Math 120A — Introduction to Group Theory

Neil Donaldson

Fall 2018

Text

- *An Introduction to Abstract Algebra*, John Fraleigh, 7th Ed 2003, Adison–Wesley (optional).
- Also check the library for entries under "Group Theory" and "(Abstract) Algebra". There have been a plethora of textbooks written for Undergraduate group theory courses and the first few chapters of most of them will cover similar ground to the core text.

1 Introduction: what is abstract algebra and why study groups?

To be *abstract* is to remove context and application and study the *structure* of something. Abstract mathematics essentially involves studying the patterns and symmetries inherent in the real world from an abstract viewpoint so as to see the commonalities between structures in seemingly distinct places: we shall see an example of a common structure shortly.

A *group* is one of the simplest algebraic structures. This in itself is a good reason to study groups: they are (relatively) easy! Indeed you have been working with groups for years: a group is a set with one operation (like the real numbers $\mathbb{R}$ with $+$) that has a small number of additional properties.[1] Since there is only one operation, the number of options is very limited. Sometimes *doing the only thing you can* will lead you to a correct proof!

The real reason to study groups is that they have wide applications. For instance:

Geometry A large part of modern Geometry involves the study of groups — surfaces, polyhedra, the set of lines in a vector space — these sets have many different groups associated to them which help the geometer describe and classify them.

Combinatorics When studying collections of objects, groups of permutations (reorderings) of sets are widely used.

Galois Theory Groups describe symmetries in the roots of polynomial equations.

Chemistry Groups are used to describe the symmetries of molecules and of crystalline substances.

Physics Materials science sees group theory similarly to Chemistry, while modern theories of the nature of the Universe (e.g. string theory) rely heavily on groups.

[1] You are already familiar with objects far more complicated than this (e.g. $\mathbb{R}$ with the two operations $+, \cdot$ is a *field*, $(\mathbb{R}^n, +, \cdot)$ is a *vector space*, the set of equivalence classes modulo six $(\mathbb{Z}_6, +_6, \cdot_6)$ is a *ring*.

Motivational example

What do an equilateral triangle and an arbitrary collection $\{1,2,3\}$ of three objects have in common? The obvious answer is the number *three,* but we can say a lot more. Both objects have *symmetries*: rotations and reflections of the triangle and permutations of the set $\{1,2,3\}$. Considering *compositions* of these symmetries, we will see that they are essentially the *same*.

Permuations of $\{1,2,3\}$ These can be written in *cycle notation*:[2] for example, the cycle (12) represents swapping 1 and 2 and leaving 3 alone. For instance, as functions,

$$(12): \begin{cases} 1 \mapsto 2 \\ 2 \mapsto 1 \\ 3 \mapsto 3 \end{cases} \qquad \text{and} \qquad (123): \begin{cases} 1 \mapsto 2 \\ 2 \mapsto 3 \\ 3 \mapsto 1 \end{cases}$$

It is not hard to convince yourself that there are six distinct permutations of $\{1,2,3\}$: for brevity, we will use the symbols $e, \mu_1, \mu_2, \mu_3, \rho_1, \rho_2$.

Identity: leave everything alone	Swap two numbers	Permute all three
$e = ()$	$\mu_1 = (23)$	$\rho_1 = (123)$
	$\mu_2 = (13)$	$\rho_2 = (132)$
	$\mu_3 = (12)$	

We can compose these permutations. For instance

$$\mu_1 \circ \rho_2 = (23)(132): \begin{cases} 1 \mapsto 3 \mapsto 2 \\ 2 \mapsto 1 \mapsto 1 \\ 3 \mapsto 2 \mapsto 3 \end{cases}$$

The result is the same as that obtained by the permutation $(12) = \mu_3$, whence we write

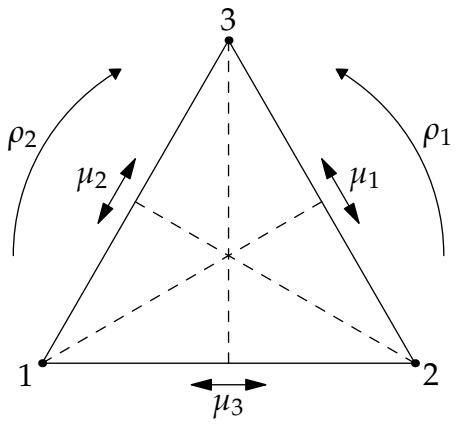
$$\mu_1 \circ \rho_2 = \mu_3$$

The full list of compositions of the symmetries is shown in the following table: read the left column first, then the top row: our previous calculation is shown in red.

$\circ$	e	ρ_1	ρ_2	μ_1	μ_2	μ_3
e	e	ρ_1	ρ_2	μ_1	μ_2	μ_3
ρ_1	ρ_1	ρ_2	e	μ_3	μ_1	μ_2
ρ_2	ρ_2	e	ρ_1	μ_2	μ_3	μ_1
μ_1	μ_1	μ_2	μ_3	e	ρ_1	ρ_2
μ_2	μ_2	μ_3	μ_1	ρ_2	e	ρ_1
μ_3	μ_3	μ_1	μ_2	ρ_1	ρ_2	e

[2] We will return to this notation later so don't feel you have to be an expert on it now. The permutation (12) is known as a *2-cycle* because it permutes two objects. The permutation (123) is similarly referred to as a *3-cycle.*

The Equilateral Triangle What does all this have to do with a triangle? If we label the vertices of an equilateral triangle 1,2,3, then the above permutations correspond to symmetries of the triangle: ρ_1 and ρ_2 are rotations, while each μ_i performs a reflection in the altitude through the vertex i. The two sets of symmetries apply to different objects, but their interactions are identical.



One might obtain intuition about the permutations of $\{1, 2, 3\}$ by viewing them as symmetries of a triangle. In particular, there is a qualitative difference between the *rotations* ρ_1, ρ_2 and the *reflections* μ_1, μ_2, μ_3. That composition of reflections produces a rotation is clear in the triangle setting. That composition of 2-cycles makes a 3-cycle is not so clear.

Group theory is about ideas like this: in group theory the symmetries and patterns associated to objects are more important than the objects themselves and can lead to unexpected connections. In this introduction we considered two groups:

S_3: the *symmetric group* on three letters/permutations of $\{1, 2, 3\}$.

D_3: the *dihedral group* of order six/symmetries of the equilateral triangle.

The fact that the resulting structures are identical will be written $S_3 \cong D_3$, and we will say that these groups are *isomorphic*.[3]

2 Groups

2.1 The Axioms of a Group

We start by defining our main objects of study.

Definition 2.1. A (*multiplicative*) *group* is a set G with the following properties.

Closure There exists a function $\cdot : G \times G \to G$. This type of function is also termed a *binary operation*. Abstractly, the closure axiom states that

$$\forall g, h \in G,\ g \cdot h \in G$$

Associativity $\forall g, h, j \in G,\ g \cdot (h \cdot j) = (g \cdot h) \cdot j$.

Identity $\exists e \in G$ such that $\forall g \in G,\ e \cdot g = g \cdot e = g$.

Inverse $\forall g \in G,\ \exists g^{-1} \in G$ such that $g \cdot g^{-1} = g^{-1} \cdot g = e$.

Additionally, a group is *abelian* if the group operation is commutative:[4]

$$\forall g, h \in G,\ g \cdot h = h \cdot g$$

[3] We will explain the term *isomorphic* more concretely later on and revisit both examples. Also observe that was use the congruence symbol $\cong$ to denote isomorphic groups: you should think about why this makes sense...

[4] In honor of the Norwegian mathematician Niels Abel, one of the godfathers of pure mathematics.

Example The simplest example of a group, given the above notation, is the set of positive real numbers $\mathbb{R}^+ = (0, \infty)$ equipped with multipliction. You should mentally check each of the above axioms.[5]

Closure If $x > 0$ and $y > 0$, then $xy > 0$.

Associativity We are used to writing xyz for a product of three real numbers. This reflects the fact that multiplication of numbers is associative.

Identity 1 is a positive real number, and certainly satisfies $1 \cdot x = x \cdot 1 = x$ for all x.

Inverse If $x > 0$, then $x^{-1} = \frac{1}{x}$ is also a well-defined positive real number.

In fact the positive reals under multiplication is an *abelian* group, since multiplication of real numbers is also commutative.

Notation and Conventions Formally, a group is often written as a pair $(G, \cdot)$ in order to stress the operation. It is possible for a given set to form a group un many different ways, so this is important. However, most of the time the operation is understood by all readers and so it can be omitted.

Abstract groups are commonly written *multiplicatively,* as in the above definition. The group operation can then be written as *juxtaposition,* i.e. $g \cdot h = gh$.

In a multiplicative group the power notation is a convenient short-hand:

$$a^n = \underbrace{a \cdots a}_{n\text{times}} \qquad \text{and} \qquad a^{-n} = (a^{-1})^n = (a^n)^{-1}$$

Exponents follow the usual additive law $a^n a^m = a^{m+n}$. We also write $a^0 = e$.

Groups can also be written *additively,* using $+$ as the symbol for the binary operaation. This is especially common for abstract abelian groups. In such cases we use minus $(-)$ for the inverse. For example, in the group $(\mathbb{Z}, +)$, the expression $2 - 3 = -1$ is a shorthand for

$$2 + (-3) = -1 : \quad \text{2 plus the } \textit{inverse} \text{ of 3 is the inverse of 1!}$$

Being precise about this is extremely tedious, so everyone just says 'two minus three' as usual.

In an additive group, multiplicaton becomes a shorthand for repeated additions: e.g. $3x = x + x + x$.

If a group is non-abstract—you have an *explicit* set and operation—you should use the correct symbol for the operation!

