$\begin{bmatrix} a & b \\ c & d \end{bmatrix} \rightarrow \left[z \rightarrow \frac{az + b}{cz + d} \right] \quad (3.2.2)$$

is a group homomorphism. The kernel of $\mathcal{T}$ is the group of nonzero scalar matrices.

$$\ker \mathcal{T} = \left\{ \begin{bmatrix} k & 0 \\ 0 & k \end{bmatrix}, k \neq 0 \right\}.$$

The quotient group $GL(2, \mathbb{C})/\ker \mathcal{T}$ is called the **projective linear group** $PGL(2, \mathbb{C})$. Thus we have a group isomorphism

$$PGL(2, \mathbb{C}) \approx \mathbf{M}.$$

Checkpoint 3.2.5.

Show that the map $\mathcal{T}$ is a group homomorphism. Show that the kernel of $\mathcal{T}$ is

$$\ker \mathcal{T} = \left\{ \begin{bmatrix} k & 0 \\ 0 & k \end{bmatrix}, k \neq 0 \right\}.$$

Homotheties, rotations, translations, and inversions (see **Table 3.1.4** in Section 3.1) are special cases of Möbius transformations. These basic transformations can be viewed as building blocks for general Möbius transformations, as follows.

Proposition 3.2.6.

Every Möbius transformation is a composition of homotheties, rotations, translations, and inversions.

Proof.

See **Exercise 3.2.6.1**

Checkpoint 3.2.7.

1. Identify the values of the coefficients a, b, c, d in a Möbius transformation $z \rightarrow \frac{az+b}{cz+d}$ that is a homothety, rotation, translation, and inversion, respectively.
2. Write a Möbius transformation that does "clockwise rotation by one-quarter rotation about the point $2 - i$ ".

Corollary 3.2.8.

Möbius transformations are conformal.

Proof.

Apply **Proposition 3.2.6** and **Exercise Group 3.1.4.2–5**.

Next, a simple observation, in the form of the following Lemma, leads to a result called the Fundamental Theorem of Möbius Geometry.

Lemma 3.2.9.

If a Möbius transformation has more than two fixed points, then it is the identity transformation.

Proof.

Hint: just solve $z = \frac{az+b}{cz+d}$. You will need to consider cases.

Proposition 3.2.10. The Fundamental Theorem of Möbius Geometry.

A Möbius transformation is completely determined by any three input-output pairs. This means that for any triple of distinct input values z_1, z_2, z_3 in $\hat{\mathbb{C}}$ and any triple of distinct output values w_1, w_2, w_3 in $\hat{\mathbb{C}}$, there is a unique $T \in \mathbf{M}$ such that $Tz_i = w_i$ for $i = 1, 2, 3$.

Proof.

Outline: Suppose there are two such transformations, S and T . Show that $S \circ T^{-1}$ fixes three points. Now apply the previous Lemma.

Cross ratio

In what follows, we consider the special case of the output triple $w_1 = 1, w_2 = 0, w_3 = \infty$. Given three distinct points z_1, z_2, z_3 in $\hat{\mathbb{C}}$, we write $(\cdot, z_1, z_2, z_3)$ to denote the unique Möbius transformation that satisfies $z_1 \rightarrow 1, z_2 \rightarrow 0$, and $z_3 \rightarrow \infty$. We write (z_0, z_1, z_2, z_3) to denote the image of z_0 under $(\cdot, z_1, z_2, z_3)$. The expression (z_0, z_1, z_2, z_3) is called the **cross ratio** of the 4-tuple z_0, z_1, z_2, z_3 . The next two propositions give important properties of cross ratio.

Proposition 3.2.11. Cross ratio is invariant.

Let z_1, z_2, z_3 be distinct points in $\hat{\mathbb{C}}$, let $z_0 \in \hat{\mathbb{C}}$, and let T be any Möbius transformation. Then we have

$$(z_0, z_1, z_2, z_3) = (Tz_0, Tz_1, Tz_2, Tz_3).$$

Proof.

The transformations $(\cdot, z_1, z_2, z_3)$ and $(\cdot, Tz_1, Tz_2, Tz_3) \circ T$ both send $z_1 \rightarrow 1$, $z_2 \rightarrow 0$, and $z_3 \rightarrow \infty$, so they must be equal, by the Fundamental Theorem. Now apply both transformations to z_0 .

Proposition 3.2.12.

Let z_1, z_2, z_3 be distinct points in $\hat{\mathbb{C}}$, let $T = (\cdot, z_1, z_2, z_3)$, and let $C_T = T^{-1}(\hat{\mathbb{R}})$ be the inverse image of the extended real line $\hat{\mathbb{R}} = \mathbb{R} \cup \{\infty\}$ under T . Then C_T is a Euclidean circle or straight line. Furthermore, C_T is the unique Euclidean circle or straight line that contains the points z_1, z_2, z_3 .

Proof.

See Exercise 3.2.6.4

Corollary 3.2.13.

The cross ratio (z_0, z_1, z_2, z_3) is real if and only if z_0, z_1, z_2, z_3 lie on a Euclidean circle or straight line.

Corollary 3.2.14.

Let C be a Euclidean circle or straight line in $\hat{\mathbb{C}}$ and let T be any Möbius transformation. Then $T(C)$ is a Euclidean circle or straight line.

A Euclidean circle or straight line is called a **cline** (pronounced "kline") or **generalized circle**. The propositions and corollaries above show that the set of all clines is a single congruence class of figures in Möbius geometry.

Symmetry with respect to a cline

Geometrically, the conjugation map $z \rightarrow z^*$ in the complex plane is *reflection* across the real line. This "mirror" symmetry generalizes to symmetry with respect to any cline, as follows. Given a cline C that contains z_1, z_2, z_3 in $\hat{\mathbb{C}}$, let $T = (\cdot, z_1, z_2, z_3)$. Given any point z , the **symmetric point with respect to C** is

$$z^{*C} = (T^{-1} \circ \text{conj} \circ T)(z) \quad (3.2.3)$$

where $\text{conj}: \hat{\mathbb{C}} \rightarrow \hat{\mathbb{C}}$ is the extension of the conjugation map to the extended complex plane that sends $\infty \rightarrow \infty^* = \infty$. The idea is to map C to the real line via T , then conjugate, then map the real line back to C . See Figure 3.2.15.

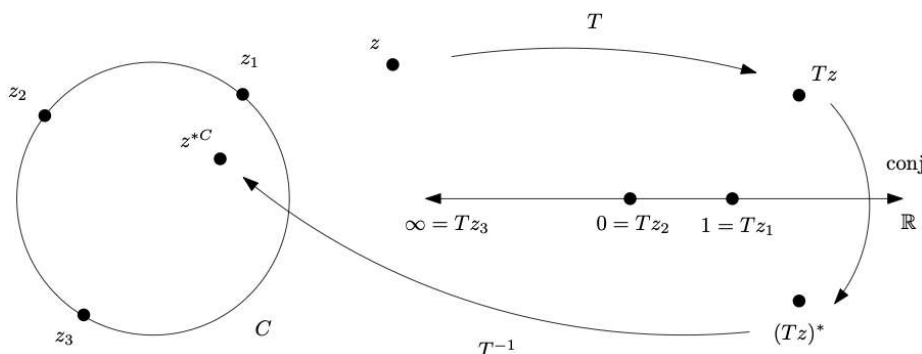


Figure 3.2.15. Symmetric points z, z^{*C} with respect to the circle C

The definition of symmetric point depends only on the circle C , and not on the three points z_1, z_2, z_3 . This fact is a corollary of the following Proposition.

Proposition 3.2.16.

Let C be a cline and let S be a Möbius transformation. If z, z' are a pair of points that are symmetric with respect to C , then Sz, Sz' are symmetric with respect to the cline $S(C)$. That is, we have

$$(Sz)^{*S(C)} = S(z^{*C}).$$

Proof.

Let z_1, z_2, z_3 be three points on C , so that Sz_1, Sz_2, Sz_3 are three points on $S(C)$. Let $T = (\cdot, z_1, z_2, z_3)$ and let $U = (\cdot, Sz_1, Sz_2, Sz_3)$. By invariance of the cross ratio, we have

$$(U \circ S)z = Tz.$$

Thus we have

$$\begin{aligned} (Sz)^{*S(C)} &= (U^{-1} \circ \text{conj} \circ U)(Sz) \text{ (by definition)} \\ &= (S \circ S^{-1} \circ U^{-1} \circ \text{conj} \circ U \circ S)(z) \\ &= S(S^{-1} \circ U^{-1} \circ \text{conj} \circ U \circ S)(z) \\ &= S(T^{-1} \circ \text{conj} \circ T)(z) \\ &= S(z^{*C}) \end{aligned}$$

as desired.

Corollary 3.2.17.

The definition of z^{*C} depends only on the circle C , and not on the three points z_1, z_2, z_3 used in the definition (3.2.3).

Proof.

See Exercise 3.2.6.6.

Normal forms

We conclude this section on Möbius geometry with a discussion of the **normal form** of a Möbius transformation. We begin with a Lemma.

Lemma 3.2.18.

If a Möbius transformation has exactly two fixed points 0 and ∞ , then it has the form $z \rightarrow \alpha z$ for some nonzero $\alpha \in \mathbb{C}$. If a Möbius transformation has a single fixed point at ∞ , then it has the form $z \rightarrow z + \beta$ for some nonzero $\beta \in \mathbb{C}$.

Proof.

See Exercise 3.2.6.5.

Now suppose that a Möbius transformation T has two fixed points, p and q . Let S be given by $Sz = \frac{z-p}{z-q}$. Let $w = Sz$ and let $U = S \circ T \circ S^{-1}$ be the transformation of the w -plane that is conjugate to T via S (see Exercise Group 1.3.3.3–6). It is easy to check that U has exactly two fixed points 0 and ∞ . Applying the previous Lemma, we have $Uw = \alpha w$ for some nonzero $\alpha \in \mathbb{C}$. Applying both sides of $S \circ T = U \circ S$ to z , we have the following **normal form** for T .

$$\frac{Tz - p}{Tz - q} = \alpha \frac{z - p}{z - q} \quad (3.2.4)$$

The transformation T is called **elliptic**, **hyperbolic**, or **loxodromic** if U is a rotation ($|\alpha| = 1$), a homothety ($\alpha > 0$), or neither, respectively.

Finally, suppose that a Möbius transformation T has exactly one fixed point at p . Let S be given by $Sz = \frac{1}{z-p}$. Again, let $w = Sz$ and let $U = S \circ T \circ S^{-1}$. This time, U has exactly one fixed point at ∞ . Applying the Lemma, we have $Uw = w + \beta$ for some nonzero $\beta \in \mathbb{C}$. Applying both sides of $S \circ T = U \circ S$ to z , we have the following *normal form* for T .

$$\frac{1}{Tz-p} = \frac{1}{z-p} + \beta \quad (3.2.5)$$

A Möbius transformation of this type is called **parabolic**. Here is a summary of the classification terminology associated with normal forms.

Table 3.2.19. Summary of normal forms of $T \in \mathbf{M}$

normal form type	normal form	conjugate transformation type
elliptic	$\frac{Tz-p}{Tz-q} = \alpha \frac{z-p}{z-q}, \alpha = 1$	rotation
hyperbolic	$\frac{Tz-p}{Tz-q} = \alpha \frac{z-p}{z-q}, \alpha > 0$	homothety
loxodromic	$\frac{Tz-p}{Tz-q} = \alpha \frac{z-p}{z-q}, \alpha \neq 0$ $ \alpha \neq 1, \alpha \neq 0$	composition of homothety with rotation
parabolic	$\frac{1}{Tz-p} = \frac{1}{z-p} + \beta, \beta \neq 0$	translation

Steiner circles

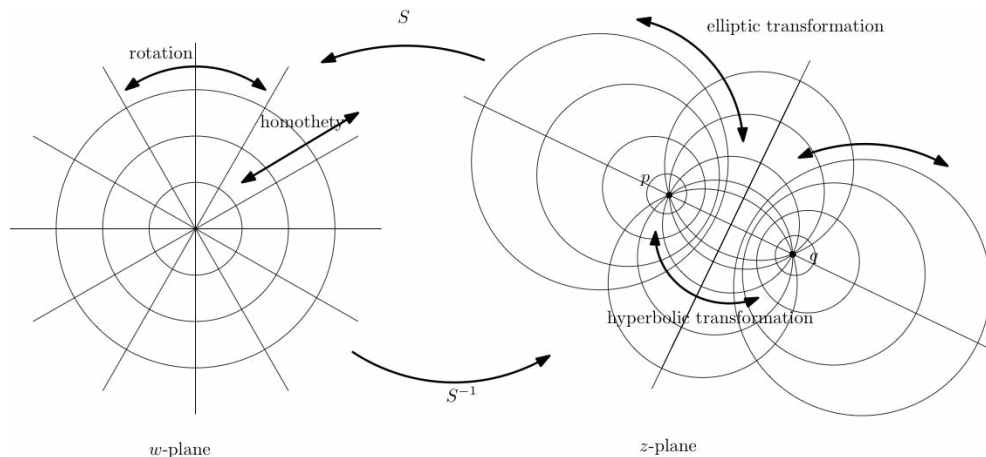


Figure 3.2.20. The polar coordinate grid and Steiner circle coordinate grid

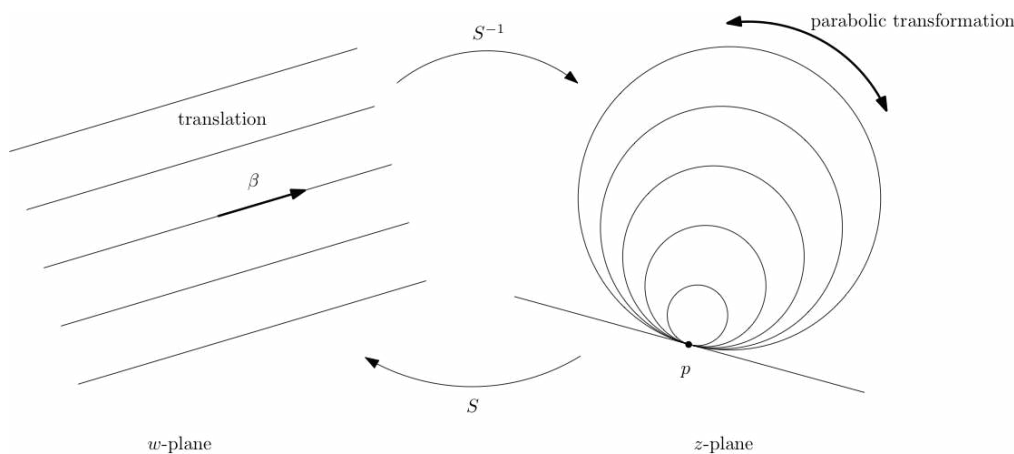


Figure 3.2.21. Degenerate coordinate grid lines and degenerate Steiner circles

The discussion of normal forms show that any non-identity Möbius transformation is conjugate to one of two basic forms, $w \rightarrow \alpha w$ or $w \rightarrow w + \beta$. The natural coordinate system for depicting the action of $w \rightarrow \alpha w$ is standard polar coordinates. See **Figure 3.2.20**. A homothety is a flow along radial lines and a rotation is a flow around polar circles. The natural "degenerate" coordinate system for depicting a translation $w \rightarrow w + \beta$ is a family of lines parallel to the line that contains the origin and β . A translation by β is a flow along these parallel lines. See **Figure 3.2.21**.