Easy Examples

1. The sets $\mathbb{C}, \mathbb{R}, \mathbb{Q}, \mathbb{Z}$ are abelian groups under addition:
   Check All are closed under addition ✓
   Addition is associative ✓
   0 is the additive identity: $0 + x = x + 0 = x$ ✓
   The inverse of x is $-x$ ✓

[5] It is not really possible to *prove* most of these, since (arguably) these axioms are part of the *definition* of the real numbers! This is common for elementary groups: try to get in the habit of mentally checking the axioms, even if you feel like a formal proof is essentially impossible.

2. The non-zero elements in $\mathbb{C}, \mathbb{R}, \mathbb{Q}$ form abelian groups under multiplication.
   Check Closure: $x, y \neq 0 \implies xy \neq 0$ ✓
   Multiplication of numbers is associative ✓
   $1 \in \mathbb{Q} \subseteq \mathbb{R} \subseteq \mathbb{C}$ is the multiplicative identity: $1 \cdot x = x \cdot 1 = x$ ✓
   The inverse of x is $x^{-1} = \frac{1}{x}$, which lies in $\mathbb{C}, \mathbb{R}, \mathbb{Q}$ if n does ✓
   These groups are often denoted $\mathbb{R}^\times, \mathbb{C}^\times, \mathbb{Q}^\times$, etc.

3. Vector spaces: any vector space is an abelian group under addition. Note that this includes the set of $m \times n$ matrices under addition, since this is really an $m \times n$-dimensional vector space.

4. The set $2\mathbb{Z}$ of *even* integers forms an abelian group under addition. More generally, the multiples of n, labelled $n\mathbb{Z}$ forms an abelian group for any integer n.

Easy Non-examples

1. The set of *all* real numbers $\mathbb{R}$ (as opposed to $\mathbb{R}^\times = \mathbb{R} \setminus \{0\}$) does not form a group under multiplication. $(\mathbb{R}, \cdot)$ is closed, associative and has the identity element 1, but the single element 0 has no inverse: $\nexists r \in \mathbb{R}$ such that $0 \cdot r = r \cdot 0 = 1$.
   Similarly $(\mathbb{Q}, \cdot)$ and $(\mathbb{C}, \cdot)$ are *not* groups because of the non-invertibility of 0.

2. The set of *odd* integers $1 + 2\mathbb{Z} = \{1 + 2n : n \in \mathbb{Z}\}$ is not a group under addition since it is not closed: for instance, $1 + 1 = 2 \notin 1 + 2\mathbb{Z}$.

3. The set of natural numbers $\mathbb{N} = \{1, 2, 3, \ldots\}$ is not a group under addition. It is closed and satisfies associativity, but does not have an identity: $0 \notin \mathbb{N}$. Without an identity, the inverse axiom makes no sense.

4. $\mathbb{R}^3$ with cross/vector product $\times$. This is closed, but not associative, for example

   $$\mathbf{i} \times (\mathbf{i} \times \mathbf{j}) = \mathbf{i} \times \mathbf{k} = -\mathbf{j} \neq \mathbf{0} = (\mathbf{i} \times \mathbf{i}) \times \mathbf{j}$$

   There is also no identity element: if $\mathbf{e} \in \mathbb{R}^3$ were the identity, then we'd have to have

   $$\mathbf{e} \times \mathbf{i} = \mathbf{i}$$

   However, recall that $\mathbf{v} \times \mathbf{w}$ is orthogonal to *both* $\mathbf{v}$ and $\mathbf{w}$, whence $\mathbf{i}$ would have to be orthogonal to itself: contradiction! With no identity, there can be no inverses either.

5. $(\mathbb{Q}, *)$ with $a * b = \frac{a}{b}$ is not a group: it fails the closure axiom since $a * 0$ is undefined for all a.

6. Let $\mathcal{M} = \{2 \times 2 \text{ matrices with determinant } 7\}$ with $A * B = AB$ being matrix multiplication. Since $\det(AB) = \det A \det B$, it follows that $\det(A * B) = 49$ and so $A * B \notin \mathcal{M}$. Thus $*$ is not a binary operation on $\mathcal{M}$ and the closure axiom fails.

There are many, many more examples and non-examples. It is worth treating a couple of these more slowly.

The group of remainders modulo n

Modular arithmetic provides an important family of groups. For the present, we will take the following definition:

Definition 2.2. $\mathbb{Z}_n = \{0, 1, 2, 3 \ldots, n-1\}$ is the set of remainders modulo n.

Theorem 2.3. *The binary operation '+ modulo n' defines an abelian group structure on $\mathbb{Z}_n$.*

Proof. *Closure* If $x, y \in \mathbb{Z}_n$, then $x + y \mod n$ is a remainder modulo n, and thus lies in $\mathbb{Z}_n$.

Associativity This is tedious: for the purposes of this calculation, we write $x +_n y$ instead of $x + y \mod n$. Let $x, y, z \in \mathbb{Z}$ and observe first that

$$x +_n y = \begin{cases} x + y & \text{if } x + y < n \\ x + y - n & \text{if } x + y \geq n \end{cases}$$

Therefore

$$(x +_n y) +_n z = \begin{cases} x + y & \text{if } x + y + z < n \\ x + y + z - n & \text{if } x + y \geq n \text{ and } x + y + z < 2n \\ x + y + z - 2n & \text{if } x + y + z \geq 2n \end{cases}$$

In each case, we simply obtain $(x +_n y) +_n z$ as the remainder when $x + y + z$ is divided by n. There is no difference when computing $x +_n (y_n + z_n)$. Indeed we are using the fact that $+$ is associative on $\mathbb{Z}$.

Identity $0 \in \mathbb{Z}_n$ satisfies $0 + x \equiv x + 0 \equiv x \mod n$ for all $x \in \mathbb{Z}_n$.

Inverse $-x \equiv n - x$ is the inverse of $x \in \mathbb{Z}_n$.

Commutativity $x + y \equiv y + x \mod n$ for all $x, y \in \mathbb{Z}_n$. ∎

You should find the above discussion really ugly! Later in the term, we shall properly encounter $\mathbb{Z}_n$ as a factor group. In particular, recall that congruence modulo n is an equivalence relation[6] on the integers $\mathbb{Z}$:

$$x \sim y \iff x \equiv y \mod n$$

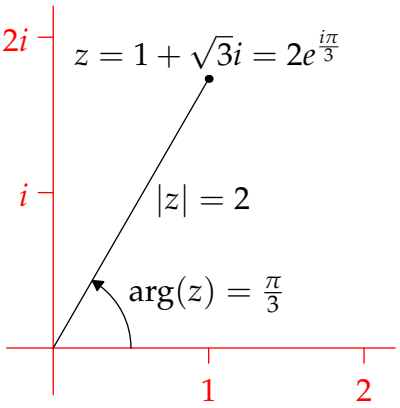
If $[x] = \{x + \lambda n : \lambda \in \mathbb{Z}\}$ is the equivalence class of $x \in \mathbb{Z}$, then we can define

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

In a previous course, you proved that $+_n$ is well-defined. Properly speaking $\mathbb{Z}_n$ is the set of equivalence classes $\mathbb{Z}/\sim = \{[x] : x \in \mathbb{Z}\}$ with respect to the operation $+_n$. In this language, it becomes really easy to see that $\mathbb{Z}_n$ is a group!

[6] Recall that an equivalence relation is *reflexive* $x \sim x$, *symmetric* $x \sim y \implies y \sim x$, and *transitive* $x \sim y$ and $y \sim z \implies x \sim z$. Moreover, recall that the equivalence classes of $\sim$ *partition* the big set $\mathbb{Z}_n$. In this case, every integer x lies in precisely one equivalence class of remainders $[x] = \{x + \lambda n : \lambda \in \mathbb{Z}\}$.

The circle group and the roots of unity: a primer on the complex numbers



Recall that $\mathbb{C} = \{x + iy : x, y \in \mathbb{R}\}$ where i is a 'number' satisfying $i^2 = -1$. The complex numbers may be represented using an *Argand diagram*, essentially as the vector space $\mathbb{R}^2$ spanned by the basis $\{1, i\}$. Given a complex number $z = x + iy$, we can consider several objects:

- The *complex conjugate* $\overline{z} = x - iy$.
- The *modulus* $|z| = \sqrt{z\overline{z}} = \sqrt{x^2 + y^2}$.
- The *argument* $\arg z$ is the angle made by the vector $\binom{x}{y}$ with the positive x-axis.
- The *polar form* is $|z|\, e^{i \arg(z)}$.

The polar form is nothing more than using standard polar co-ordinates to describe points on the Argand diagram. The primary non-trivial aspect of this is the *complex exponential*, which may be computed using *Euler's formula*:[7]

$$e^{i\theta} = \cos\theta + i \sin\theta$$

which is the source of the famous identity $e^{i\pi} = -1$. A quick computation with the polar form allows one to check the following:

Lemma 2.4. *Suppose that $z, w \in \mathbb{C}$. Then*

- $|zw| = |z|\,|w|$.
- $\arg(zw) \equiv \arg(z) + \arg(w) \mod 2\pi$.

Definition 2.5. The *circle group* S^1 is the set

$$S^1 = \{e^{i\theta} : \theta \in [0, 2\pi)\}$$

under multiplication. This group is abelian.

You should easily be able to run through the group axioms yourself: in particular $e^{i\theta}e^{i\psi} = e^{i(\theta+\psi)}$ does most of the work.

Definition 2.6. Let $n \in \mathbb{N}_{\geq 2}$. The n^{th} roots of unity[8] are the (complex) solutions to the equation $z^n = 1$.

For example, the square-roots of unity are ± 1. Thanks to Euler's formula, we can easily describe the n^{th} roots.

Theorem 2.7. *Suppose that n is fixed and let $\zeta = e^{\frac{2\pi i}{n}}$. Then the n^{th} roots of unity are precisely the values*

$$1, \zeta, \zeta^2, \cdots, \zeta^{n-1}$$

[7] More generally, $e^{x+iy} = e^x e^{iy} = e^x \cos y + ie^x \sin y$. To prove Euler's formula, one can either use differential equations or Maclaruin series (after assuming that these make sense for complex numbers).

[8] In this context, *unity* is simply a pretentious term for the number 1.

Proof. We find all the solutions to the equation $z^n = 1$. Take the modulus of both sides to obtain $|z|^n = 1$. Since $|z|$ is a positive real number (it certainly can't be zero!), the only solution is $|z| = 1$. The polar form is therefore $z = e^{i\theta}$. Now compute:

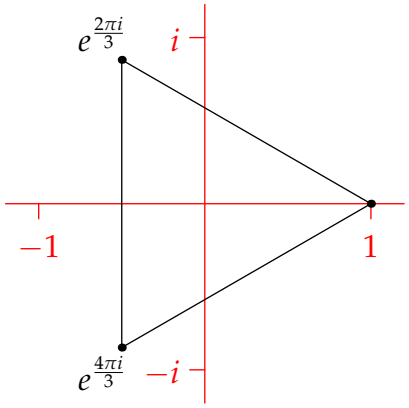
$$1 = z^n = (e^{i\theta})^n = e^{in\theta} \iff n\theta = 2\pi k$$

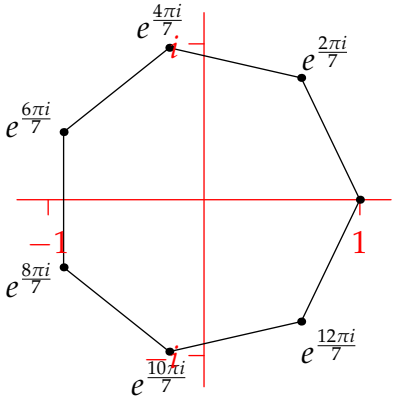
for some integer k. Thus $\theta = \frac{2\pi k}{n}$ and so

$$z = e^{i\theta} = e^{\frac{2\pi i}{n}k} = \left(e^{\frac{2\pi i}{n}}\right)^k = \zeta^k$$

■

The n^{th} roots are equally spaced around the unit circle, forming the corners of a regular n-gon centered at the origin, with one corner at 1.





Why are we interested in the n^{th} roots? Because they are *closed under multiplication*: $\zeta^k \cdot \zeta^l = \zeta^{k+l}$. Indeed:

Theorem 2.8. *The set U_n of n^{th} roots of unity form an abelian group under multiplication.*

In fact this is really just $\mathbb{Z}_n$ in disguise! Consider the function

$$\mu : \mathbb{Z}_n \to U_n : x \mapsto \zeta^x$$

This satisfies two important properties:

- If is *bijective*.
- $\mu(x + y) = \mu(x) \cdot \mu(y)$.

The first property merely says that U_n is a relabelling of $\mathbb{Z}_n$. The second property is far more interesting. It says that the *binary/group structures* of the sets are related. In particular, given two elements $x, y \in \mathbb{Z}_n$ we can do two things:

1. Combine (add) $x + y$ in $\mathbb{Z}_n$ then map (using μ) U_n.
2. Map both x, y to U_n and then combine (multiply) in U_n.

We are *guaranteed always to get the same result!* This is such an important idea that it merits some terminology.

Definition 2.9. Suppose that $(G, \cdot)$ and $(H, \star)$ are binary structures (in this course, almost always groups) and that $\phi : G \to H$. We say that ϕ is a *homomorphism* if

$$\forall x, y \in G,\ \phi(x \cdot y) = \phi(x) \star \phi(y)$$

Additionally, if ϕ is bijective,[9] we say that it is an *isomorphism.* If there exists an isomorphism ϕ, we say that $(G, \cdot)$ and $(H, \star)$ are *isomorphic binary structures (groups),*[10] and write $G \cong H$.

We will see many, many more examples of homo- and isomorphisms later!

Associativity

When checking the group axioms for a given example, typically the associativity axiom is the most troublesome. In practice, you can almost always avoid a nasty calculation using one of the following two approaches.

Restriction to a subset If H is a subset of G and you know that $\cdot$ is associative on G, then it is automatically associative on H. Look back at the associativity axiom: unlike the closure axiom, there is no requirement for $x(yz)$ to lie in any particular subset! For instance, you know that $\cdot$ is associative on $\mathbb{R}$, indeed this is part of the definition of the real numbers and so cannot strictly be proved, thus $\cdot$ is associative on any subset such as $\mathbb{Q}, \mathbb{Z}, 4\mathbb{Z}$, etc.

Composition of functions If you can recognize your binary operation as some sort of composition of functions, then the next result clears everything up for you!

Theorem 2.10. *Let V be any set. Composition of functions $f : V \to V$ is associative.*
If V has at least 2 elements, then composition is non-commutative.

Proof. We need to prove that for all functions $f, g, h : V \to V$ we have $(f \circ g) \circ h = f \circ (g \circ h)$. Two functions are equal if and only if they do the same thing to every element $x \in V$. Now

$$((f \circ g) \circ h)(x) = (f \circ g)(h(x)) = f(g(h(x))) \quad \text{and,}$$
$$(f \circ (g \circ h))(x) = f((g \circ h)(x)) = f(g(h(x)))$$

Thus $\circ$ is associative. Showing non-commutativity is an exercise. ∎

The challenge in applying the theorem is to be able to view a binary operation as a composition of functions. Doing this is not always easy! Here are three more important families of groups.

Symmetric groups The symmetric group S_n is the set of permutations of a set of n elements. Typically we take the set of bijective functions

$$\sigma : \{1, 2, \ldots, n\} \to \{1, 2, \ldots, n\}$$

This is easily see to be a group under composition of functions.

[9] Recall the definitions: A function $\phi : G \to H$ is said to be;

- *injective/1–1* if $\phi(x) = \phi(y) \implies x = y$ for all $x, y \in G$.
- *surjective/onto* if $\text{range}(\phi) = H$.
- *bijective* if it is both injective and surjective.

[10] If two structures are isomorphic, there likely exist several different isomorphisms. There are alternative notations for when you want to stress the particular isomorphism, for instance $\phi : G \cong H$ or $\phi : G \xrightarrow{\cong} H$.

Closure The composition of bijective functions is bijective.

Associativity This is just Theorem 2.10.

Identity The identity function is $e : x \mapsto x$ for all $x \in \{1, 2, \ldots, n\}$.

Inverse Since every $\sigma \in S_n$ is bijective, it has an inverse function: clearly $\sigma \circ \sigma^{-1} = e$.

Dihedral (and geometric-symmetry) groups The set of symmetries of any geometric figure forms a group under composition. By *symmetry* we consider a function from the set of all possible configurations of the figure to itself. In this sense, the group operation is composition of functions and associativity follows from the Theorem.
The *dihedral group* D_n is the special case of the symmetries of a regular n-sided polygon.

Matrix groups There are many examples of groups of matrices *under multiplication.* The easiest example is the *general linear group*

$$\mathrm{GL}_n(\mathbb{R}) = \{n \times n \text{ matrices with non-zero determinant}\}$$

You should have done all the relevant work in a basic linear algebra course: the closure and inverse axioms follow from the familiar result on determinants

$$\det(AB) = \det A \det B$$

In the presence of a basis, matrix multiplication by a square matrix corresponds to the action of a linear map (a function) on a vector space. Multiplying matrices corresponds to composition of linear maps. Combining this with Theorem 2.10 results in the following:

Corollary 2.11. *Matrix multiplication of square matrices is associative and non-commutative.*

Aside: Bases and Linear Maps If the above discussion is too rapid, consider and example. Let $V = \mathbb{R}^2$, then the square matrix $A = \begin{pmatrix} 1 & 3 \\ 2 & -1 \end{pmatrix}$ describes a linear map $L_A : \mathbb{R}^2 \to \mathbb{R}^2$ by

$$L_A : \begin{pmatrix} x \\ y \end{pmatrix} \mapsto \begin{pmatrix} 1 & 3 \\ 2 & -1 \end{pmatrix} \begin{pmatrix} x \\ y \end{pmatrix} = \begin{pmatrix} x + 3y \\ 2x - y \end{pmatrix}$$

Conversely, the linear map defined by

$$L_B : \begin{pmatrix} x \\ y \end{pmatrix} \mapsto \begin{pmatrix} 2x + 7y \\ -x + 3y \end{pmatrix}$$

has matrix $B = \begin{pmatrix} 2 & 7 \\ -1 & 3 \end{pmatrix}$. The matrix of the linear map $L_A \circ L_B$ is precisely the matrix AB: observe

$$L_A \circ L_B : \begin{pmatrix} x \\ y \end{pmatrix} \mapsto L_A \begin{pmatrix} 2x + 7y \\ -x + 3y \end{pmatrix} = \begin{pmatrix} (2x + 7y) + 3(-x + 3y) \\ 2(2x + 7y) - (-x + 3y) \end{pmatrix} = \begin{pmatrix} -x + 16y \\ 5x + 11y \end{pmatrix} = AB \begin{pmatrix} x \\ y \end{pmatrix}$$

In this way, matrix multiplication of 2×2 real matrices, corresponds precisely to the composition of linear maps on $\mathbb{R}^2$.