Pulling the polar and degenerate coordinate grids back to the z -plane by S^{-1} leads to coordinate grids called **Steiner circles**.¹ In the case where T has two fixed points p, q , the conjugating map $Sz = \frac{z-p}{z-q}$ takes $p \rightarrow 0, q \rightarrow \infty$. Therefore S^{-1} maps $0 \rightarrow p$ and $\infty \rightarrow q$. The transformation S^{-1} maps radial lines in the w -plane to clines in the z -plane that contain p and q called **Steiner circles of the first kind** and S^{-1} maps polar circles in the w -plane to clines in the z -plane called **Steiner circles of the second kind** or **circles of Apollonius**. See **Figure 3.2.20**.

In the case where T has one fixed point p , the conjugating map $Sz = \frac{1}{z-p}$ sends $p \rightarrow \infty$, so S^{-1} maps $\infty \rightarrow p$, and S^{-1} maps lines in the w -plane that are parallel to the line through 0 and β to clines in the z -plane that contain p . Every cline in this family is tangent to every other cline in this family at exactly the one point p . Clines in this family are called **degenerate Steiner circles**. See **Figure 3.2.21**. **Table 3.2.22** summarizes the graphical depiction of Möbius transformations.

Table 3.2.22. Summary of Steiner circle pictures of Möbius transformations

normal form type	graphical dynamic
elliptic	flow along Steiner circles of the second kind
hyperbolic	flow along Steiner circles of the first kind
loxodromic	composition of elliptic and hyperbolic flows
parabolic	flow along degenerate Steiner circles

Exercises

Exercise 1

Decomposition of Möbius transformations into four basic types.

1. Explain why a transformation of the form $z \rightarrow az$, with a any nonzero complex constant, is a composition of a homothety and a rotation.
2. Explicitly identify each homothety, rotation, translation, and inversion in (3.2.6) to (3.2.9) in the derivation below for the case $c \neq 0$.

$$z \rightarrow cz + d \quad (3.2.6)$$

$$\rightarrow \frac{1}{cz + d} \quad (3.2.7)$$

$$\rightarrow \frac{bc - ad}{cz + d} + a \quad (3.2.8)$$

$$\rightarrow \frac{1}{c} \left(\frac{bc - ad}{cz + d} + a \right) \quad (3.2.9)$$

$$= \frac{az + b}{cz + d} \quad (3.2.10)$$

3. Write your own decomposition for the case $c = 0$.

Exercise 2

Explicit form for the transformation $(\cdot, z_1, z_2, z_3)$.

1. Show that, for the special case when z_1, z_2, z_3 are complex (that is, none of the three points is ∞), we have the following.

$$(\cdot, z_1, z_2, z_3) = \left[z \rightarrow \frac{z - z_2}{z - z_3} \frac{z_1 - z_3}{z_1 - z_2} \right] \quad (3.2.11)$$

$$(z_0, z_1, z_2, z_3) = \frac{z_0 - z_2}{z_0 - z_3} \frac{z_1 - z_3}{z_1 - z_2} \quad (3.2.12)$$

2. Find explicit formulas for $(\cdot, z_1, z_2, z_3)$ when $z_1 = \infty$, then do the same for $z_2 = \infty$ and $z_3 = \infty$.

Exercise 3

Find Möbius transformations that make the following assignments.

1. $1 \rightarrow a, 0 \rightarrow b, \infty \rightarrow c$

2. $a \rightarrow d, b \rightarrow e, c \rightarrow f$

Exercise 4

Prove **Proposition 3.2.12**. Suggestion: Let $Tz = \frac{az+b}{cz+d}$, then manipulate $Tz = (Tz)^*$ to an equation with $|z|^2, z, z^*$ terms and coefficients involving a, b, c, d and their conjugates. Then use "complex completing the square" (see (1.1.24)). The hint below shows a version of a circle equation; peek if you need to, and use it to work partially forwards from $Tz = (Tz)^*$, and partially backwards from the equation in the hint.

Hint

$$\left| z - \left(\frac{a^*d - bc^*}{ac^* - a^*c} \right) \right|^2 = \left| \frac{ad - bc}{ac^* - a^*c} \right|^2$$

Exercise 5

Prove **Lemma 3.2.18**.

Exercise 6

Symmetry with respect to a cline.

1. Prove **Corollary 3.2.17**.

2. Let $\mathcal{C}$ be the unit circle. Show that $z^{*\mathcal{C}} = 1/z^*$. Suggestion: This is just a computation, but the choice of z_1, z_2, z_3 might make it more or less tedious. You might try $\omega, \omega^2, \omega^3 = 1$, where $\omega = e^{2\pi i/3}$.

3. Now let $\mathcal{C}$ be a circle with center a and radius $r > 0$. Use **Proposition 3.2.16** to show that $z^{*\mathcal{C}} = \frac{r^2}{(z-a)^*} + a$.

4. Let $\mathcal{C}$ be a straight line. Show that $z^{*\mathcal{C}}$ is the reflection of z across $\mathcal{C}$.

Normal forms and Steiner circles.

Exercise 7

Find the normal form and sketch a graph using Steiner circles for the following transformations.

1. $z \rightarrow \frac{1}{z}$
2. $z \rightarrow \frac{3z-1}{z+1}$

Exercise 8

Let p be the single fixed point of a Möbius transformation that is conjugate to $w \rightarrow w + \beta$ via $Sz = \frac{1}{z-p}$. Show that the single line in the degenerate Steiner clines through p is parallel to the direction given by β^* .

Hint

Show that $S^{-1}w = \frac{pw+1}{w}$, so S^{-1} takes $0, \beta, \infty$ to $\infty, \frac{p\beta+1}{\beta}, p$. Thus the single degenerate Steiner straight line through p is in the direction given by $\frac{p\beta+1}{\beta} - p = \frac{1}{\beta} \propto \beta^*$.

Exercise 9

Show that a (generalized) circle of Apollonius (a Steiner circle of the second kind) is characterized as the set of points of the form

$$C = \left\{ P \in \mathbb{C} : \frac{d(P, A)}{d(P, B)} = k \right\}$$

for some $A, B \in \mathbb{C}$ and some real constant $k > 0$.

This page titled [3.2: Möbius Geometry](#) is shared under a [CC BY-NC-SA 4.0](#) license and was authored, remixed, and/or curated by [David W. Lyons](#) via [source content](#) that was edited to the style and standards of the LibreTexts platform.

3.3: Hyperbolic geometry

Before the discovery of hyperbolic geometry, it was believed that Euclidean geometry was the only possible geometry of the plane. In fact, hyperbolic geometry arose as a byproduct of efforts to prove that there was no alternative to Euclidean geometry. In this section, we present a Kleinian version of hyperbolic geometry.

Definition 3.3.1.

Let $\mathbb{D} = \{z: |z| < 1\}$ denote the open unit disk in the complex plane. The **hyperbolic group**, denoted $\mathbf{H}$, is the subgroup of the Möbius group $\mathbf{M}$ of transformations that map $\mathbb{D}$ onto itself. The pair $(\mathbb{D}, \mathbf{H})$ is the **(Poincaré) disk model** of hyperbolic geometry.

Comments on terminology: Beware of the two different meanings of the adjective "hyperbolic". To say that a Möbius transformation is hyperbolic means that it is conjugate to a homothety (see Subsection 3.2.4). That is not the same thing as an element of the group of hyperbolic transformations.

The hyperbolic transformation group

We begin with an observation about Möbius transformations that map open disks onto themselves. Let $C = \{z: |z - a| = r\}$ be a circle with center a and radius $r > 0$. Let $D = \{z: |z - a| < r\}$ denote the open disk bounded by C , and let $E = \{z: |z - a| > r\}$ denote the complement of the closed disk bounded by C . Now suppose that a Möbius transformation T maps D onto itself. Every point $z \in D$ has a symmetric point $z^C \in E$, and because T takes symmetric points to symmetric points (**Proposition 3.2.16**), it must be that T maps E onto itself. By process of elimination, it must be that T maps C onto itself. Thus we have proved the following Lemma as a special case.

Lemma 3.3.2.

If $T \in \mathbf{H}$, then T maps the unit circle onto itself.

Given $T \in \mathbf{H}$, let $z_0 \in \mathbb{D}$ be the point that T maps to 0. It must be that T maps the symmetric point $\frac{1}{z_0^*}$ to ∞ , so T has the form

$$Tz = \alpha \frac{z - z_0}{z - \frac{1}{z_0^*}} = \alpha z_0^* \frac{z - z_0}{1 - z_0^* z}$$

for some α . A straightforward derivation shows that $|\alpha z_0^*| = 1$, so that we have (3.3.1) below. Another computation establishes an alternative formula (3.3.2) for $T \in \mathbf{H}$. See **Exercise 3.3.6.1**.

Proposition 3.3.3.

A Möbius transformation T is in $\mathbf{HH}$ if and only if T can be written in the form

$$Tz = e^{it} \frac{z - z_0}{1 - z_0^* z} \quad (3.3.1)$$

for some $t \in \mathbb{R}$ and $z_0 \in \mathbb{D}$. Alternatively, we have $T \in \mathbf{H}$ if and only if T can be written in the form

$$Tz = \frac{az + b}{b^* z + a^*} \quad (3.3.2)$$

for some $a, b \in \mathbb{C}$ such that $|a|^2 - |b|^2 = 1$.

Classification of clines in hyperbolic geometry

The clines of Möbius geometry are classified into several types in hyperbolic geometry, as summarized in **Table 3.3.4**.

Table 3.3.4. Clines in hyperbolic geometry

hyperbolic curve type	cline type
<i>hyperbolic straight line</i>	a cline that intersects the unit circle at right angles
<i>hyperbolic circle</i>	a circle completely contained in $\mathbb{D}$
<i>horocycle</i>	a circle with all but one point in $\mathbb{D}$, tangent to the unit circle
<i>hypercycle</i>	a cline that intersects the unit circle at a non-right angle

Normal forms for the hyperbolic group

In this subsection, we follow the development of normal forms for general Möbius transformations given in Subsection 3.2.4 to derive normal forms and graphical interpretations for transformations in the hyperbolic group. We begin with an observation about fixed points of a Möbius transformation that maps a cline to itself.

Lemma 3.3.5.

Let $T \in \mathbf{M}$ and let C be a cline. If $Tz = z$, then $T(z^{*C}) = z^{*C}$.

Proof.

Apply **Proposition 3.2.16**

Now let T be a non-identity element of $\mathbf{H}$. The fact that T maps the unit circle to itself implies that there are exactly three possible cases for fixed points of T .

1. There is a pair of fixed points p, q with $|p| < 1$, $|q| > 1$, and $q = \frac{1}{\bar{p}}$, that is, p, q are a pair of symmetric points (with respect to the unit circle) that do not lie on the unit circle.
2. There is a pair of fixed points that lie on the unit circle.
3. There is a single fixed point that lies on the unit circle.

Checkpoint 3.3.6.

Give an argument to justify the three cases above.

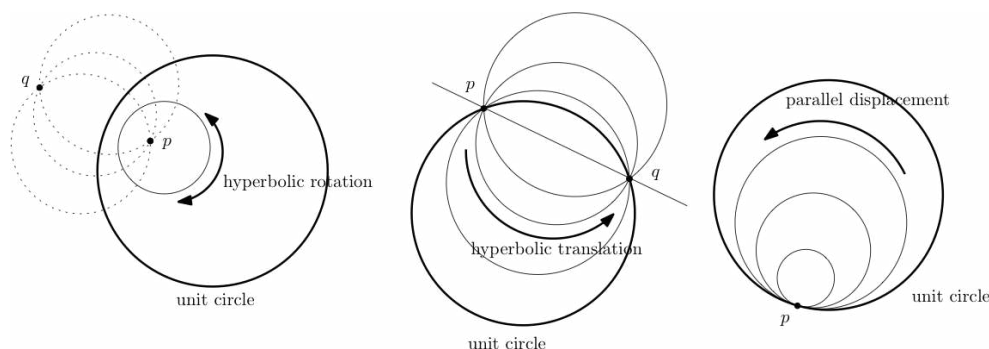


Figure 3.3.7. Three types of hyperbolic transformations

For cases 1 and 2 above, the map T acting on the z -plane is conjugate to the map $U = S \circ T \circ S^{-1}$ acting on the w -plane by $Uw = \lambda w$, for some nonzero $\lambda \in \mathbb{C}$, via the map $w = Sz = \frac{z-p}{z-q}$. In case 1, the map S takes the unit circle to some polar circle, say C , so U must map C to itself. It follows that $|\lambda| = 1$, so the Möbius normal form type for T is elliptic. The action of T is a rotation about Steiner circles of the second kind (hyperbolic circles) with respect to the fixed points p, q . A transformation $T \in \mathbf{H}$ of this type is called a *hyperbolic rotation*. See **Figure 3.3.7**.