The correspondence holds in general, if $\mathcal{B} = \{\mathbf{e}_1, \ldots, \mathbf{e}_n\}$ is a basis of a vector field V, then a linear map $L : V \to V$ has matrix

$$[L]_{\mathcal{B}} = \big([L(\mathbf{e}_1)]_{\mathcal{B}} \cdots [L(\mathbf{e}_n)]_{\mathcal{B}}\big)$$

with respect to $\mathcal{B}$. That is, the j^{th} column of $[L]$ is the co-ordinate vector of $L(\mathbf{e}_j)$ with respect to $\mathcal{B}$. If L_1, L_2 are linear maps then their matrices satisfy

$$[L_1 \circ L_2]_{\mathcal{B}} = [L_1]_{\mathcal{B}} \circ [L_2]_{\mathcal{B}}$$

If you haven't already done so, you will eventually prove this in a linear algebra course.

You might instead try to prove the Corollary directly using sigma-notation or the Einstein summation convention, though the mess of indices is not for the faint-hearted.
If a_{ij}, etc., denotes the i^{th} row, j^{th} column of an $n \times n$ matrix A, then

$$(AB)_{ik} = \sum_{j=1}^{n} a_{ij}b_{jk} \implies \big((AB)C\big)_{il} = \sum_{k=1}^{n}\left(\sum_{j=1}^{n} a_{ij}b_{jk}\right)c_{kl} = \sum_{j,k=1}^{n}(a_{ij}b_{jk})c_{kl}$$
$$= \sum_{j,k=1}^{n} a_{ij}(b_{jk}c_{kl}) = \sum_{j=1}^{n} a_{ij}\left(\sum_{k=1}^{n} b_{jk}c_{kl}\right) = \big(A(BC)\big)_{il}$$

Since the il^{th} entries are equal (by the associativity of $(\mathbb{R}, \cdot)$) we conclude that $(AB)C = A(BC)$.

More generally, both Theorem 2.10 and Corollary 2.11 hold for any functions f and for multiplication of non-square matrices, provided that composition/multiplication is defined.

Basic Results for Groups The most simplest statements regarding groups rely on nothing beyond the definition. The first issue is one of grammar. The inverse axiom says that a binary structure need have *at least one* inverse. We'd like to be able to say *the* inverse rather than using the indefinite article *an.* Our first result clears this up, not only for indentites, but for inverses as well.

Theorem 2.12 (Uniqueness of Identities and Inverses)**.**

1. *In any binary structure $(G, \cdot)$, if $e \in G$ is an identity, then it is unique.*
2. *If $(G, \cdot)$ is a group, then inverses are unqiue.*

Proof. 1. Suppose that $e, \hat{e} \in G$ are identities. Then

$$e * \hat{e} = \begin{cases} \hat{e} & \text{since } e \text{ is an identity} \\ e & \text{since } \hat{e} \text{ is an identity} \end{cases}$$

In particular, $\hat{e} = e$.

2. Suppose that x has two inverses $y \neq z$. Then, by associativity,

$$\begin{aligned} y(xz) = (yx)z &\implies ye = ez && \text{(since } y, z \textit{ both} \text{ inverses of } x\text{)} \\ &\implies y = z && \text{(identity axiom)} \end{aligned}$$

Again we have a contradiction.[11]

■

Corollary 2.13 (Cancellation laws & Inverses)**.** *In any group G we have:*

1. $xy = xz \implies y = z$
2. $yx = zx \implies y = z$
3. $(xy)^{-1} = y^{-1}x^{-1}$

Proof. The first two statements are immediate—just multiply on the left (resp. right) by x^{-1}. For part (c), note that

$$y^{-1}x^{-1}(xy) = y^{-1}(x^{-1}x)y = y^{-1}ex = y^{-1}y = e$$

Thus $y^{-1}x^{-1}$ is an inverse of xy. But inverses are unique by Theorem 2.12.

■

2.2 Cayley (Multipliction) Tables and Low-order Groups

Group operations (and binary operations more generally) on finite sets can be written in tabular form. For example, the set $G = \{0, 1, 2, 3\}$ under multiplication modulo 4 has multiplication table

$\cdot$	0	1	2	3
0	0	0	0	0
1	0	1	2	3
2	0	2	0	2
3	0	3	2	1

where we find $a \cdot b$ by taking a in the left column and b along the top.

Of course, this example isn't a group as the inverse axiom fails (0 and 2 have no multiplicative inverses).

In general, multiplication tables are not very useful. They are only practical for *small* sets. However, once you have a table, every fact regarding the binary structure is encoded therin, and can often easily be read off.

Terminology Recall that abstract binary operations are often written multiplicatively, hence we often call these *multiplication tables.* If the operation is addition, feel free to call it an *Addition table.* Arthur Cayley (1821–1895) was an English mathematician and one of the founders of group theory. When a binary structure is a group, it is common to refer to its multiplication table as a *Cayley table* in his honor.

Theorem 2.14 (Magic Square Property)**.** *If G is a group, then its Cayley table has two properties:*

1. *A row and column (by convention the first) which is a perfect copy of G itself.*
2. *Every element of G appears exactly once in each row and column.*

[11] Notice how we used associativity in the proof. Do you think that there might exist an algebraic structure which is non-associative in which inverses are non-unique?

Proof. Since G has an identity e, the identity row and column will simply be copies of G.
Now suppose that $a \in G$ and consider the function $f : G \to G$ defined by $f(x) = ax$. Since

$$f(x) = f(y) \implies ax = ay \implies x = y$$

by the left cancellation law, we see that f is injective. Moreover, $f(a^{-1}x) = x$ for all $x \in G$, whence f is surjective. Since the image of f is the a^{th} row of the Cayley table, we conclude that the a^{th} row is merely a rearrangement of the group G.
The argument for columns is similar.

■

In fact the theorem makes sense for infinite groups, it is practically useless also: how could one write down an *infinite* Cayley table?!

A partial converse is available, this will help us hunt for *small* groups.

Theorem 2.15. *If the multiplication table of an* associative *binary operation satisfies the magic square properties, then it also satisfies the identity and inverse axioms.*

It follows that an associative magic square is a group. Unfortunately, checking associativity directly from a table is usually impractically time-consuming.

Proof. The first property says that G has an identity. The second property says that the identity must appear exactly once in each row and column. Thus, given row a, there must be some $b \in G$ such that $ab = e$. Similarly, considering column a, we find the exists $c \in G$ such that $ca = e$. Now compute, similarly to the argument Theorem 2.12,

$$c(ab) = (ca)b \implies ce = eb \implies c = b$$

Thus a has an inverse.

■

It should also be clear that a binary operation is *commutative* if and only if its multiplication table has a symmetry of reflection across the main $\searrow$ diagonal.

Group tables for low order groups

Armed with the magic square discussion, we can start a project: identify *all* small group srructures. The process is this:

1. Every group must have an identity e. Put this first: we can now complete the first row and column of the table. For example, if $(\{e, a, b, c\}, \cdot)$ is to be a group of order 4, then our starting table is as shown.
2. Complete every row and column so that every element appears exactly once in each.
3. The result is *guaranteed* to be a group *if the table is associative*!

$\cdot$	e	a	b	c
e	e	a	b	c
a	a			
b	b			
c	c			

Definition 2.16. The *order* of a group G is the cardinality of the set G. Groups with infinite cardinality are usually referred to as *infinite groups.*

By following the magic square approach, we can easily construct all possible Cayley tables for small order groups. Indeed it is easy to see that there is only one group each (up to isomorphism[12]) of orders 1, 2 and 3.

$\cdot$	e
e	e

Order 1

$\cdot$	e	a
e	e	a
a	a	e

Order 2

$\cdot$	e	a	b
e	e	a	b
a	a	b	e
b	b	e	a

Order 3

Definition 2.17. The *abstract* groups listed above are denoted C_1, C_2 and C_3 respectively. The C stands for *cyclic*.

As abstract groups, no particular interpretation of the symbols e, a, b is required. We already know explicit examples of groups which have precisely these structures: compare the following Cayley tables for the groups $\mathbb{Z}_1, \mathbb{Z}_2, \mathbb{Z}_3$.

$+$	0
0	0

$+$	0	1
1	0	1
1	1	0

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

Proposition 2.18. *If $n \in \mathbb{N}$, then there is at least one group of order n, namely $\mathbb{Z}_n$.*

Why do we distinguish between abstract and explicit groups? In part because we want to stress the *common structure* even while acknowledging difference: for example, the Cayley table for the group U_3 of cube roots of unity under multiplication is shown: it doesn't take much imagination to see that the *structure* of the table is identical to that of $\mathbb{Z}_3$: both are examples of the abstract group C_3.

$\cdot$	1	ζ	ζ^2
1	1	ζ	ζ^2
ζ	ζ	ζ^2	1
ζ^2	ζ^2	1	ζ

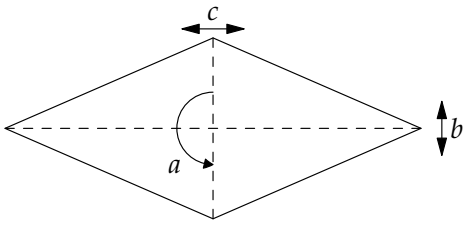
Groups of Order 4 Things start to get more interesting when we try to find Cayley tables of order 4. There are in fact four distinct ways to do this using the elements $\{e, a, b, c\}$, although three of them are seen to be identical once you permute the roles of the non-identity elements a, b, c: try figuring this out as an exercise!

$\cdot$	e	a	b	c
e	e	a	b	c
a	a	b	c	e
b	b	c	e	a
c	c	e	a	b

The cyclic group C_4

$\cdot$	e	a	b	c
e	e	a	b	c
a	a	e	c	b
b	b	c	e	a
c	c	b	a	e

The Klein 4-group V



Interpretation of V

[12] By this we mean that two group tables are considered equivalent (Representing the same abstract group) if they differ only by a relabelling, or a permutation of rows/columns. This amounts to the existence of an isomorphism (Definition 2.9) between the two groups.