For case 2, the map $w = Sz = \frac{z-p}{z-q}$ takes the unit circle to a straight line, say L , through the origin, so $U = S \circ T \circ S^{-1}$ must map L to itself. It follows that λ is real. Since S maps $\mathbb{D}$ to one of the two half planes on either side of L , the map U must take this half plane to itself. It follows that λ must be a *positive* real number, so the Möbius normal form type for T is hyperbolic. The action of T is a flow about Steiner circles of the first kind (hypercycles and one hyperbolic straight line) with respect to the fixed points p, q . A transformation $T \in \mathbf{H}$ of this type is called a **hyperbolic translation**. See Figure 3.3.7.

For case 3, the conjugating map $w = Sz = \frac{1}{z-p}$ takes T to $U = S \circ T \circ S^{-1}$ of the form $Uw = w + \beta$ for some $\beta \neq 0$. The Möbius normal form type for T is parabolic. The action of T is a flow along degenerate Steiner circles (horocycles) tangent to the unit circle at p . A transformation $T \in \mathbf{H}$ of this type is called a **parallel displacement**. See Figure 3.3.7.

This completes the list of transformation types for the hyperbolic group. See Table 3.3.8 for a summary.

Table 3.3.8. Normal forms for the hyperbolic group

hyperbolic transformation type	Möbius normal form	graphical dynamic
hyperbolic rotation	elliptic	flow around hyperbolic circles
parallel displacement	parabolic	flow around horocycles
hyperbolic translation	hyperbolic	flow along hypercycles
(none)	loxodromic	

Hyperbolic length and area

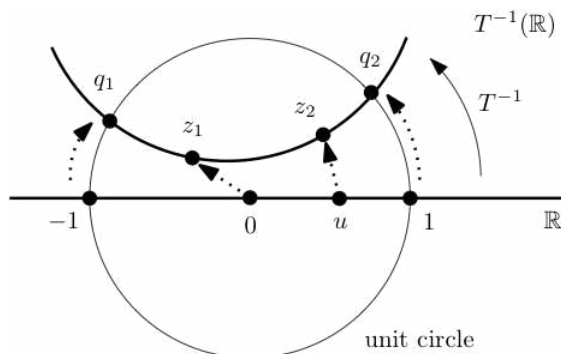


Figure 3.3.9. Constructing the hyperbolic straight line containing two points z_1, z_2

Let z_1, z_2 be distinct points in $\mathbb{D}$. Let $T \in \mathbf{H}$ be the transformation that sends $z_1 \rightarrow 0$ and $z_2 \rightarrow u > 0$. Then $T^{-1}(\mathbb{R})$ is a hyperbolic straight line that contains z_1, z_2 . Let $q_1 = T^{-1}(-1)$ and $q_2 = T^{-1}(1)$. See Figure 3.3.9.

Checkpoint 3.3.10.

Use Proposition 3.3.3 to write a formula for the transformation T in the previous paragraph.

Solution

Let $Sz = \frac{z-z_1}{1-\bar{z}_1 z}$, let $t = -\arg(Sz_2)$, and let $Tz = e^{it}Sz$, so that we have $Tz_1 = 0$ and $Tz_2 = u > 0$. Because $T \in \mathbf{H}$, T is determined by the two parameters.

A simple calculation verifies that $(0, u, 1, -1) = \frac{1+u}{1-u}$. By invariance of the cross ratio, we have $(z_1, z_2, q_2, q_1) = \frac{1+u}{1-u}$. For $0 \leq u < 1$, we have

$$1 \leq \frac{1+u}{1-u} < \infty$$

with equality on the left if and only if $u = 0$.

Checkpoint 3.3.11.

Do the simple calculation mentioned above.

Hint

Use (3.2.12).

Now, given any points z_1, z_2 in $\mathbb{D}$ not necessarily distinct, define the quantity $d(z_1, z_2)$ by

$$d(z_1, z_2) = \begin{cases} \ln((z_1, z_2, q_2, q_1)) & z_1 \neq z_2 \\ 0 & z_1 = z_2 \end{cases} \quad (3.3.3)$$

where q_1, q_2 are the ideal points on the hyperbolic straight line connecting z_1, z_2 (with each q_i at the z_i end of the line) as described above, in the case $z_1 \neq z_2$. From the discussion above we have

$$d(z_1, z_2) = \ln \left(\frac{1+u}{1-u} \right) \quad (3.3.4)$$

where $u = \left| \frac{z_2 - z_1}{1 - \bar{z}_1 z_2} \right|$.

Checkpoint 3.3.12.

Justify the value of u in (3.3.4).

Proposition 3.3.13.

The function d given by (3.3.3) is invariant under the action of the hyperbolic group. That is, we have

$$d(z_1, z_2) = d(Tz_1, Tz_2) \quad (3.3.5)$$

for all $z_1, z_2 \in \mathbb{D}$ and for all $T \in \mathbf{H}$.

Checkpoint 3.3.14.

Prove Proposition 3.3.13.

The following Proposition shows that d is a *metric* on hyperbolic space, and justifies referring to $d(z_1, z_2)$ as the (**hyperbolic**) **distance** between the points z_1, z_2 .

Proposition 3.3.15.

The function d given by (3.3.3) defines a metric on $\mathbb{D}$. That is, d satisfies

1. $d(z_1, z_2) \geq 0$, and $d(z_1, z_2) = 0$ if and only if $z_1 = z_2$
2. $d(z_1, z_2) = d(z_2, z_1)$
3. $d(z_1, z_3) \leq d(z_1, z_2) + d(z_2, z_3)$ (the triangle inequality)

for all z_1, z_2, z_3 in $\mathbb{D}$.

Proof.

Property 1 follows immediately from (3.3.4). Property 2 is a simple calculation: just write down the cross ratio expressions for $d(z_1, z_2)$ and $d(z_2, z_1)$ and compare. The proof of Property 3 is outlined in exercise **Exercise 3.3.6.4**.

Now let γ be a curve parameterized by $t \rightarrow z(t) = x(t) + iy(t)$, where $x(t), y(t)$ are differentiable real-valued functions of the real parameter t on an interval $a < t < b$. Consider a short segment of γ , say, on an interval $t_0 \leq t \leq t_1$. Let $z_0 = z(t_0)$ and $z_1 = z(t_1)$. Then we have $d(z(t_0), z(t_1)) = \ln \left(\frac{1+u}{1-u} \right)$ where $u = \left| \frac{z_1 - z_0}{1 - \bar{z}_0 z_1} \right|$. The quantity $|z_1 - z_0|$ is well-approximated by $|z'(t_0)|dt$, where $z'(t) = x'(t) + iy'(t)$ and $dt = t_1 - t_0$. Thus, u is well-approximated by $\frac{|z'(t_0)|}{1 - |z(t_0)|^2} dt$. The first order Taylor approximation for $\ln((1+u)/(1-u))$ is $2u$. Putting this all together, we have the following.

$$\text{Length}(\gamma) = 2 \int_a^b \frac{|z'(t)|}{1 - |z(t)|^2} dt \quad (3.3.6)$$

Checkpoint 3.3.16.

Show that the first order Taylor approximation of $\ln((1+u)/(1-u))$ is $2u$.

Checkpoint 3.3.17.

Find the length of the hyperbolic circle parameterized by $z(t) = \alpha e^{it}$ for $0 \leq t \leq 2\pi$, where $0 < \alpha < 1$

We conclude this subsection on hyperbolic length and area with an integral formula for the area of a region R in $\mathbb{D}$, following the development in [4]. As a function of the two real variables r and θ , the polar form expression $z = re^{i\theta}$ gives rise to the two parameterized curves $r \rightarrow z_1(r) = re^{i\theta}$ (where θ is constant) and $\theta \rightarrow z_2(\theta) = re^{i\theta}$ (where r is constant). Using $z_1'(r) = e^{i\theta}$ and $z_2'(\theta) = ire^{i\theta}$, the arc length differential $ds = \frac{2|z'(t)| dt}{1-|z(t)|^2}$ for the two curves are the following.

$$\frac{2|e^{i\theta}| dr}{1-r^2} = \frac{2 dr}{1-r^2} \text{ (for curve } z_1)$$

$$\frac{2|ire^{i\theta}| d\theta}{1-r^2} = \frac{2r d\theta}{1-r^2} \text{ (for curve } z_2)$$

Thus we have $dA = \frac{4r dr d\theta}{(1-r^2)^2}$, so that the area of a region R is

$$\text{Area}(R) = \iint_R dA = \iint_R \frac{4r dr d\theta}{(1-r^2)^2}. \quad (3.3.10)$$

Checkpoint 3.3.18.

Find the area of the hyperbolic disk $\{|z| \leq \alpha\}$, for $0 < \alpha < 1$.

The upper-half plane model

Definition 3.3.19. The upper half-plane model of hyperbolic geometry.

Let $\mathbb{U} = \{z: \text{Im}(z) > 0\} = \{z: \text{Im}(z) > 0\}$ denote the upper half of complex plane above the real axis, and let $\mathbf{H}_{\mathbb{U}}$ denote the subgroup of the Möbius group $\mathbf{M}$ of transformations that map $\mathbb{U}$ onto itself. The pair $(\mathbb{U}, \mathbf{H}_{\mathbb{U}})$ is the **upper half-plane model** of hyperbolic geometry.

Proposition 3.3.20.

A Möbius transformation T is in $\mathbf{H}_{\mathbb{U}}$ if and only if T can be written in the form

$$Tz = \frac{az + b}{cz + d} \quad (3.3.11)$$

such that a, b, c, d are real and $ad - bc > 0$.

Hyperbolic straight lines in the upper half-plane model are clines that intersect the real line at right angles. The hyperbolic distance between two points z_1, z_2 in the upper half-plane is

$$d(z_1, z_2) = \ln((z_1, z_2, q_2, q_1)) \quad (3.3.12)$$

where q_1, q_2 are the points on the (extended) real line at the end of the hyperbolic straight line that contains z_1, z_2 , with each q_i on the same "side" as the corresponding z_i . The hyperbolic length of a curve γ parameterized by $t \rightarrow z(t) = x(t) + iy(t)$ on the interval $a \leq t \leq b$ is

$$\text{Length}(\gamma) = \int_a^b \frac{|z'(t)|}{y(t)} dt. \quad (3.3.13)$$

The hyperbolic area of a region R in $\mathbb{U}$ is

$$\text{Area}(R) = \iint_R dA = \iint_R \frac{dx dy}{y^2}. \quad (3.3.14)$$

Exercises

Exercise 1

Prove **Proposition 3.3.3** using the following outline.

1. Complete the proof of (3.3.1) using this outline: Let $|z| = 1$ and apply **Lemma 3.3.2**. We have

$$1 = |Tz| = |\alpha z_0^*| \left| \frac{z - z_0}{1 - z_0^* z} \right|.$$

Continue this derivation to show that $|\alpha z_0^*| = 1$.

2. Prove (3.3.2) by verifying the following. Given $z_0 \in \mathbb{D}$ and $t \in \mathbb{R}$, show that the assignments $a = \frac{e^{it/2}}{\sqrt{1-|z_0|^2}}, b = \frac{-e^{it/2} z_0}{\sqrt{1-|z_0|^2}}$ satisfy $|a|^2 - |b|^2 = 1$ and that

$$\frac{az + b}{b^* z + a^*} = e^{it} \frac{z - z_0}{1 - z_0^* z}. \quad (3.3.15)$$

Conversely, given $a, b \in \mathbb{C}$ with $|a|^2 - |b|^2 = 1$, show that the assignments $t = 2 \arg a, z_0 = -\frac{b}{a}$ satisfy $z_0 \in \mathbb{D}$, and that (3.3.15) holds.

Exercise 2

Two points determine a line.

Let p, q be distinct points in $\mathbb{D}$. Show that there is a unique hyperbolic straight line that contains p and q .

Hint

Start by choosing a transformation that sends $p \rightarrow 0$.

Exercise 3

Dropping a perpendicular from a point to a line.

Let L be a hyperbolic straight line and let $p \in \mathbb{D}$ be a point not on L . Show that there is a unique hyperbolic straight line M that contains p and is orthogonal to L .

Hint

Start by choosing a transformation that sends $p \rightarrow 0$.

Exercise 4

The triangle inequality for the hyperbolic metric.

Show that $d(a, b) \leq d(a, c) + d(c, b)$ for all a, b, c in $\mathbb{D}$ using the outline below.

1. Show that the triangle inequality holds with strict equality when a, b, c are collinear and c is between a and b . Suggestion: This is a straightforward computation using the cross ratio expressions for the values of d .
2. Show that the triangle inequality holds with strict inequality when a, b, c are collinear and c is not between a and b .
3. Let $p \in \mathbb{D}$ lie on a hyperbolic line L , let $q \in \mathbb{D}$, let M be a line through q perpendicular to L (this line M exists by **Exercise 3.3.6.3**), and let q' be the point of intersection of L, M . Show that $d(p, q') \leq d(p, q)$. Suggestion: apply $T \in \mathbf{H}$ that takes $p \rightarrow 0$ and takes $L \rightarrow \mathbb{R}$. Let $t = -\arg(Tq)$ if $\operatorname{Re}(Tq) \geq 0$ and let $t = \pi - \arg(Tq)$ if $\operatorname{Re}(Tq) < 0$. Let $r = e^{it} Tq$. See **Figure 3.3.21**.
4. Given arbitrary a, b, c , apply a transformation T to send $a \rightarrow 0$ and b to a nonnegative real point. Drop a perpendicular from Tc to the real line, say, to c' . Apply results from the previous steps of this outline.