Finally(!) we have two distinct groups of the same order. We already have a concrete description of the cyclic group, namely the remainders $\mathbb{Z}_4$ under addition modulo 4. What about the Klein[13] 4-group? An example of this might be the group of rotations and reflections of a rhombus (or a rectangle): choose one of a, b, c to be rotation by 180° and the remaining terms to be reflections.

It is progressively harder exercise to see that there is only abstract group C_5 or order 5, and *two* abstract groups of order 6, including the smallest non-abelian example (we met D_3 and its Cayley table in the introduction).

2.3 Subgroups

As with *subspaces* in linear algebra, whenever you see the prefix *sub-* in mathematics, you should think of the juxtaposition of *subset* with whatever is the following structure. Thus:

Definition 2.19. Let G be a group and $H \subseteq G$ a subset. H is a *subgroup* of G if H is a group in its own right with respect to the *same* group operation.
A subgroup H is a *proper subgroup* if $H \neq G$.
The *trivial subgroup* is the 1-element set $\{e\}$. All other subgroups are *non-trivial*.

We write $H \leq G$. Sometimes $H < G$ is written if H is a proper subgroup.

Examples

1. $(\mathbb{Z}, +) < (\mathbb{Q}, +) < (\mathbb{R}, +) < (\mathbb{C}, +)$
2. $(\mathbb{Q}^\times, \cdot) < (\mathbb{R}^\times, \cdot) < (\mathbb{C}^\times, \cdot)$
3. $\{e\} \leq G$ and $G \leq G$ for *any* G
4. $(\mathbb{R}^n, +) < (\mathbb{C}^n, +)$
5. $(\mathbb{R}^m, +) \leq (\mathbb{R}^n, +)$ if $m \leq n$

You don't have to check all the axioms of a group to see that a subset is a subgroup, indeed you only have to check the closure and inverse axioms, as per the following result.

Theorem 2.20. *A non-empty subset H of G is a subgroup if and only if H is closed under the group operation and inverses. That is:*

$$H \leq G \iff \begin{cases} \forall h_1, h_2 \in H, \ \ h_1 h_2 \in H \\ \forall h \in H, \ \ h^{-1} \in H \end{cases}$$

Proof. ($\Rightarrow$) If H is a subgroup, then it is a group, and thus satisfies the closure and inverse axioms.

($\Leftarrow$) Since H is a subset of G, it is automatic that the group operation of G is associative on H. Our assumption is that H also satisfies the closure and inverse axioms. It remains therefore only to check the identity axiom.
By assumption, if $h \in H$ we have

$$e = hh^{-1} \in H$$

[13] Named for Felix Klein. *V* refers to the German *vier,* meaning 'four.

since inverses and products remain in H. The identity e of G is therefore in H, and so H is a subgroup.

■

You should show directly that the above examples are subgroups using the Theorem. We also give a couple of explicit examples.

1. Let $3\mathbb{Z} = \{3n : n \in \mathbb{Z}\}$ be the multiples of 3. This is a subgroup of $\mathbb{Z}$ since
   - $\forall 3m, 3n \in 3\mathbb{Z}$ we have $3m + 3n = 3(m+n) \in 3\mathbb{Z}$.
   - $\forall 3m \in 3\mathbb{Z}$ we have $-(3m) = 3(-m) \in 3\mathbb{Z}$.
2. Recall the circle group $(S^1, \cdot)$ where $S^1 = \{z \in \mathbb{C} : |z| = 1\}$ describes the unit circle in the complex plane. This is a subgroup of the non-zeor complex numbers $(\mathbb{C}^\times, \cdot)$ under multiplication. We check
   - $\forall e^{i\theta}, e^{i\psi} \in S^1$ we have $e^{i\theta} \cdot e^{i\psi} = e^{i(\theta+\psi)} \in S^1$.
   - $\forall e^{i\theta} \in S^1$ we have $\left(e^{i\theta}\right)^{-1} = e^{-i\theta} \in S^1$.

   It is precisely the *exponential laws* which show that we have a subgroup.
3. Similarly to the previous example, the group U_n of n^{th} roots of unity is a subgroup of S^1. We also see that, for example $U_3 \leq U_6$, etc.

Non-examples of subgroups

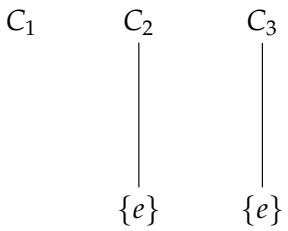
1. The positive integers $\mathbb{N} = \{1, 2, \ldots\}$ are closed under addition but not inverses: thus $\mathbb{N}$ is not a subgroup of $\mathbb{Z}$ under addition.
2. Let $Y \subseteq \mathbb{Z}$ be the set of integers whose remainder is 1 when divided by 3: i.e.

   $$Y = 3\mathbb{Z} + 1 = \{x \in \mathbb{Z} : x \equiv 1 \mod 3\} = \{1, 4, 7, 10, 13, \ldots, -2, -5, -8, \ldots\}$$

   Since $1 \in Y$ but $1 + 1 = 2 \notin Y$, we see that Y is not a subgroup of $\mathbb{Z}$ under addition.
   It is worth noting that Y is closed under *multiplication,* although it is still not a group for it is not closed under multiplicative inverses.

Subgroups of low order groups and subgroup diagrams

Recall the groups C_1, C_2, C_3 on page 13. It is straightforward to check that the only subgroups of these groups are the trivial group $\{e\}$ and the whole group itself. Their subgroup structures are not very interesting. We can summarize this by drawing *subgroup diagrams*: if a group lies below another and joined by a line, then the lower is a proper subgroup.



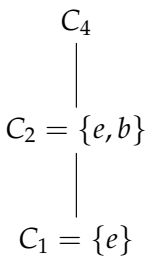
With groups of order 4, there is more variety.

Subgroups of C_4 In our abstract table defining C_4, then only proper non-trivial subgroup is $\{e, b\}$. One can see this by highlighting the entries only in the rows and columns for e and b: deleting the other rows and columns leaves a copy of the group table for C_2!

$\cdot$	e	a	b	c
e	e	a	b	c
a	a	b	c	e
b	b	c	e	a
c	c	e	a	b

$\rightsquigarrow$

$\cdot$	e	a
e	e	b
b	b	e



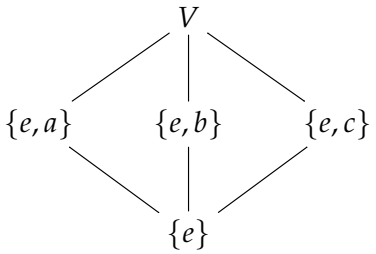
A little play (do this!) shows that you can't do the same thing with a or c. If you try to have a in a subgroup, then $a^2 = b$ must lie in the subgroup, as must $a^3 = c$ and $a^4 = e$: we get the whole group!

The subgroup diagram is drawn. We write $C_2 = \{e, b\}$ because the structure of the subgroup $\{e, b\}$ is that of the abstract cyclic group C_2.

We could alternatively have worked with the explicit[14] group $\mathbb{Z}_4 = \{0, 1, 2, 3\}$ under addition modulo 4. This time, we see that if $\{0, 2\}$ is a subgroup and that if 1 lies in a subgroup, so must $2 = 1 + 1$ and $3 = 1 + 1 + 1$, etc. The only proper non-trivial subgroup is $\{0, 2\}$.

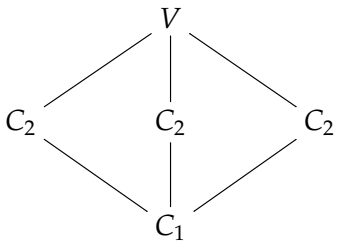
Subgroups of V We can play the same game with the abstract tabular definition, though it is easier to think about the rhombus description. Each of the elements a, b, c is its own inverse (rotate twice, or perform the same reflection twice and one recovers the original orientation of the rhombus). It follows that we have *three* distinct subgroups, each with two elements, namely

$$\{e, a\}, \quad \{e, b\}, \quad \{e, c\}$$



We also clearly have the subgroups $\{e\}$ and V. Why are there no other subgroups? If, say a and b *both* lie in a subgroup, then so must $ab = c$ and we obtain the entirety of V. The same thing happens for other pairs.

We can write the subgroup diagram in a couple of ways: the first diagram shows the elements in each subgroup, while the second shows the abtract names of each subgroup. Notice that V has *three distinct subgroups* with the C_2-structure!

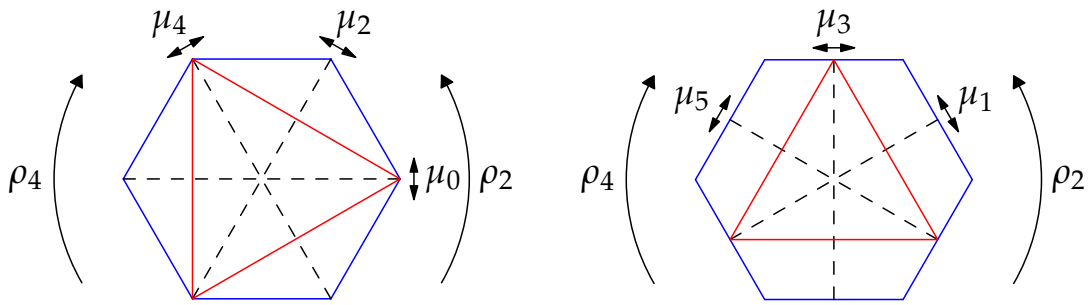


Geometric Subgroup Proofs

Sometimes it is much easier to make a geometric argument for being a subgroup. Recall that the set of symmetries of any physical object is a group under composition. Suppose that you can arrange two objects in such a way that every symmetry of the first is also a symmetry of the second. Then immediately the first group is a subgroup of the second.