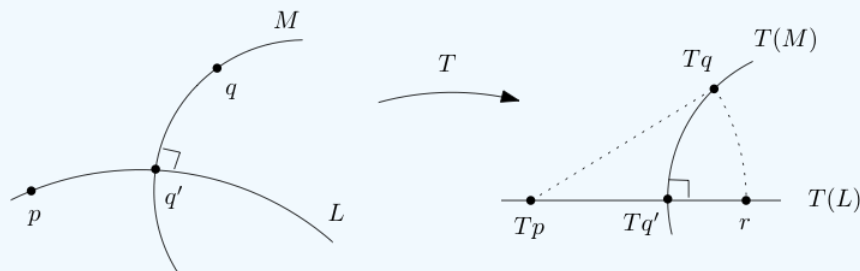


Figure 3.3.21.

Exercise 5

Prove **Proposition 3.3.20**.

Exercise 6

Length integral in the upper half-plane model.

This exercise is to establish (3.3.13). The strategy is to obtain the differential expression

$$d(z(t_0), z(t_1)) \approx \frac{|z'(t)|dt}{y(t)}$$

for a curve $z(t) = x(t) + iy(t)$ with $z(t_0) = z_0$, $z(t_1) = z_1$, and $dt = t_1 - t_0$ using the following sequence of steps.

- First, map z_0, z_1 in $\mathbb{U}$ to z'_0, z'_1 in $\mathbb{D}$ using a transformation μ that preserves distance.
- Using the analysis we used to get the disk model length integral formula (3.3.6), we have

$$d(z'_0, z'_1) = \ln \left(\frac{1+u}{1-u} \right)$$

where $u = \left| \frac{z'_1 - z'_0}{1 - (z'_0)^* z'_1} \right|$.

- Translate the above expression in terms of z_0, z_1 , and show that the differential approximation is $\frac{|z'(t)|dt}{y(t)}$.

Complete the exercise parts below to carry out the strategy just outlined.

1. Show that $\mu z = \frac{z-i}{z+i}$ takes $\mathbb{U}$ to $\mathbb{D}$.
2. Let $z'_0 = \mu z_0$ and $z'_1 = \mu z_1$. Show that

$$\frac{z'_1 - z'_0}{1 - (z'_0)^* z'_1} = e^{it} \frac{z_1 - z_0}{z_0^* - z_1}$$

for some real t .

3. Let $u = \left| \frac{z_1 - z_0}{z_0^* - z_1} \right|$. Show that

$$\ln \left(\frac{1+u}{1-u} \right) \approx \frac{|z(t)|dt}{y(t)}.$$

Exercise 7

Area integral in the upper half-plane model.

Adapt the argument in the paragraph preceding the disk model area integral (3.3.10) to establish the upper half-plane area integral (3.3.14).

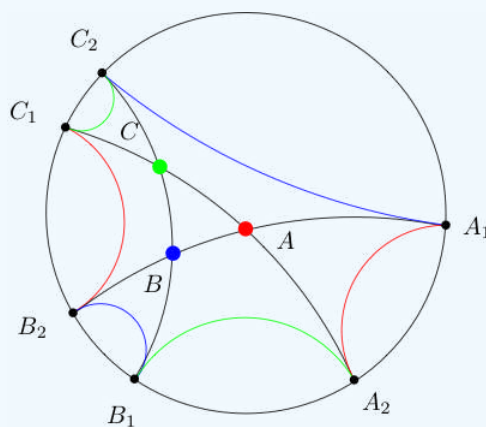


Figure 3.3.22. Hyperbolic triangle $\triangle ABC$

Area of a hyperbolic triangle.

The following sequence of exercises establishes the area formula for hyperbolic triangles.

Exercise 8

Area of a doubly-asymptotic triangle.

A triangle with one vertex in $\mathbb{D}$ and two vertices on the unit circle, connected by arcs of circles that are orthogonal to the unit circle, is called a **doubly-asymptotic** hyperbolic triangle. Examples are $\triangle AA_1A_2$, $\triangle BB_1B_2$, and $\triangle CC_1C_2$ in Figure 3.3.22.

1. Explain why any doubly-asymptotic triangle in the upper half-plane is congruent to the one shown in Figure 3.3.23 for some angle α .
2. Now use the integration formula for the upper half-plane model to show that the area of the doubly-asymptotic triangle with angle α (at the vertex interior to $\mathbb{U}$) is $\pi - \alpha$.

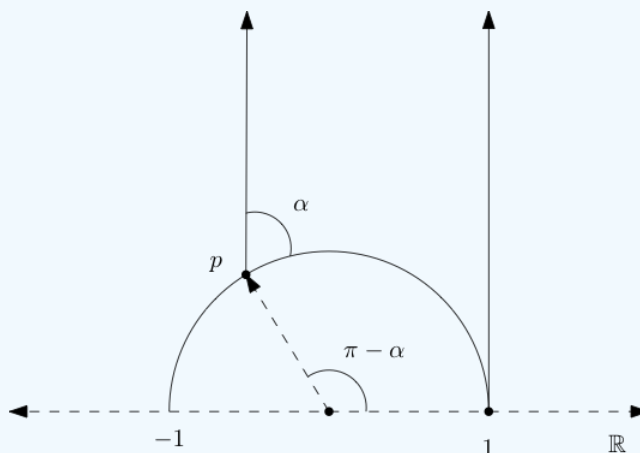


Figure 3.3.23. Doubly-asymptotic hyperbolic triangle in the upper half-plane with vertices $1, p, \infty$ with p on the upper half of the unit circle

Exercise 9

Area of an asymptotic n -gon.

A polygon with $n \geq 3$ vertices on the unit circle, connected by arcs of circles that are orthogonal to the unit circle, is called an **asymptotic n -gon**. An example of an asymptotic hexagon is the figure with vertices $A_1, A_2, B_1, B_2, C_2, C_1$ connected by the colored hyperbolic lines in Figure 3.3.22. Show that the area of an asymptotic n -gon is $\pi(n - 2)$.

Hint

Partition the asymptotic n -gon into n doubly-asymptotic triangles.

Exercise 10

Area of a hyperbolic triangle.

Let $\triangle ABC$ be a hyperbolic triangle. Extend the three sides AB , BC , AC to six points on the unit circle. See **Figure 3.3.22**. Use a partition of the asymptotic hexagon whose vertices are these six points to show that the area of $\triangle ABC$ is

$$\text{Area}(\triangle ABC) = \pi - (\angle A + \angle B + \angle C). \quad (3.3.16)$$

Hint

Partition the asymptotic hexagon with vertices $A_1, A_2, B_1, B_2, C_1, C_2$. Start with the six overlapping doubly-asymptotic triangles whose bases are colored arcs and whose vertex in $\mathbb{D}$ is whichever of A, B, C matches the color of the base. For example, the two red doubly-asymptotic triangles are $\triangle AA_1A_2$ and $\triangle AC_1B_2$.

This page titled [3.3: Hyperbolic geometry](#) is shared under a [CC BY-NC-SA 4.0](#) license and was authored, remixed, and/or curated by [David W. Lyons](#) via [source content](#) that was edited to the style and standards of the LibreTexts platform.

3.4: Elliptic geometry

Elliptic geometry is the geometry of the sphere (the 2-dimensional surface of a 3-dimensional solid ball), where congruence transformations are the rotations of the sphere about its center.

We will work with three models for elliptic geometry: one based on quaternions, one based on rotations of the sphere, and another that is a subgeometry of Möbius geometry. Using the natural identification $xi + yj + zk \leftrightarrow (x, y, z)$ of the pure quaternions $\mathbb{R}_{\mathbb{H}}^3$ with $\mathbb{R}^3$, we will write $S_{\mathbb{H}}^2$ to denote the set of unit pure quaternions.

$$S_{\mathbb{H}}^2 = \{xi + yj + zk \in \mathbb{H} : x^2 + y^2 + z^2 = 1\}$$

We begin by establishing some basic facts about the relevant transformation groups.

The group of unit quaternions

Recall from Section 1.2 that $U(\mathbb{H})$ is the set of quaternions of modulus 1. In fact, $U(\mathbb{H})$ is a group.

Checkpoint 3.4.1.

Show that $U(\mathbb{H})$ is a group.

Recall that the map $M: \mathbb{H} \rightarrow \mathcal{M}_{\mathbb{H}}$ sends $r = a + bi + cj + dk$ to the matrix

$$\begin{bmatrix} a + bi & c + di \\ -c + di & a - bi \end{bmatrix}.$$

The image of $U(\mathbb{H})$ under M is the matrix group $SU(2)$, called the *special unitary* group.

$$SU(2) = \left\{ \begin{bmatrix} a & b \\ -b^* & a^* \end{bmatrix} : a, b \in \mathbb{C}, |a|^2 + |b|^2 = 1 \right\} \quad (3.4.1)$$

Restricting the domain of M to $U(\mathbb{H})$ and restricting the codomain of M to $M(U(\mathbb{H})) = SU(2)$ is an isomorphism of groups

$$U(\mathbb{H}) \approx SU(2).$$

Checkpoint 3.4.2.

Show that $SU(2)$ is a group. Show that $M: U(\mathbb{H}) \rightarrow SU(2)$ is a homomorphism.

Hint

It is not necessary to perform any new computation to show that M is a homomorphism. Instead, use (1.2.5).

The action of a unit quaternion as a rotation on $\mathbb{R}_{\mathbb{H}}^3$ (see **Proposition 1.2.9**) takes the sphere $S_{\mathbb{H}}^2$ to itself. The action of the group $U(\mathbb{H})$ on $S_{\mathbb{H}}^2$ defines a model of elliptic geometry.

Definition 3.4.3: quaternion model of elliptic geometry

The *quaternion model* of elliptic geometry is $(S_{\mathbb{H}}^2, U(\mathbb{H}))$.

Checkpoint 3.4.4.

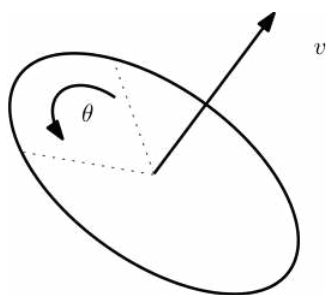
Show that the map $U(\mathbb{H}) \rightarrow \text{Perm}(S_{\mathbb{H}}^2)$ given by

$$r \rightarrow [v \rightarrow rv r^*]$$

is a group action.

The group of rotations of the 2-sphere

Let $R_{v,\theta}$ denote the rotation of $\mathbb{R}^3$ about the axis given by a unit vector v by an angle θ . We use the standard orientation, so that a positive value of θ is a counterclockwise rotation of the plane orthogonal to v , as viewed from "above" where v points in the "up" direction. See **Figure 3.4.5**.



disk in the plane perpendicular to v

Figure 3.4.5. The rotation $R_{v,\theta}$ about the vector v by the angle θ

Notation convention: For readability and convenience, we write $R_{X,\theta}, R_{Y,\theta}, R_{Z,\theta}$ to denote rotations by θ radians about the standard basis vectors $(1, 0, 0), (0, 1, 0), (0, 0, 1)$, respectively.

We will write $\text{Rot}(S^2)$ to denote the set of all rotations.

$$\text{Rot}(S^2) = \{R_{v,\theta} : v \in \mathbb{R}^3, |v| = 1, \theta \in \mathbb{R}\}$$

To see why the set $\text{Rot}(S^2)$ is a group¹ under the operation of composition, consider the map $U(\mathbb{H}) \rightarrow \text{Rot}(S^2)$ given by $r \rightarrow R_r$ established by **Proposition 1.2.9**. The fact that $R_r \circ R_s = R_{rs}$ (see **Exercise 1.2.6.3**) implies that the composition of two rotations is a rotation. The remaining group properties are straightforward. Once we have proved that $\text{Rot}(S^2)$ is a group, the same equation $R_r \circ R_s = R_{rs}$ shows that the map $r \rightarrow R_r$ is a homomorphism of groups $U(\mathbb{H}) \rightarrow \text{Rot}(S^2)$. The kernel of this homomorphism is $\{\pm 1\}$. This establishes an isomorphism

$$U(\mathbb{H})/\{\pm 1\} \approx \text{Rot}(S^2).$$

Checkpoint 3.4.6.

Complete the details to show that $\text{Rot}(S^2)$ is a group. Show that the kernel of the homomorphism $U(\mathbb{H}) \rightarrow \text{Rot}(S^2)$ given by $r \rightarrow R_r$ is $\{\pm 1\}$.

Hint

Use **Proposition 1.2.9**.

Definition 3.4.7.

The **spherical model** of elliptic geometry is $(S^2, \text{Rot}(S^2))$.

We conclude with a useful fact about constructing arbitrary rotations by composing rotations from a specific set elementary types, namely, rotations about the z -axis by arbitrary angles, and rotations about the x -axis by $\pi/2$ radians. We start with a Lemma that shows how to do this for y -axis rotations.

Lemma 3.4.8. Rotations about the y -axis.

An arbitrary rotation about the y -axis is a composition of a rotations about the x -axis by $\pi/2$ radians with a rotation about the z -axis. Specifically, we have the following.

$$R_{Y,\theta} = R_{X,\pi/2}^{-1} \circ R_{Z,\theta} \circ R_{X,\pi/2} \quad (3.4.2)$$

Proof.

Visualize! You can also verify by checking that both sides of (3.4.2) yield the same result when evaluated on the three standard basis vectors. Yet another proof is to do a quaternion computation.

Proposition 3.4.9. Generators for $Rot(S^2)$

The set

$$\{R_{Z,\theta} : \theta \in \mathbb{R}\} \cup \{R_{X,\pi/2}\}$$

is a generating set for $Rot(S^2)$. This means that any rotation may be written as a composition of rotations about the z -axis and rotations about the x -axis by $\pi/2$ radians.

Proof.