For example, the regular hexagon has symmetry group D_6: this consist of six rotations $(e, \rho_1, \rho_2, \ldots, \rho_5)$, where we view the identity as 'rotate 0°,' and six reflections $(\mu_1, \ldots, \mu_6)$. Now draw an equilateral triangle inside a hexagon in two distinct ways.

[14] The correspondence is $e \mapsto 0$, $a \mapsto 1$, $b \mapsto 2$, $c \mapsto 3$.



Each of the six symmetries of the equilateral triangle is also a symmetry of the hexagon. It follows that the symmetry group D_3 of the triangle is a subgroup of that of the hexagon D_6 in two different ways:

$$\{e, \rho_2, \rho_4, \mu_0, \mu_2, \mu_4\} \leq D_6 \qquad \text{and} \qquad \{e, \rho_2, \rho_4, \mu_1, \mu_3, \mu_5\} \leq D_6$$

Can you see how to use the same picture to demonstrate that the Klein 4-group is a subgroup of D_6? In how many distinct ways can this be done?
If you want a real challenge in mental rotation, try to visualize why the rotation groups of the cube and the octahedron are isomorphic.

2.4 Homomorphisms

One of the purposes of abstract algebra is to observe and describe common structure. Mathematicians do this by defining functions: a *morphism* is a function which preserves some structure. Now that we have seen many examples of groups, it is worth revisiting Definition 2.9 whereby we compare structures.

Definition 2.9. Suppose that $(G, \cdot)$ and $(H, \star)$ are binary structures and that $\phi : G \to H$. We say that ϕ is a *homomorphism* if

$$\forall x, y \in G,\ \phi(x \cdot y) = \phi(x) \star \phi(y)$$

Additionally, if ϕ is bijective, we say that it is an *isomorphism.* If there exists an isomorphism ϕ, we say that $(G, \cdot)$ and $(H, \star)$ are *isomorphic* and write $G \cong H$.

Examples

1. $\phi : (\mathbb{N}, +) \to (\mathbb{N}, +)$ defined by $\phi(x) = 17x$ is a homomorphism of binary structures.
2. Let $\phi : \mathbb{Z} \to \mathbb{Z}$ be the function $\phi(x) = 2x$. Then

   $$\phi(x + y) = 2(x + y) = 2x + 2y = \phi(x) + \phi(y)$$

   so that ϕ is a homomorphism of groups ($(\mathbb{Z}, +)$ is an abelian group). This function is not an isomorphism since it is not surjective.

3. If V, W are vector spaces then they are abelian groups under vector addition. If $L : V \to W$ is a linear map then

$$\forall \mathbf{v}_1, \mathbf{v}_2 \in V,\ L(\mathbf{v}_1 + \mathbf{v}_2) = L(\mathbf{v}_1) + L(\mathbf{v}_2)$$

Otherwise said, L is a group homomorphism.[15]

4. Revisit the introduction where we long-windedly proved that $S_3 \cong D_3$ (the permutations of the set $\{1, 2, 3\}$ are isomorphic to the set of symmetries of an equilateral triangle).

5. The exponential law $e^x e^y = e^{x+y}$ says that the function $\phi(x) = e^x$ is a homomorphism of binary structures $\phi : (\mathbb{R}, +) \to (\mathbb{R}, \cdot)$.

   - ϕ isn't a *group* homomorphism, since $(\mathbb{R}, \cdot)$ isn't a group.
   - $e^x = e^y \implies x = y$ and so ϕ is *injective.*
   - Additionally, if we restrict the codomain to the range, then we obtain a *surjective* homomorphism $\phi : \mathbb{R} \to \mathbb{R}^+$ and therefore an *isomorphism*. Since $(\mathbb{R}^+, \cdot)$ is a group, we now have an isomorphism of groups.
   - The discussion works perfectly if $\phi(x) = a^x$ where a is any positive real number *except* 1.

6. The above example can be extended to the complex numbers $\phi(z) = e^z$ is a homomorphism $\phi : (\mathbb{C}, +) \to (\mathbb{C}, \cdot)$ of binary structures. This is *not* an isomorphism for two reasons:

   - $\phi(0) = \phi(2\pi i) \implies \phi$ is not injective.
   - There does not exist $z \in \mathbb{C}$ such that $\phi(z) = 0$, so ϕ is not surjective.

   However, recall page 8, where we saw that the group $\mathbb{Z}_n$ under addition is isomorphic to the set of n^{th} roots of unity under the isomorphism

$$\phi(x) = \zeta^n = e^{\frac{2\pi i x}{n}}$$

   The moral of the story is to be really careful with domains and codomains!

Showing Isomorphicity

Often the challenge is to determine whether two structures $(X, *)$ and $(Y, \star)$ are isomorphic. The first step is to develop a gut feeling—this only comes with practice! If you think that structures are isomorphic, then you should follow the steps below:

- Define a function $\phi : X \to Y$,
- Check that ϕ is a homomorphism: $\phi(x * y) = \phi(x) \star \phi(y)$,
- Check ϕ is injective: $\phi(x) = \phi(y) \implies x = y$,
- Check ϕ is surjective: $\forall y \in Y,\ \exists x \in X$ such that $y = \phi(x)$.

You can perform the final three steps in any order you like. Sometimes it is easier to first think of a bijection, then check that such is a homomorphism; other times it is easier to use the homomorphism property to choose a function, then check that you have a bijection.

[15] The scalar multiplication condition $L(\alpha \mathbf{v}) = \alpha L(\mathbf{v})$ satisfied by a linear map does not come into our consideration of homomorphisms.

Examples

1. Prove that $2\mathbb{Z} \cong 3\mathbb{Z}$ with the binary operation of addition on both sides.

   Define ϕ: Let $\phi : 2\mathbb{Z} \to 3\mathbb{Z} : 2n \mapsto 3n$, i.e. $\phi(x) = \frac{3}{2}x$.
   Homomorphism: $\phi(x+y) = \frac{3}{2}(x+y) = \frac{3}{2}x + \frac{3}{2}y = \phi(x) + \phi(y)$. ✓
   Injective: $\phi(x) = \phi(y) \implies \frac{3}{2}x = \frac{3}{2}y \implies x = y$. ✓
   Surjective: An arbitrary element of $3\mathbb{Z}$ is $z = 3m$ where $m \in \mathbb{Z}$. But $3m = \phi(2m)$. ✓

   ϕ is therefore an isomorphism $\phi : 2\mathbb{Z} \cong 3\mathbb{Z}$.

2. The bijection $\phi(x) = \frac{3}{2}x$ is also an isomorphism $2\mathbb{Z} \cong 3\mathbb{Z}$ with respect to the binary operations $x * y = \frac{1}{2}xy$ on $2\mathbb{Z}$ and $x \star y = \frac{1}{3}xy$ on $3\mathbb{Z}$.

Pull-backs

It is very easy to create examples of isomorphic structures. Given a *bijection* $\phi : X \to Y$ and a binary operation $\star$ on Y, you can always define an operation $*$ on X by *pulling-back* $\star$ to X:

$$x_1 * x_2 := \phi^{-1}(\phi(x_1) \star \phi(x_2))$$

Moreover, if $(Y, \star)$ happens to be a group, so also will $(X, *)$ be.

1. The map $\phi : \mathbb{R}^+ \to \mathbb{R}^+ : x \mapsto x^2$ is a bijection. Suppose we want ϕ to be an isomorphism $\phi : (\mathbb{R}^+, *) \to (\mathbb{R}^+, +)$. Then we must define $*$ by

   $$x * y := \phi^{-1}(\phi(x) + \phi(y)) = \phi^{-1}(x^2 + y^2) = \sqrt{x^2 + y^2}$$

   In this case we do not have an isomorphism of groups, since $(\mathbb{R}^+, +)$ is not a group.

2. Now suppose that we want ϕ to be an isomorphism $\phi : (\mathbb{R}^+, +) \to (\mathbb{R}^+, \star)$. This time we must have ϕ satisfying

   $$\phi(x) \star \phi(y) = \phi(x+y) \implies x^2 \star y^2 = (x+y)^2$$

   The required binary operation is therefore $X \star Y = (\sqrt{X} + \sqrt{Y})^2$.

3. A group structure on $X = (-\frac{\pi}{2}, \frac{\pi}{2})$ could be defined as follows:

   $$\forall x_1, x_2 \in X, \text{ define } x_1 * x_2 = \tan^{-1}(\tan(x) + \tan(y))$$

   Since $\tan : (-\frac{\pi}{2}, \frac{\pi}{2}) \to \mathbb{R}$ is a bijection, we see that $*$ is simply the pull-back of the group structure $(\mathbb{R}, +)$ to $(-\frac{\pi}{2}, \frac{\pi}{2})$ so that $\tan : X \to \mathbb{R}$ is an isomorphism.

Showing non-isomorphicity

This often seems harder, as there is no general method. Unless X, Y are very small sets, you can't realistically test every function $X \to Y$. Instead we have to be a little more cunning.

Definition 2.21. A *structural property* of $(X, *)$ is a property which is preserved under isomorphism: i.e. if $\phi : (X, *) \to (Y, \star)$ is an isomorphism then $(X, *)$ and $(Y, \star)$ have the same structural properties.

The following is a non-exhaustive list of structural properties: suppose $\phi : X \to Y$ is an isomorphism throughout.

Cardinality If $X \cong Y$, then the elements of X, Y are bijectively paired, whence the cardinalities of X and Y are the same. This is true even for infinite sets: recall that $|\mathbb{N}| = |\mathbb{Q}| = \aleph_0 \lneq |\mathbb{R}|$, so there are *no* isomorphisms between $\mathbb{Q}$ and $\mathbb{R}$, no matter what binary operations you have.

Commutativity & Associativity For instance if $(X, *)$ is commutative, then

$$\forall a, b \in X,\ \phi(a) \star \phi(b) = \phi(a * b) = \phi(b * a) = \phi(b) \star \phi(a)$$

Since ϕ is bijective, every element of Y has the form $\phi(a)$ for some $a \in X$. Thus $(Y, \star)$ is commutative.

Identity If X has an identity element e then $\phi(e)$ is an identity for Y.

Solutions to equations If an equation has a solution in X and $X \cong Y$, then (typically) a related equation will have the same number of solutions in Y.
For example, an element $x \in X$ is *idempotent* if $x * x = x$. It follows that $\phi(x) \star \phi(x) = \phi(x)$ in Y. Thus if idempotents exist in X, but do not in Y, there can be no isomorphism.

Being a group! In particular, if $(X, *) \cong (Y, \star)$ where $(X, *)$ isa group, so is $(Y, \star)$.

There are many other possible structural properties. The more complex the structure, the more potential properties there are to consider. Disproving isomorphicity is somewhat of an art, requiring a flash of inspiration to find the correct structural property. It is also important to note that there are many concepts that are not necessarily preserved by an isomorphism: the type of element (a number, a matrix, etc.), the type of binary operation (e.g. addition versus multiplication).

Examples

1. Consider the binary operations with tables

$*$	a	b
a	a	b
b	b	a

and

$\star$	c	d
c	c	d
d	c	d

   The first is commutative while the second is not: the structures are non-isomorphic.

2. $(\mathbb{R}^3, +) \ncong (\mathbb{R}^3, \times)$ (cross product). This is since $+$ is commutative and associative, while $\times$ is neither. Indeed $(\mathbb{R}^3, +)$ is an abelian group, while $(\mathbb{R}^3, \times)$ only satisfies the closure axiom.

3. $(\mathbb{N}_0, +) \ncong (\mathbb{N}, +)$ since $\mathbb{N}_0$ contains an identity element 0 while $\mathbb{N}$ does not.

4. $(\mathbb{Q}, +) \ncong (\mathbb{Q}^+, \cdot)$. This is harder, since *both* structures are abelian groups and both have the same cardinality. This is where solutions to equations come in.
   Consider the equation $x + x = c$ in $(\mathbb{Q}, +)$ where c is a given rational number. This *always* has exactly one solution $x = \frac{c}{2}$. If $\phi : \mathbb{Q} \to \mathbb{Q}^+$ were an isomorphism, then we would have to have

   $$\phi(x) \cdot \phi(x) = \phi(c)$$

   which says that $y = \phi(x)$ solves $y^2 = \phi(c)$.
   However, being an isomorphism, ϕ must be surjective, whence $\exists c \in \mathbb{Q}$ such that $\phi(c) = 2$. We are therefore claiming that the equation $y^2 = 2$ has a solution $y \in \mathbb{Q}^+$: a contradiction.
   To summarize, the equation $y^2 = 2$ has no solution in $\mathbb{Q}^+$, but the 'corresponding equation' $x + x = c$ in $\mathbb{Q}$ has a solution for every $c \in \mathbb{Q}$.

Aside: Matrix groups

There are many groups of matrices under multiplication. These are of particular interest to geometers because they are often defined with an intention of preserving certain geometric properties: e.g. volume, length, angle, etc. We will not use these very often and you're not expected to be an expert on these.

Definition 2.22. The *general linear group* $\mathrm{GL}_n(\mathbb{R})$ is the set of invertible linear transformations of an n-dimensional real vector space under composition. Since all such vector spaces in the presence of a basis may be viewed as $\mathbb{R}^n$, this group may be represented by the set of invertible $n \times n$ matrices under multiplication.

$$\mathrm{GL}_n(\mathbb{R}) = \{A \in M_n(\mathbb{R}) : \det A \neq 0\}$$

This is certainly a group:

Closure If $A, B \in \mathrm{GL}_n(\mathbb{R})$, then $\det(AB) = \det A \cdot \det B \neq 0$, whence $AB \in \mathrm{GL}_n(\mathbb{R})$.

Associativity We discussed this in Corollary 2.11.

Identity $\mathrm{I}_n = \mathrm{diag}(1, 1, \ldots, 1)$ is the multiplicative identity.

Inverse If $A \in \mathrm{GL}_n(\mathbb{R})$, then the matrix inverse satisfies $\det(A^{-1}) = \frac{1}{\det A}$ which is defined and non-zero. Thus $A^{-1} \in \mathrm{GL}_n(\mathbb{R})$.

Note that $\mathrm{GL}_n(\mathbb{R})$ is *non-abelian* since matrix multiplication is not commutative. For example

$$\begin{pmatrix} 1 & 1 \\ 0 & 2 \end{pmatrix} \begin{pmatrix} 2 & 1 \\ 0 & 1 \end{pmatrix} = \begin{pmatrix} 2 & 2 \\ 0 & 2 \end{pmatrix} \neq \begin{pmatrix} 2 & 4 \\ 0 & 2 \end{pmatrix} = \begin{pmatrix} 2 & 1 \\ 0 & 1 \end{pmatrix} \begin{pmatrix} 1 & 1 \\ 0 & 2 \end{pmatrix}$$

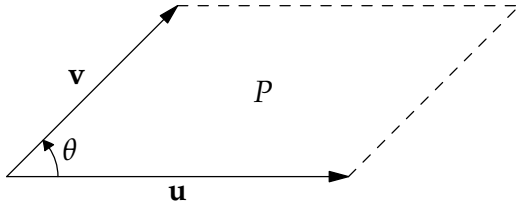
Special linear group

The first property that we might want to consider is *measure* (i.e. area in 2D, volume in 3D, etc.). You should have seen the following in a linear algebra class.

Theorem 2.23. *Suppose that P is a parallelogram spanned by the vectors $\mathbf{u}, \mathbf{v}$. Then its signed area is*

$$Area(P) = |\mathbf{u}|\,|\mathbf{v}| \sin\theta_{\mathbf{u},\mathbf{v}} = \det \begin{pmatrix} u_1 & v_1 \\ u_2 & v_2 \end{pmatrix}$$

θ is measured counter-clockwise from $\mathbf{u}$ to $\mathbf{v}$, whence the signed area is positive if and only if $0 < \theta < \pi$.



Suppose that A is a 2×2 matrix. Let us compute what A does to the parallelogram P. It is easy to check that the result is a new parallelogram spanned by the vectors $A\mathbf{u}$ and $A\mathbf{v}$. We can therefore compute its signed area:

$$\text{Area}(A(P)) = \det \begin{pmatrix} (A\mathbf{u})_1 & (A\mathbf{v})_1 \\ (A\mathbf{u})_2 & (A\mathbf{v})_2 \end{pmatrix} = \det \left(A \begin{pmatrix} u_1 & v_1 \\ u_2 & v_2 \end{pmatrix} \right) = \det A \cdot \text{Area}(P)$$

If we want the new parallelogram $A(P)$ to have the same signed area as P, then we must restrict to matrices with determinant 1.

Definition 2.24. The *special linear group* $\mathrm{SL}_n(\mathbb{R})$ is the group under multiplication of $n \times n$ matrices with determinant 1.

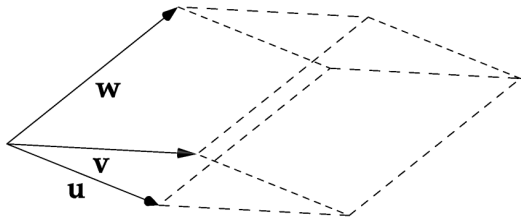
We can check that this is a subgroup of $\mathrm{GL}_n(\mathbb{R})$ by appealing to Theorem 2.20: suppose that $A, B \in \mathrm{SL}_n(\mathbb{R})$, then

$$\det(AB) = \det A \det B = 1 \qquad \text{and} \qquad \det(A^{-1}) = \frac{1}{\det A} = 1$$

whence $\mathrm{SL}_n(\mathbb{R})$ is a subset of $\mathrm{GL}_n(\mathbb{R})$ closed under multiplication and inverses.

The interpretation of $\mathrm{SL}_3(\mathbb{R})$ is similar to that of $\mathrm{SL}_2(\mathbb{R})$. The *signed volume* of a parallelepiped in $\mathbb{R}^3$ spanned by the vectors $\mathbf{u}, \mathbf{v}, \mathbf{w}$ is the *scalar triple product*

$$\text{Volume} = [\mathbf{u}, \mathbf{v}, \mathbf{w}] = (\mathbf{u} \times \mathbf{v}) \cdot \mathbf{w}$$



If A is a 3×3 matrix, then the parallelepiped spanned by $A\mathbf{u}, A\mathbf{v}, A\mathbf{w}$ will have volume

$$[A\mathbf{u}, A\mathbf{v}, A\mathbf{w}] = \det(A)[\mathbf{u}, \mathbf{v}, \mathbf{w}]$$

$\mathrm{SL}_3(\mathbb{R})$ is therefore the group of signed[16] volume-preserving linear transformations of $\mathbb{R}^3$.

[16] $\mathbf{u} \times \mathbf{v}$ points perpendicular to the plane spanned by the two vectors. A parallelepiped has positive signed-volume if $\mathbf{w}$ points to the same side of this plane as $\mathbf{u} \times \mathbf{v}$. If $\mathbf{u}$ points out of the page and $\mathbf{v}$ into the page, then the picure denotes a parallelepiped with positive signed volume. This convention is essentially the right-hand rule.
More generally, transformations with $\det > 0$ are said to *preserve orientation.* $\mathrm{SL}_n(\mathbb{R})$ is then the set of orientation- and (hyper-)volume-preserving linear transformations of $\mathbb{R}^n$. Quite the mouthful.