Consider a model of the sphere printed with a map of the world (i.e., a geographic globe) in such a way that the north pole is on top of the sphere and Greenwich, England (at zero degrees longitude) is in the x, z -plane. The sphere in the upper left of **Figure 3.4.10** depicts this "start" position of the north pole N , Greenwich G , and the great circle C that is the intersection of the sphere with the x, z -plane (C is shown in red in all four spheres for reference). Now let R be an arbitrary rotation. The sphere in the upper right of **Figure 3.4.10** shows how N , G , and C are transformed by R . The rest of the diagram shows how we can write R^{-1} as a composition of rotations by "putting the north pole back on top" and "putting zero degrees back in place", as follows. From the upper right in the diagram, we "put the north pole back" by first performing a rotation R_{Z,θ_1} about the z -axis that brings the north pole into the x, z -plane. Next, we perform the rotation R_{Y,θ_2} about the y -axis (use the Lemma) to bring the north pole back to the top. Finally, we perform a rotation R_{Z,θ_3} to bring Greenwich back home in the x, z -plane. Reading clockwise from the upper left of the diagram, the sequence of transformations

$$R, R_{Z,\theta_1}, R_{Y,\theta_2}, R_{Z,\theta_3}$$

takes the north pole N through the sequence

$$N \rightarrow R(N) \rightarrow N' \rightarrow N'' = N \rightarrow N.$$

Meanwhile, G traces the path

$$G \rightarrow R(G) \rightarrow G' \rightarrow G'' \rightarrow G$$

while the great circle C is transformed in the sequence

$$C \rightarrow R(C) \rightarrow C' \rightarrow C'' \rightarrow C.$$

This leads to the decomposition $R = R_{Z,-\theta_1} \circ R_{Y,-\theta_2} \circ R_{Z,-\theta_3}$.

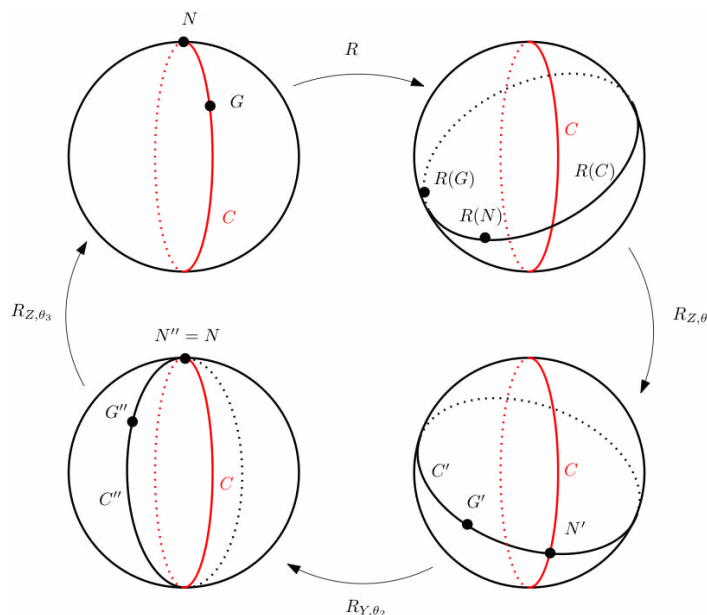


Figure 3.4.10. Decomposition of the rotation R

The elliptic subgroup of the Möbius group

Let $\mathbf{S}$ denote the group of transformations of $\hat{\mathbb{C}}$ that are conjugate to rotations of S^2 via the stereographic projection.

$$\mathbf{S} = \{s \circ R \circ s^{-1} : R \in \text{Rot}(S^2)\}$$

The group $\mathbf{S}$ is called the **elliptic group**. It is easy to check that the map $\text{Rot}(S^2) \rightarrow \mathbf{S}$ given by $R \rightarrow s \circ R \circ s^{-1}$ is an isomorphism of groups, so we have

$$\mathbf{S} \approx \text{Rot}(S^2).$$

Checkpoint 3.4.11.

Show that $\mathbf{S}$ is indeed a group. Show that $R \rightarrow s \circ R \circ s^{-1}$ is a group isomorphism $\text{Rot}(S^2) \rightarrow \mathbf{S}$.

Exercises in Section 1.3 show that $s \circ R_{Z,\theta} \circ s^{-1}$ the Möbius transformation $T_{Z,\theta}$ given by $z \rightarrow e^{i\theta}z$ (see **Exercise 1.3.3.4**) and that $s \circ R_{X,\pi/2} \circ s^{-1}$ is the Möbius transformation $T_{X,\pi/2}$ given by $z \rightarrow \frac{z+i}{iz+1}$ (see **Exercise 1.3.3.6**). The fact (**Proposition 3.4.9**) that rotations of the form $R_{Z,\theta}, R_{X,\pi/2}$ generate $\text{Rot}(S^2)$ implies that the Möbius transformations $T_{Z,\theta}$ and $T_{X,\pi/2}$ generate $\mathbf{S}$. Therefore $\mathbf{S}$ is in fact a subgroup of the Möbius group.

Definition 3.4.12.

The **Möbius subgeometry model** of elliptic geometry is $(\hat{\mathbb{C}}, \mathbf{S})$.

We can say more about the specific form of elements in $\mathbf{S}$ in terms of the group homomorphism $\mathcal{T}: GL(2, \mathbb{C}) \rightarrow \mathbf{M}$ that sends the matrix $\begin{bmatrix} a & b \\ c & d \end{bmatrix}$ to the Möbius transformation $z \rightarrow \frac{az+b}{cz+d}$ (see (3.2.2)). Observe that the transformations

$$T_{Z,\theta} = \mathcal{T} \left(\begin{bmatrix} e^{i\theta/2} & 0 \\ 0 & e^{-i\theta/2} \end{bmatrix} \right) \quad (3.4.3)$$

$$T_{X,\pi/2} = \mathcal{T} \left(\begin{bmatrix} \frac{1}{\sqrt{2}} & \frac{i}{\sqrt{2}} \\ \frac{i}{\sqrt{2}} & \frac{1}{\sqrt{2}} \end{bmatrix} \right) \quad (3.4.4)$$

are images of elements of the group $SU(2)$ (see (3.4.1)). Because $T_{Z,\theta}, T_{X,\pi/2}$ generate $\mathbf{S}$, it follows that every element of $\mathbf{S}$ is the image under $\mathcal{T}$ of an element of $SU(2)$.

Checkpoint 3.4.13.

Let $M_{Z,\theta}, M_{X,\pi/2}$ denote the matrices $\begin{bmatrix} e^{i\theta/2} & 0 \\ 0 & e^{-i\theta/2} \end{bmatrix}, \begin{bmatrix} \frac{1}{\sqrt{2}} & \frac{i}{\sqrt{2}} \\ \frac{i}{\sqrt{2}} & \frac{1}{\sqrt{2}} \end{bmatrix}$ respectively. Verify that $M_{Z,\theta}, M_{X,\pi/2}$ are indeed elements of $SU(2)$. Verify (3.4.3) and (3.4.4). Explain the final comment in the paragraph above. Why does it follow that every element of $\mathbf{S}$ is the image of an element of $SU(2)$?

Thus we have proved the following explicit formula for elements of $\mathbf{S}$

Proposition 3.4.14. Formula for transformations in the elliptic group.

A map T is an element of $\mathbf{S}$ if and only if T may be written in the form $Tz = \frac{az+b}{-b^*z+a^*}$ for some $a, b \in \mathbb{C}$ with $|a|^2 + |b|^2 = 1$.

Setting $e^{i\theta} = \frac{a}{a^*}$ and $z_0 = \frac{-b}{a}$, we have the following alternative form for $T \in \mathbf{S}$.

$$Tz = e^{i\theta} \frac{z - z_0}{z_0^* z + 1} \quad (3.4.5)$$

Circles in S^2 and clines in $\mathbb{C}^\wedge$

A *circle* in S^2 is a circle in a plane intersecting S^2 . A **great circle** is the intersection of S^2 with a plane through the origin. In elliptic geometry, a great circle is called an **elliptic straight line** because the path of shortest length connecting two given points in S^2 is an arc of a great circle. Circles in S^2 that are not great circles are called **elliptic cycles**. Elliptic straight lines and elliptic cycles in the

Möbius subgeometry model $(\hat{\mathbb{C}}, \mathbf{S})$ are stereographic projections of elliptic straight lines and elliptic cycles in the spherical model. It turns out that elliptic straight lines and elliptic cycles in $\hat{\mathbb{C}}$ are in fact clines. Here is the statement and proof.

Proposition 3.4.15. Stereographic projection takes circles to clines.

Let C be a circle that is the intersection of S^2 with a plane in $\mathbb{R}^3$. If C contains the north pole $(0, 0, 1)$ of S^2 , then $s(C \setminus \{(0, 0, 1)\})$ is a Euclidean straight line in $\mathbb{C}$. Otherwise, $s(C)$ is a circle in $\mathbb{C}$.

Proof.

Proof sketch: The statement about the case when C contains the north pole is geometrically clear. For the case when C does not contain $(0, 0, 1)$, choose a rotation R of S^2 that takes some point on C to the north pole. Again, let $T = s \circ R \circ s^{-1}$ be the conjugate element in $\mathbf{S}$. It is clear that R takes C to a circle, that s takes $R(C)$ to a Euclidean straight line, and that T^{-1} takes $s(R(C))$ to a cline (because T^{-1} is a Möbius transformation!). Thus $s(C) = (T^{-1} \circ s \circ R)(C)$ is a cline. Because $(0, 0, 1)$ is not on C , it must be that ∞ is not on $s(C)$, so $s(C)$ is a circle in $\mathbb{C}$.

Angles and orientation on S^2

The standard orientation for angles on S^2 (see Subsection 3.4.2) is also called the *outward-pointing normal* orientation. The standard orientation measures angles from the viewpoint of an observer standing on the *outside* of the sphere. The *inward-pointing normal* orientation is the reverse orientation that measures angles from the viewpoint of an observer walking on the inside of the sphere. See **Figure 3.4.16**.

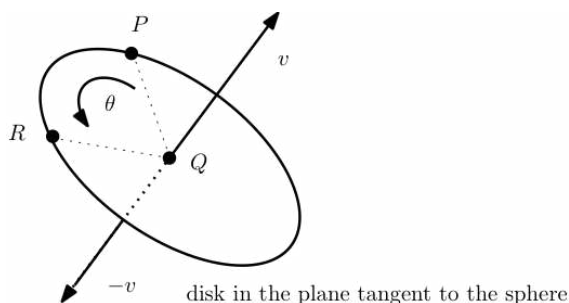


Figure 3.4.16. Two orientations on the sphere: oriented angle $\angle PQR$ is positive viewed from the outward-pointing normal vector v , but is negative viewed from the inward-pointing vector $-v$.

Corollary 3.4.17. Stereographic projection is conformal.

Stereographic projection preserves oriented angles with respect to the inward-pointing normal orientation.

Proof.

Proof sketch: Begin with the special case of curves C_1, C_2 that intersect at the south pole $S = (0, 0, -1)$. The lines L_1, L_2 that are tangent to C_1, C_2 at S lie in planes Π_1, Π_2 that contain the south pole and the origin. The tangents L_1, L_2 also lie in the plane $z = -1$ tangent to the sphere at the south pole. It is clear that the lines L'_1, L'_2 tangent to $s(C_1), s(C_2)$ at $s(S) = 0$ are straight lines that intersect at the origin. The angle made by L_1, L_2 is the same as the angle made by the planes Π_1, Π_2 , but with inward-normal orientation! See **Figure 3.4.18**. Now suppose two curves intersect at P . Choose a rotation R of S^2 that takes P to the south pole, and let $T = s \circ R \circ s^{-1}$ be the conjugate element in $\mathbf{S}$. It is clear that R and T are conformal (because T is a Möbius transformation!). Now the fact that s is conformal at $(0, 0, -1)$ implies that $s = T^{-1} \circ s \circ R$ is conformal at P .

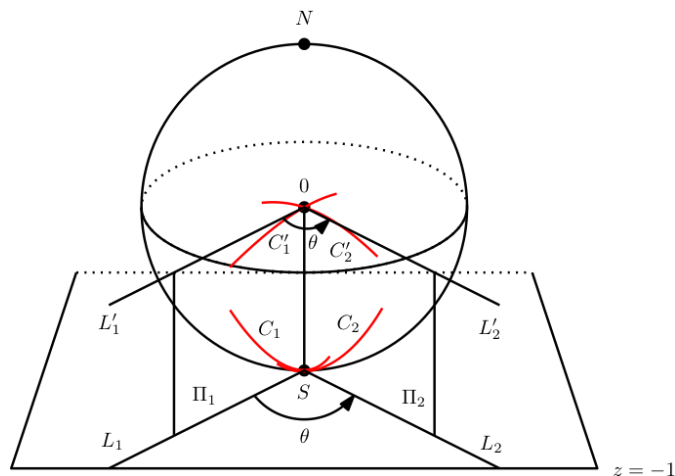


Figure 3.4.18. Stereographic projection is conformal at $S = (0, 0, -1)$.

Elliptic length and area

The distance between points P, Q on S^2 is the length of the arc of a great circle that connects them. Because the sphere has radius 1, the arc length is the same as the radian measure of the angle $\angle POQ$, where O is the origin. From vector calculus, we have the following dot product formula.

$$(\vec{OP}) \cdot (\vec{OQ}) = |\vec{OP}| |\vec{OQ}| \cos(\angle POQ)$$

Solving for $\cos(\angle POQ)$, we obtain the formula for the distance $d_{S^2}(P, Q)$ between points P, Q in S^2 .

$$d_{S^2}(P, Q) = \cos^{-1} \left((\vec{OP}) \cdot (\vec{OQ}) \right) \quad (3.4.6)$$

To "transfer" the metric (3.4.6) to $\hat{\mathbb{C}}$ by stereographic projection means that we define the elliptic metric $d_{\hat{\mathbb{C}}}$ on $\hat{\mathbb{C}}$ by the following.

$$d_{\hat{\mathbb{C}}}(p, q) := d_{S^2}(s^{-1}(p), s^{-1}(q)) \quad (3.4.7)$$

Proposition 3.4.19.

The elliptic metric (3.4.7) is invariant under the action of the elliptic group. That is, we have

$$d_{\hat{\mathbb{C}}}(p, q) = d_{\hat{\mathbb{C}}}(Tp, Tq) \quad (3.4.8)$$

for all $p, q \in \hat{\mathbb{C}}$ and for all $T \in \mathbb{S}$.

Proof.

See Exercise 3.4.7.2.

In order to obtain a formula for computing $d_{\hat{\mathbb{C}}}(p, q)$, we follow the same procedure for hyperbolic distance. First, we find the distance $d_{\hat{\mathbb{C}}}(0, u)$, where $0 \leq u \leq 1$. Let $S = (0, 0, -1) = s^{-1}(0)$ and let $U = s^{-1}(u)$. Let $O = (0, 0, 0)$, let $N = (0, 0, 1)$, let $\alpha = \angle SNU$ and let $\theta = \angle SOU$ (see Figure 3.4.20). It is a simple exercise to show that $\alpha = \theta/2$, so that we have

$$d_{\hat{\mathbb{C}}}(0, u) = d_{S^2}(S, U) = \theta = 2\alpha = 2 \arctan u. \quad (3.4.9)$$

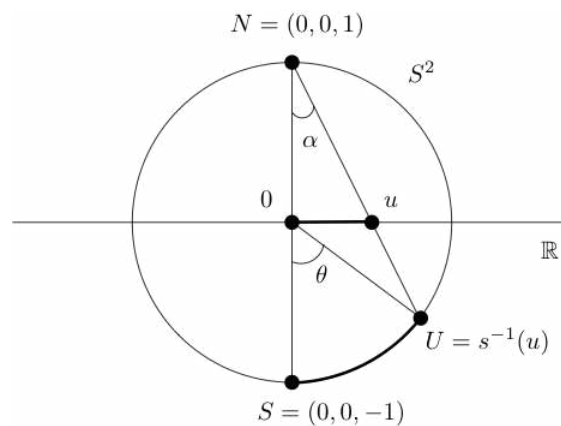


Figure 3.4.20. Transferring the natural metric on S^2 to $\hat{\mathbb{C}}$ via stereographic projection.

Checkpoint 3.4.21.

Show that $\theta/2 = \alpha = \arctan u$ in Figure 3.4.20.

For the general case, let $z_1, z_2 \in \hat{\mathbb{C}}$. Because and let $Tz = e^{it} \frac{z - z_1}{z_1^* z + 1}$ be the transformation in $\mathbf{S}$ (using the form (3.4.5)) that sends $z_1 \rightarrow 0$ and $z_2 \rightarrow u \geq 0$. Applying (3.4.9), we have the elliptic distance formula in $\hat{\mathbb{C}}$.

$$d_{\hat{\mathbb{C}}}(z_1, z_2) = 2 \arctan \left| \frac{z_2 - z_1}{z_1^* z_2 + 1} \right| \quad (3.4.10)$$

Now let γ be a parametric curve $z(t) = x(t) + iy(t)$ in $\hat{\mathbb{C}}$. Using the same argument as in the paragraph preceding the hyperbolic length integral formula (3.3.6), using the first order Taylor approximation $\arctan u \approx u$ and making the appropriate changes, we arrive at the elliptic length integral formula.

$$\text{Length}(\gamma) = 2 \int_a^b \frac{|z'(t)|}{1 + |z(t)|^2} dt \quad (3.4.11)$$

Checkpoint 3.4.22.

Show that the first order Taylor approximation for $\arctan u$ is u . Complete the details of modifying the derivation of the hyperbolic length integral formula to obtain the elliptic length integral formula.

Checkpoint 3.4.23.

Find the length of the elliptic cycle parameterized by $z(t) = \alpha e^{it}$ for $0 \leq t \leq 2\pi$, where $0 < \alpha \leq 1$

Using the same argument as in the paragraph preceding the hyperbolic area integral formula (3.3.10), using the elliptic length differential $ds = \frac{2|z'(t)| dt}{1 + |z(t)|^2}$ in place of the hyperbolic length differential and making the appropriate changes, we obtain the elliptic area integral formula.

$$\text{Area}(R) = \iint_R dA = \iint_R \frac{4r dr d\theta}{(1 + r^2)^2}. \quad (3.4.12)$$

Checkpoint 3.4.24.

Find the area of the elliptic disk $\{|z| \leq \alpha\}$, for $0 < \alpha < 1$.

Exercises

Exercise 1

Show that the three models of elliptic geometry are equivalent.

Exercise 2

Prove **Proposition 3.4.19**

Area of an elliptic triangle.

The following sequence of exercises establishes the area formula for elliptic triangles.

Exercise 3

Area of an elliptic 2-gon.

An **elliptic 2-gon** is a figure with two vertices connected by two elliptic line segments. In $\hat{\mathbb{C}}$, any 2-gon is congruent to a set of the form $R_\alpha := \{z \in \mathbb{C} : 0 \leq \arg z \leq \alpha\} \cup \{\infty\}$ for some α in the range $0 \leq \alpha < 2\pi$. See **Figure 3.4.25**. Use an area integral in $\hat{\mathbb{C}}$ to show that the area of R_α is 2α . Verify that this is the right answer using a picture of S^2 .

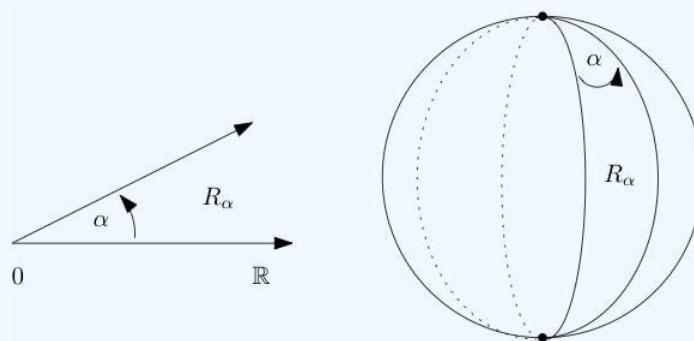


Figure 3.4.25. 2-gons in $\hat{\mathbb{C}}$ and S^2 .

Exercise 4

Area of an elliptic triangle.

Let $\triangle ABC$ be an elliptic triangle. Let $\mathcal{C}_{AB}, \mathcal{C}_{AC}, \mathcal{C}_{BC}$ denote the great circles that extend the sides AB, AC, BC of the triangle. See **Figure 3.4.26**.

1. Explain why A, A' are endpoints of the same diameter, that is, endpoints of a diameter of S^2 or their stereographic projections in $\hat{\mathbb{C}}$.
2. Explain why $\triangle A'B'C'$ has the same area as $\triangle ABC$, even though the two triangles are not necessarily congruent! (Note that the interior of $\triangle A'B'C'$ is the *exterior* of the three great circles, that is, on the side that contains the point ∞ .) Hint: What does part (a) of this problem imply about the relationship between points X and X' on S^2 for $X = A, B, C$?
3. Let R denote the interior of the region shown in the figure on the right in **Figure 3.4.26**. Explain why the area of R is

$$2\angle A + 2\angle B + 2\angle C - 2 \text{Area}(\triangle ABC).$$

Suggestion: Decompose R using overlapping 2-gons.

4. Let R' denote the exterior of the region R , that is, $R' = \hat{\mathbb{C}} \setminus R$. Explain why the area of R' is

$$2\angle A + 2\angle B + 2\angle C - 2 \text{Area}(\triangle A'B'C').$$

Suggestion: Decompose R' into overlapping 2-gons.

5. Explain why the area of elliptic triangle $\triangle ABC$ is

$$\text{Area}(\triangle ABC) = (\angle A + \angle B + \angle C) - \pi.$$

(3.4.13)

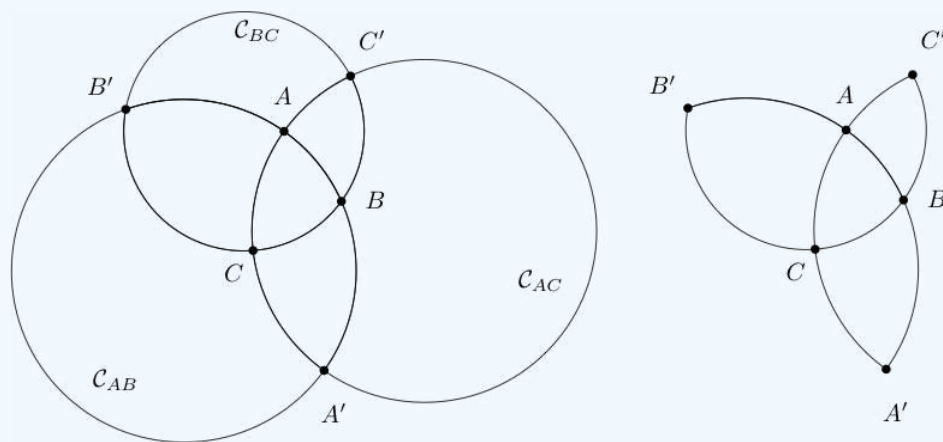


Figure 3.4.26.

This page titled 3.4: Elliptic geometry is shared under a CC BY-NC-SA 4.0 license and was authored, remixed, and/or curated by David W. Lyons via source content that was edited to the style and standards of the LibreTexts platform.

3.5: Projective Geometry

Early motivation for the development of projective geometry came from artists trying to solve practical problems in perspective drawing and painting. In this section, we present a modern Kleinian version of projective geometry.

Throughout this section, $\mathbb{F}$ is a field, V is a vector space over $\mathbb{F}$, $\mathbb{P}(V) = (V \setminus \{0\})/\mathbb{F}^*$ is the projective space, and $PGL(V) = GL(V)/\mathbb{F}^*$ is the projective transformation group. See **Exercise 2.5.3.6** for definitions and details. We will write $[T]$ for the projective transformation that is the equivalence class of the linear transformation T of V .

Projective points, lines, and flats

Points in projective space correspond bijectively to 1-dimensional subspaces of V via

$$[v] \leftrightarrow \{\alpha v : \alpha \in \mathbb{F}\}.$$

The set of 1-dimensional subspaces in V , denoted $G(1, V)$, is an alternative model space for projective geometry. We will usually denote points in projective space using capital letters, such as P, Q , etc.

A **line** in projective space is a set of the form

$$\ell_{\Pi} = \{[v] : v \in \Pi \setminus \{0\}\}$$

for some 2-dimensional subspace Π in V . Thus, projective lines correspond bijectively to 2-dimensional subspaces of V via

$$\ell_{\Pi} \leftrightarrow \Pi.$$

The set of 2-dimensional subspaces in V is denoted $G(2, V)$. Points in projective space are called **collinear** if they lie together on a projective line. We will usually denote projective lines using lower case letters, such as ℓ, m , etc.

There is an offset by 1 in the use of the word "dimension" in regards to subsets of $\mathbb{P}(V)$ and the corresponding subspace in V . In general, a **k -dimensional flat** in $\mathbb{P}(V)$ is a set of the form $\{[v] : v \in G(k+1, V)\}$, where $G(d, V)$ denotes the set of d -dimensional subspaces of V .¹ Flats are also called *subspaces* in projective space, even though projective space is not a vector space.

Points $P_1 = [v_1], P_2 = [v_2], \dots, P_k = [v_k]$ are said to be in **general position** if the vectors $v_1, v_2, \dots, v_k$ are independent in V .

Coordinates

For the remainder of this section, we consider $V = \mathbb{F}^{n+1}$. For readability, we will write $P = [v] = [x_0, x_1, x_2, \dots, x_n]$ (rather than the more cumbersome $[(x_0, x_1, x_2, \dots, x_n)]$) to denote the point in projective space that is the projective equivalence class of the point $v = (x_0, x_1, x_2, \dots, x_n)$ in $\mathbb{F}^{n+1}$. The entries x_i are called **homogeneous coordinates** of P . If $x_0 \neq 0$, then

$$P = [x_0, x_1, x_2, \dots, x_n] = \left[1, \frac{x_1}{x_0}, \frac{x_2}{x_0}, \dots, \frac{x_n}{x_0}\right].$$

The numbers x_i/x_0 for $1 \leq i \leq n$ are called **inhomogeneous coordinates** for P . The n degrees of freedom that are apparent in inhomogeneous coordinates explain why $\mathbb{P}(\mathbb{F}^{n+1})$ is called n -dimensional. Many texts write $\mathbb{FP}(n)$, $\mathbb{FP}_n$, or simply $\mathbb{P}_n$ when $\mathbb{F}$ is understood, to denote $\mathbb{P}(\mathbb{F}^{n+1})$.

Freedom in projective transformations

In an n -dimensional vector space, any n independent vectors can be mapped to any other set of n independent vectors by a linear transformation. Therefore it seems a little surprising that in n -dimensional projective space $\mathbb{FP}_n = \mathbb{P}(\mathbb{F}^{n+1})$, it is possible to map any set of $n+2$ points to any other set of $n+2$ points, provided both sets of points meet sufficient "independence" conditions. This subsection gives the details of this result, called the Fundamental Theorem of Projective Geometry.

Let $e_1, e_2, \dots, e_n, e_{n+1}$ denote the standard basis vectors for $\mathbb{F}^{n+1}$ and let $e_0 = \sum_{i=1}^{n+1} e_i$. Let $v_1, v_2, \dots, v_{n+1}$ be another basis for $\mathbb{F}^{n+1}$ and let $c_1, c_2, \dots, c_{n+1}$ be nonzero scalars. Let T be the linear transformation T of $\mathbb{F}^{n+1}$ given by $e_i \rightarrow c_i v_i$ for $1 \leq i \leq n+1$. Projectively, $[T]$ sends $[e_i] \rightarrow [v_i]$ and $[e_0] \rightarrow [\sum_i c_i v_i]$.

Now suppose there is another map $[S]$ that agrees with $[T]$ on the $n+2$ points $[e_0], [e_1], [e_2], \dots, [e_{n+1}]$. Then $[U] := [S]^{-1} \circ [T]$ fixes all the points $[e_0], [e_1], [e_2], \dots, [e_{n+1}]$. This means that $Ue_i = k_i e_i$ for some nonzero scalars $k_1, k_2, \dots, k_{n+1}$ and that $Ue_0 = k' e_0$ for some k'

$\neq 0$. This implies

$$(k_1, k_2, \dots, k_{n+1}) = (k', k', \dots, k')$$

so we have $k' = k_1 = k_2 = \dots = k_{n+1}$. Therefore $[U]$ is the identity transformation, so $[S] = [T]$. We have just proved the following existence and uniqueness lemma.

Lemma 3.5.1.

Let $v_1, v_2, \dots, v_{n+1}$ be an independent set of vectors in $\mathbb{F}^{n+1}$ and let $v_0 = \sum_{i=1}^{n+1} c_i v_i$ for some nonzero scalars $c_1, c_2, \dots, c_{n+1}$. There exists a unique projective transformation that maps $[e_i] \rightarrow [v_i]$ for $0 \leq i \leq n+1$.

Theorem 3.5.2. Fundamental Theorem of Projective Geometry.

Let $P_0, P_1, P_2, \dots, P_{n+1}$ be a set of $n+2$ points in $\mathbb{P}(\mathbb{F}^{n+1})$ such that all subsets of size $n+1$ are in general position. Let $Q_0, Q_1, Q_2, \dots, Q_{n+1}$ be another such set. There exists a unique projective transformation that maps $P_i \rightarrow Q_i$,

The real projective plane

The remainder of this section is devoted to the planar geometry $\mathbb{P}(\mathbb{R}^3) = \mathbb{RP}_2$ called the *real projective plane*. It is of historical interest because of its early practical use by artists. Lines through the origin in $\mathbb{R}^3$ model sight lines in the real world as seen from an eye placed at the origin. A plane that does not pass through the origin models the "picture plane" of the artist's canvas. **Figure 3.5.3** shows a woodcut by Albrecht Dürer that illustrates a "perspective machine" gadget used by 16th century artists to put the projective model into practice for image making.

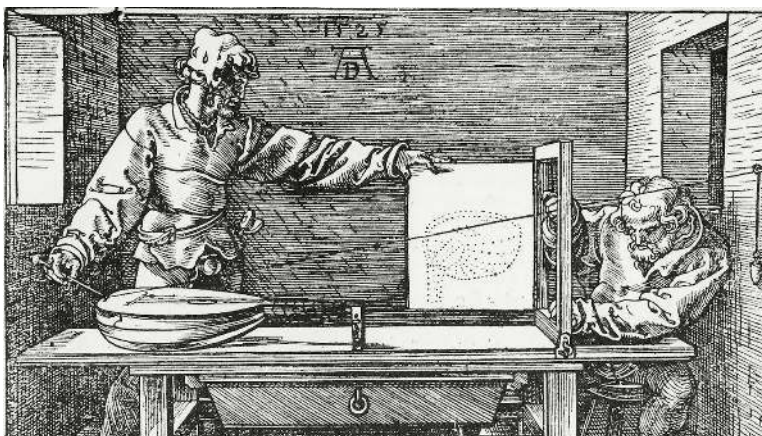


Figure 3.5.3. Man drawing a lute, Albrecht Dürer, 1525.

A two dimensional subspace Π in $\mathbb{P}^3$ is specified by a normal vector $n = (n_1, n_2, n_3)$ via the equation $n \cdot v = 0$, that is, a point $v = (x, y, z)$ lies on Π with normal vector n if and only if $n \cdot v = n_1x + n_2y + n_3z = 0$. Any nonzero multiple of n is also a normal vector for Π , so the set $G(2, \mathbb{R})$ of 2-dimensional subspaces in $\mathbb{R}^3$ is in one-to-one correspondence $\mathbb{R}^3/\mathbb{R}^*$. We will write $\ell = [n] = [n_1, n_2, n_3]$ to denote the projective line ℓ whose corresponding 2-dimensional subspace in $\mathbb{R}^3$ has normal vectors proportional to (n_1, n_2, n_3) . Beware the overloaded notation! Whether the equivalence class $[v]$ of a vector v in $\mathbb{R}^3$ denotes a projective point or a projective line has to be specified.

The equation $n \cdot v = 0$ makes sense *projectively*. This means that if $n \cdot v = 0$ for vectors n, v , then

$$(\alpha n) \cdot (\beta v) = 0 \text{ for all } \alpha, \beta \in \mathbb{F}^*, \quad (3.5.1)$$

even though the value of the dot product is *not* well-defined for projective equivalence classes! Thus we will write $\ell \cdot P = [n_1, n_2, n_3] \cdot [x, y, z] = 0$ for a projective line $\ell = [n_1, n_2, n_3]$ and a projective point $P = [x, y, z]$, to mean (3.5.1), and we make the following interpretation of the dot product as an *incidence relation* in $\mathbb{RP}_2$.

$$\ell \cdot P = 0 \Leftrightarrow P \text{ lies on } \ell \Leftrightarrow \ell \text{ contains } P. \quad (3.5.2)$$

Given two independent vectors v, w in $\mathbb{R}^3$, their cross product $v \times w$ is a normal vector for the 2-dimensional space spanned by v, w . Given two 2-dimensional subspaces Π, Σ in $\mathbb{R}^3$ with normal vectors n, m , the cross product $n \times m$ is a vector that lies along the 1-dimensional subspace $\Pi \cap \Sigma$. The bilinearity of cross product implies that cross product is well-defined on projective classes, i.e., we can write $[u] \times [v] := [u \times v]$. Thus we have the following.

Proposition 3.5.4.

Given two points $P = [u], P' = [u']$ in $\mathbb{RP}_2$, there is a unique projective line $\overline{PP'} = [u \times u']$ that contains them. Given two lines $\ell = [n], \ell' = [n']$ in $\mathbb{RP}_2$, there is a unique projective point $[n \times n']$ in their intersection $\ell \cap \ell'$.

Exercises

Exercise 1

Use **Lemma 3.5.1** to prove the Fundamental Theorem of Projective Geometry.

Exercise 2: Coordinate charts and inhomogeneous coordinates

To facilitate thinking about the interplay between the projective geometry $\mathbb{P}(\mathbb{F}^{n+1}) = \mathbb{FP}_n$ and the geometry of $\mathbb{F}^n$ (rather than $\mathbb{F}^{n+1}$!) it is useful to have a careful definition for "taking inhomogeneous coordinates in position i ". Here it is: Let U_i be the subset of $\mathbb{FP}_n$ of points whose homogeneous coordinate x_i is nonzero. Let $\pi_i: U_i \rightarrow \mathbb{F}^n$ be given by

$$[x_0, x_2, \dots, x_{i-1}, x_i, x_{i+1}, \dots, x_n] \rightarrow \left(\frac{x_0}{x_i}, \frac{x_2}{x_i}, \dots, \frac{x_{i-1}}{x_i}, \frac{x_{i+1}}{x_i}, \dots, \frac{x_n}{x_i} \right).$$

The one-sided inverse $\mathbb{F}^n \rightarrow \mathbb{FP}_n$ given by

$$(x_0, x_1, \dots, x_{i-1}, \widehat{x_i}, x_{i+1}, \dots, x_n) \rightarrow [x_0, x_1, \dots, x_{i-1}, 1, x_{i+1}, \dots, x_n]$$

(where the circumflex hat indicates a deleted item from a sequence) is called the i -th **coordinate chart** for $\mathbb{FP}_n$. What is the map that results from applying the 0-th coordinate chart $\mathbb{C} \rightarrow \mathbb{CP}_2$ followed by taking homogeneous coordinates in position 1?

Exercise 3: Möbius geometry is projective geometry

Show that Möbius geometry $(\hat{\mathbb{C}}, \mathbf{M})$ and the projective geometry $(\mathbb{P}(\mathbb{C}^2), PGL(2))$ are equivalent via the map $\mu: \mathbb{P}(\mathbb{C}^2) \rightarrow \hat{\mathbb{C}}$ given by

$$\mu([\alpha, \beta]) = \begin{cases} \alpha/\beta & \beta \neq 0 \\ \infty & \beta = 0 \end{cases}. \quad (3.5.3)$$

Comment: Observe that μ is an extension of $\pi_1: U_1 \rightarrow \mathbb{C}$ given by $\pi_1([x_0, x_1]) = \frac{x_0}{x_1}$ (defined in **Exercise 3.5.5.2**).

Exercise 4: Cross ratio

The projective space $\mathbb{P}_1 = \mathbb{P}(\mathbb{F}^2)$ is called the **projective line**. The map $\mu: \mathbb{P}_1 \rightarrow \hat{\mathbb{F}}$, given by $\mu([x_0, x_1]) = \frac{x_0}{x_1}$ (defined in **Exercise 3.5.5.3**, but where $\mathbb{F}$ may be any field, with $\hat{\mathbb{F}} = \mathbb{F} \cup \{\infty\}$) takes the points

$$[e_0] = [1, 1], [e_2] = [0, 1], [e_1] = [1, 0]$$

in $\mathbb{P}_1$ to the points $1, 0, \infty$ in $\hat{\mathbb{F}}$, respectively. Let $(\cdot, P_1, P_2, P_3)$ denote the unique projective transformation $[T]$ that takes P_1, P_2, P_3 to $[e_0], [e_2], [e_1]$. The **cross ratio** (P_0, P_1, P_2, P_3) is defined to be $\mu([T](P_0))$.

1. Show that this definition of cross ratio in projective geometry corresponds to the cross ratio of Möbius geometry for the case $\mathbb{F} = \mathbb{C}$, via the map μ , that is, show that the following holds.

$$(P_0, P_1, P_2, P_3) = (\mu(P_0), \mu(P_1), \mu(P_2), \mu(P_3))$$

2. Show that

$$(P_0, P_1, P_2, P_3) = \frac{\det(P_0 P_2) \det(P_1 P_3)}{\det(P_1 P_2) \det(P_0 P_3)}$$

where $\det(P_i P_j)$ is the determinant of the matrix $\begin{bmatrix} a_i & a_j \\ b_i & b_j \end{bmatrix}$, where $P_i = [a_i, b_i]$.

Exercise 5: Condition for collinearity in $\mathbb{RP}_2$

Let $u = (u_1, u_2, u_3), v = (v_1, v_2, v_3), w = (w_1, w_2, w_3)$ be vectors in $\mathbb{R}^3$, and let M be the matrix $M = \begin{bmatrix} u_1 & v_1 & w_1 \\ u_2 & v_2 & w_2 \\ u_3 & v_3 & w_3 \end{bmatrix}$. Show that $[u], [v], [w]$ are collinear in $\mathbb{RP}_2$ if and only if $\det M = 0$.

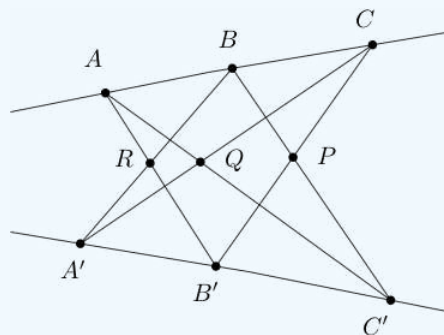


Figure 3.5.5. Pappus' Theorem

The following is a famous theorem of classical geometry.

Exercise 6: Pappus' Theorem

Let A, B, C be three distinct collinear points in $\mathbb{RP}_2$. Let A', B', C' be another three distinct collinear points on a different line. Let P, Q, R be the intersection points $P = BC' \cap B'C$, $Q = AC' \cap A'C$, $R = AB' \cap A'B$. Then points P, Q, R are collinear. See Figure 3.5.5.

Follow the outline below to prove Pappus' Theorem under the additional assumption that no three of A, A', P, R are collinear. Applying the Fundamental Theorem of Projective Geometry, we may assume $A = [e_1]$, $A' = [e_2]$, $P = [e_3]$, and $R = [e_0]$.

- Check that $AR = [0, -1, 1]$ and $A'R = [1, 0, -1]$.
- Explain why it follows that $B' = [r, 1, 1]$ and $B = [1, s, 1]$ for some r, s .
- Explain why $C = [rs, s, 1]$ and $C' = [r, rs, 1]$.
- Explain why $Q = [rs, rs, 1]$.
- Observe that P, Q, R all lie on $[1, -1, 0]$.

Hint

For the second bullet point, use the fact that $B' = [x, y, z]$ lies on AR to get $y = z$. For the third bullet point, use known coordinates for A, B, B', P to get coordinates for lines AB, PB' . Then $C = AB \cap PB'$. Use a similar process for C' . For the fourth bullet point, use $Q = AC' \cap A'C$.

Exercise 7: Quadrics

A **quadric** in $\mathbb{P}(\mathbb{F}^{n+1})$ is a set of points whose homogeneous coordinates satisfy an equation of the form

$$\sum_{0 \leq i < j \leq n} c_{ij} x_i x_j = 0. \quad (3.5.4)$$

A quadric in $\mathbb{RP}_2$ is called a **conic**.

1. Explain why (3.5.4) is a legitimate definition of a set of points in $\mathbb{P}(\mathbb{F}^{n+1})$.

2. Consider the conic $\mathcal{C}$ given by

$$x_0^2 + x_1^2 - x_2^2 = 0.$$

What are the figures in $\mathbb{R}^2$ that result from taking inhomogeneous coordinates (see **Exercise 3.5.5.2**) on $\mathcal{C}$ in positions 0, 1, 2?

This page titled [3.5: Projective Geometry](#) is shared under a [CC BY-NC-SA 4.0](#) license and was authored, remixed, and/or curated by [David W. Lyons](#) via [source content](#) that was edited to the style and standards of the LibreTexts platform.

3.6: Additional exercises

Exercises

Exercise 1

Euclidean subgroup of the Möbius group.

Let $\mathbf{E}$ denote the subgroup of the Möbius group $\mathbf{M}$ generated by rotations and translations, that is, transformations of the type $z \rightarrow e^{it}z$ for $t \in \mathbb{R}$ and $z \rightarrow z + b$ for $b \in \mathbb{C}$. The geometry $(\mathbb{C}, \mathbf{E})$ is sometimes called "Euclidean geometry". Is $(\mathbb{C}, \mathbf{E})$ equivalent to the Euclidean geometry defined in Subsection 3.1.1? Why or why not?

Exercise 2

Elliptic geometry and spherical geometry.

Is elliptic geometry $(\hat{\mathbb{C}}, \mathbf{S})$ equivalent to spherical geometry defined in Subsection 3.1.1? Why or why not?

Exercise 3

Parallel displacements in hyperbolic geometry.

Let T be an element of the hyperbolic group $\mathbf{H}$, with a single fixed point p and normal form

$$\frac{1}{Tz - p} = \frac{1}{1 - p} + \beta.$$

Show that $p\beta$ must be a pure imaginary number, that is, there must be a real number k such that $p\beta = ki$.

Exercise 4

Prove that all elements of the elliptic group $\mathbf{S}$ are elliptic in the normal form sense, i.e., we have $|\alpha| = 1$ in the normal form expression

$$\frac{Tz - p}{Tz - q} = \alpha \frac{z - p}{z - q}.$$

Suggestion: First find the fixed points p, q , then put $z = \infty$ in the normal form equation and solve for α .

Exercise 5

Alternative derivation of the formula for elliptic group elements.

To obtain an explicit formula for elements of the elliptic group, we begin with a necessary condition. Let $R = s^{-1} \circ T \circ s$ be the rotation of S^2 that lifts T via stereographic projection. If P, Q are a pair of endpoints of a diameter of S^2 , then $R(P), R(Q)$ must also be a pair of endpoints of a diameter. **Exercise 1.3.3.7** establishes the condition that two complex numbers p, q are stereographic projections of endpoints of a diameter if and only if $pq^* = -1$. Thus we have the following necessary condition for T .

$$pq^* = -1 \quad \text{implies} \quad Tp(Tq)^* = -1 \quad (3.6.1)$$

Now suppose that $Tz = \frac{az+b}{cz+d}$ with $ad - bc = 1$. Solving the equation $Tp = \frac{-1}{(T(\frac{-1}{p}))^*}$ leads to $c = -b^*$ and $d = a^*$. Thus we conclude that T has the following form.

$$Tz = \frac{az + b}{-b^*z + a^*}, \quad |a|^2 + |b|^2 = 1 \quad (3.6.2)$$

Carry out the computation to derive (3.6.2). Explain why there is no loss of generality by assuming $ad - bc = 1$.

Exercise 6

Identifications of $U(H)$ and S with $Rot(S^2)$.

The discussion of elliptic geometry (Section 3.4) establishes two ways to construct rotations from matrices. The purpose of this exercise is to reconcile these identifications. Given $a, b \in \mathbb{C}$ with $|a|^2 + |b|^2 = 1$, let us define the following objects, all parameterized by a, b .

$$\begin{aligned} M_{a,b} &= \begin{bmatrix} a & b \\ -b^* & a^* \end{bmatrix} \\ r_{a,b} &= Re(a) + Im(a)i + Re(b)j + Im(b)k \\ R_{r_{a,b}} &= [u \rightarrow r_{a,b} u r_{a,b}^*] \text{ for } u \in S_{\mathbb{H}}^2 \\ T_{a,b} &= \left[z \rightarrow \frac{az + b}{-b^*z + a^*} \right] \text{ for } z \in \hat{\mathbb{C}} \\ R_{T_{a,b}} &= s^{-1} \circ T_{a,b} \circ s \end{aligned}$$

The above objects are organized along two sequences of mappings. The rotation $R_{r_{a,b}}$ is at the end of the "quaternion path"

$$\begin{aligned} SU(2) &\rightarrow U(\mathbb{H}) \rightarrow Rot(S_{\mathbb{H}}^2) \\ M_{a,b} &\rightarrow r_{a,b} \rightarrow R_{r_{a,b}} \end{aligned} \quad (3.6.3)$$

and the rotation $R_{T_{a,b}}$ is at the end of the "Möbius path"

$$\begin{aligned} SU(2) &\rightarrow \S \rightarrow Rot(S^2) \\ M_{a,b} &\rightarrow T_{a,b} \rightarrow R_{T_{a,b}}. \end{aligned} \quad (3.6.4)$$

This problem is about comparing the rotations $R_{r_{a,b}}$ and $R_{T_{a,b}}$ (see Table 3.6.1) and reconciling the difference. The angles of rotation are the same, but the axes are different, but only by a reordering of coordinates and a minus sign.

Table 3.6.1. Axis and angle of rotation for quaternion and Möbius rotation constructions

$R_{v,\theta}$	axis of rotation v	angle of rotation θ
$R_{r_{a,b}}$	$\frac{(Im(a), Re(b), Im(b))}{\sqrt{1-(Re(a))^2}}$	$2 \arccos(Re(a))$
$R_{T_{a,b}}$	$\frac{(Im(b), -Re(b), Im(a))}{\sqrt{1-(Re(a))^2}}$	$2 \arccos(Re(a))$

The exercises outlined below verify the values for v, θ in Table 3.6.1.

1. Use **Proposition 1.2.9** to justify the values for v and θ for $R_{r_{a,b}}$ in Table 3.6.1.
2. Solve $T_{a,b}z = z$ to show that one of the fixed points of $T_{a,b}$ is

$$p = -ib \left(\frac{\sqrt{1-(Re(a))^2} + Im(a)}{|b|^2} \right).$$

3. Show that $s \left(\frac{(Im(b), -Re(b), Im(a))}{\sqrt{1-(Re(a))^2}} \right) = p$.
4. Show that

$$T_{a,b} = s \circ h \circ R_{r_{a,b}} \circ h \circ s^{-1} \quad (3.6.5)$$

where $h: \mathbb{R}^3 \rightarrow \mathbb{R}^3$ is given by $(x, y, z) \rightarrow (z, -y, x)$. Here's one way to do this: evaluate both sides of (3.6.5) on the three points $p, 0, \infty$. Explain why this is sufficient! Use quaternion multiplication to evaluate $R_{r_{a,b}}$. For example, $R_{r_{a,b}}(1, 0, 0) = r_{a,b} i r_{a,b}^*$ under the natural identification $\mathbb{R}^3 \leftrightarrow \mathbb{R}_{\mathbb{H}}^3$.

5. Here is one way to reconcile the quaternion path (3.6.3) with the Möbius path (3.6.4). Let $H = \frac{1}{\sqrt{2}} \begin{bmatrix} 1 & 1 \\ 1 & -1 \end{bmatrix}$ (the matrix H is sometimes called the *Hadamard* matrix) and let C_{iH} denote the map $M \rightarrow (iH)M(iH)^{-1}$. Show that the diagram in **Figure 3.6.2** commutes. Hint: Notice that $iH \in SU(2)$ and that $Q(iH) = \frac{1}{\sqrt{2}}(i + k)$, and that $R_{Q(iH)} = h$.

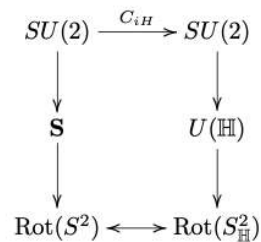


Figure 3.6.2. The map C_{iH} is given by $C_{iH}(T) = (iH)T(iH)^{-1}$. The column of maps on the left is the "Möbius path", and the column of maps on the right is the "quaternion path".

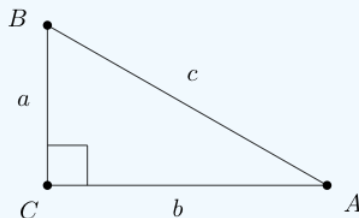


Figure 3.6.3. Right triangle $\triangle ABC$

Exercise 7

Pythagorean Theorems.

Let $\triangle ABC$ be a right triangle with right angle $\angle C$ with side lengths $a = d(B, C)$, $b = d(A, C)$, and $c = d(A, B)$ so that the length of the hypotenuse is c . See **Figure 3.6.3**.

1. Prove the following identities.

$$\cosh\left(\ln\left(\frac{1+u}{1-u}\right)\right) = \frac{1+u^2}{1-u^2} \quad (0 < u < 1) \quad (3.6.6)$$

$$\cos(2 \arctan u) = \frac{1-u^2}{1+u^2} \quad (3.6.7)$$

2. **The Hyperbolic Pythagorean Theorem.** Show that

$$\cosh(c) = \cosh(a) \cosh(b) \quad (3.6.8)$$

if T is a hyperbolic triangle.

3. **The Elliptic Pythagorean Theorem.** Show that

$$\cos(c) = \cos(a) \cos(b) \quad (3.6.9)$$

if T is an elliptic triangle.

Suggestion: Use a transformation to place C at 0 in $\mathbb{D}$ or $\hat{\mathbb{C}}$, with A is real and B pure imaginary. Use the formula $d(p, q) = \ln((1+u)/(1-u))$ with $u = \left|\frac{q-p}{1-\bar{p}q}\right|$ for hyperbolic distance. Use the formula $d(p, q) = 2 \arctan(u)$, with $u = \left|\frac{q-p}{1+\bar{p}q}\right|$ for elliptic distance. The identities from part (a) will be useful.

Index

C

circle group

[2.1: Examples of groups](#)

complex numbers

[1.1: Complex Numbers](#)

conjugate transformations

[1.3: Stereographic Projection](#)

D

dihedral group

[2.1: Examples of groups](#)

E

elliptic geometry

[3.4: Elliptic geometry](#)

elliptic group

[3.4: Elliptic geometry](#)

equivalence relation

[1.4: Equivalence Relations](#)

extended complex numbers

[1.3: Stereographic Projection](#)

F

factor group

[2.4: Group Homomorphisms](#)

G

group

[2.1: Examples of groups](#)

H

homogeneous coordinates

[3.5: Projective Geometry](#)

homomorphism

[2.4: Group Homomorphisms](#)

Hyperbolic geometry

[3.3: Hyperbolic geometry](#)

I

inhomogeneous coordinates

[3.5: Projective Geometry](#)

isomorphism

[2.4: Group Homomorphisms](#)

M

Möbius geometry

[3.2: Möbius Geometry](#)

P

Pappus' theorem

[3.5: Projective Geometry](#)

permutation

[2.1: Examples of groups](#)

projective geometry

[3.5: Projective Geometry](#)

Q

quaternion

[1.2: Quaternions](#)

quaternions

[3.4: Elliptic geometry](#)

quotient group

[2.4: Group Homomorphisms](#)

R

real projective plane

[3.5: Projective Geometry](#)

reflexive

[1.4: Equivalence Relations](#)

S

stereographic projection

[1.3: Stereographic Projection](#)

subgeometry

[3.1: Geometries and Models](#)

symmetric

[1.4: Equivalence Relations](#)

symmetric group

[2.1: Examples of groups](#)

T

transitive

[1.4: Equivalence Relations](#)

Detailed Licensing

Overview

Title: [Introduction to Groups and Geometries \(Lyons\)](#)

Webpages: 29

Applicable Restrictions: Noncommercial

All licenses found:

- [CC BY-NC-SA 4.0](#): 69% (20 pages)
- [Undeclared](#): 31% (9 pages)

By Page

- [Introduction to Groups and Geometries \(Lyons\)](#) - [CC BY-NC-SA 4.0](#)
 - [Front Matter](#) - [Undeclared](#)
 - [TitlePage](#) - [Undeclared](#)
 - [InfoPage](#) - [Undeclared](#)
 - [Table of Contents](#) - [Undeclared](#)
 - [Licensing](#) - [Undeclared](#)
 - [1: Preliminaries](#) - [CC BY-NC-SA 4.0](#)
 - [1.1: Complex Numbers](#) - [CC BY-NC-SA 4.0](#)
 - [1.2: Quaternions](#) - [CC BY-NC-SA 4.0](#)
 - [1.3: Stereographic Projection](#) - [CC BY-NC-SA 4.0](#)
 - [1.4: Equivalence Relations](#) - [CC BY-NC-SA 4.0](#)
 - [2: Groups](#) - [CC BY-NC-SA 4.0](#)
 - [2.1: Examples of groups](#) - [CC BY-NC-SA 4.0](#)
 - [2.2: Definition of a group](#) - [CC BY-NC-SA 4.0](#)
 - [2.3: Subgroups and Cosets](#) - [CC BY-NC-SA 4.0](#)
 - [2.4: Group Homomorphisms](#) - [CC BY-NC-SA 4.0](#)
 - [2.5: Group Actions](#) - [CC BY-NC-SA 4.0](#)
 - [2.6: Additional exercises](#) - [CC BY-NC-SA 4.0](#)
 - [3: Geometries](#) - [CC BY-NC-SA 4.0](#)
 - [3.1: Geometries and Models](#) - [CC BY-NC-SA 4.0](#)
 - [3.2: Möbius Geometry](#) - [CC BY-NC-SA 4.0](#)
 - [3.3: Hyperbolic geometry](#) - [CC BY-NC-SA 4.0](#)
 - [3.4: Elliptic geometry](#) - [CC BY-NC-SA 4.0](#)
 - [3.5: Projective Geometry](#) - [CC BY-NC-SA 4.0](#)
 - [3.6: Additional exercises](#) - [CC BY-NC-SA 4.0](#)
 - [Back Matter](#) - [Undeclared](#)
 - [Index](#) - [Undeclared](#)
 - [Glossary](#) - [Undeclared](#)
 - [Detailed Licensing](#) - [Undeclared](#)