The Orthogonal group

The orthogonal group is the set of matrices which preserve lengths of vectors and the angles between them. Recall that both of these concepts can be described in terms of the *scalar/dot product:*

Scalar product $\mathbf{u} \cdot \mathbf{v} = \mathbf{u}^T \mathbf{v}$

Length $|\mathbf{u}| = \sqrt{\mathbf{u} \cdot \mathbf{u}}$

Angle $\cos\theta = \dfrac{\mathbf{u} \cdot \mathbf{v}}{|\mathbf{u}|\,|\mathbf{v}|}$

If we want a matrix A to preserve angles between and lengths of vectors, it is enough to have the matrix preserve the value of the scalar product of any two vectors. That is, we require

$$\forall \mathbf{u}, \mathbf{v}, \quad (A\mathbf{u}) \cdot (A\mathbf{v}) = \mathbf{u} \cdot \mathbf{v}$$

This is equivalent to

$$\mathbf{u}^T \mathbf{v} = (A\mathbf{u})^T (A\mathbf{v}) = \mathbf{u}^T A^T A \mathbf{v}$$

Definition 2.25. The *orthogonal group* is the following set under multiplication

$$\mathrm{O}_n(\mathbb{R}) = \{A \in M_n(\mathbb{R}) : A^T A = I\}$$

where I is the $n \times n$ identity matrix.
The *special orthogonal group* $\mathrm{SO}_n(\mathbb{R}) = \mathrm{O}_n(\mathbb{R}) \cap \mathrm{SL}_n(\mathbb{R})$ is the subset of determinant 1 orthogonal matrices.

Taking determinants of the property $A^T A = I$ gives $\det(A)\det(A^T) = \det(A)^2 = 1 \implies \det(A) = \pm 1$. Thus $\mathrm{SO}_n(\mathbb{R})$ consists of exactly half the orthogonal group.

Interpretations When $n = 2$ the group $\mathrm{SO}_2(\mathbb{R})$ consists of the rotations around the origin ($\det = 1$) while $\mathrm{O}_2(\mathbb{R})$ also includes the set of reflections across lines through the origin ($\det = -1$).
$\mathrm{SO}_3(\mathbb{R})$ comprises all rotations around the origin. $\mathrm{O}_3(\mathbb{R})$ also includes reflections across any plane through the origin.

Pseudo-orthogonal groups The scalar product definition of $\mathrm{O}_n(\mathbb{R})$ can be extended. Suppose you put a non-positive-definite scalar product on $\mathbb{R}^n$, for example

$$(\mathbf{u}, \mathbf{v}) := \mathbf{u}^T \begin{pmatrix} 1 & 0 & 0 & 0 \\ 0 & -1 & 0 & 0 \\ 0 & 0 & -1 & 0 \\ 0 & 0 & 0 & -1 \end{pmatrix} \mathbf{v}$$

on $\mathbb{R}^4$. The group which preserves this inner product is the *pseudo-orthogonal group* $\mathrm{O}(1,3)$. This example is much more than abstract mathematical nonsense: in Physics this is the *Lorentz Group*, which is critical to the study of relativity.

Complex matrix groups All of the above examples can be constructed with complex entries, yielding the groups $\mathrm{GL}_n(\mathbb{C})$, $\mathrm{O}_n(\mathbb{C})$, etc.

The Unitary group The unitary group is constructed similarly to the orthogonal group. This time we take the Hermitian product on $\mathbb{C}^n$: $\langle \mathbf{u}, \mathbf{v} \rangle = \mathbf{u}^* \mathbf{v} = \overline{\mathbf{u}}^T \mathbf{v}$. The unitary group is the set of complex matrices which preserve this product:

$$\mathrm{U}_n = \{A \in \mathrm{GL}_n(\mathbb{C}) : \overline{A}^T A = \mathrm{I}\}$$

The *special unitary group* SU_n is the set of determinant 1 unitary matrices, that is $\mathrm{SU}_n = \mathrm{U}_n \cap \mathrm{SL}_n(\mathbb{C})$.

A discrete matrix group Matrix groups need not be continuous. The set

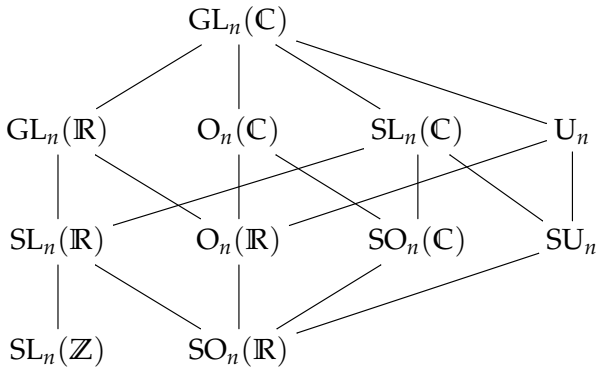
$$\mathrm{SL}_n(\mathbb{Z}) = \{A \in \mathrm{SL}_n(\mathbb{R}) : \text{ all entries are integers}\}$$

is a group. It is clearly a subset of $\mathrm{SL}_n(\mathbb{R})$ and it is easy to see that the product of two matrices with integer entries also has integer entries, so it remains to check inverses. Recall from linear algebra the formula

$$A^{-1} = \frac{1}{\det A} \mathrm{adj}(A)^T$$

where $\mathrm{adj}(A)$ is the adjoint of A, formed by taking positive and negative multiples of determinant minors of A. If $A \in \mathrm{SL}_n(\mathbb{Z})$, then $\mathrm{adj}(A)$ has integer entries and so therefore has its transpose. Since $\det(A) = 1$ it follows that the inverse not only has determinant 1, but has integer entries. $\mathrm{SL}_n(\mathbb{Z})$ is therefore a group.

A subgroup diagram for matrix groups For reference, we give the subgroup relations between the various groups mentioned.



These are just a taste of some of the more common matrix groups. There are many more out there!

3 Cyclic groups

Cyclic groups are a very basic class of groups: we have already seen some examples such as $\mathbb{Z}_n$. Cyclic groups are nice in that their complete structure can be easily described. The overall approach in this section is to define and classify all cyclic groups and to understand their subgroup structure.

3.1 Definitions and Examples

The basic idea of a cyclic group is that it can be generated by a single element. Here are two motivating examples:

1. The group of integers under addition can generated by 1. By this we mean that the element 1 can be combined with itself using only the group operation and inverses to produce the entire set of integers: if $n > 0$, then

   $$n = 1 + 1 + \cdots + 1$$

   from which we can easily produce $-n$ and $0 = 1 + (-1)$. The element -1 could also be used to generate $\mathbb{Z}$.

2. The group $U_4 = \{1, -1, i, -i\}$ of 4^{th} roots of unity under multiplication and also be generated from a single element i:

   $$U_4 = \{i, i^2, i^3, i^4\} = \{i, -1, -i, 1\}$$

   The same construction can be performed using $-i$.

Now we formalize this idea.

Lemma 3.1. *Let G be a multiplicative group and let $g \in G$. Then the set*

$$\langle g \rangle := \{g^n : n \in \mathbb{Z}\} = \{\ldots, g^{-1}, e, g, g^2, \ldots\}$$

is a subgroup of G.

Proof. *Non-emptiness* Clearly $e \in \langle g \rangle$ (similarly $g \in \langle g \rangle$).

Closure Every element of $\langle g \rangle$ has the form g^k for some $k \in \mathbb{Z}$. It suffices to check that

$$g^k \cdot g^l = g^{k+l} \in \langle g \rangle$$

Inverses Since $(g^k)^{-1} = g^{-k} \in \langle g \rangle$, we are done. ∎

Definition 3.2. The subgroup $\langle g \rangle$ defined in Lemma 3.1 is the *cyclic subgroup of G generated by g.*
The *order* of an element $g \in G$ is the order $|\langle g \rangle|$ of the subgroup generated by g.
G is a *cyclic group* if $\exists g \in G$ such that $G = \langle g \rangle$: we call g a *generator* of G.

We now have *two* concepts of *order*.

The order of a *group* is the cardinality of the group viewed as a set.

The order of an *element* is the cardinality of the cyclic group generated by that element.

Cyclic groups are the precisely those groups containing elements having the same order as that of the group: these are the generators of the cyclic group.

Examples

Integers The integers $\mathbb{Z}$ form a cyclic group under addition. $\mathbb{Z}$ is generated by either 1 or -1. Note that this group is written *additively,* so that, for example, the subgroup generated by 2 is the group of even numbers under addition:

$$\langle 2 \rangle = \{2m : m \in \mathbb{Z}\} = 2\mathbb{Z}$$

Modular Addition For each $n \in \mathbb{N}$, the group of remainders $\mathbb{Z}_n$ under addition modulo n is a cyclic group. It is also written additively, and is generated by 1. Typically $\mathbb{Z}_n$ is also generated by several other elements. For example, $\mathbb{Z}_4 = \{0, 1, 2, 3\}$ is generated by both 1 and 3:

$$\langle 1 \rangle = \{1, 2, 3, 0\} \qquad \langle 3 \rangle = \{3, 2, 1, 0\}$$

Roots of Unity For each $n \in \mathbb{N}$, the n^{th} roots of unity $U_n = \{1, \zeta, \ldots, \zeta^{n-1}\}$ form a cyclic group under multiplication. This group is generated by ζ, amongst others. The generators of U_n are termed the *primitive n^{th} roots of unity.*

We shall see shortly that every cyclic group is isomorphic to either the integers or the modular integers. Regardless, we will still write abstract cyclic groups multiplicatively. This, at least in part, is because the application of cyclic groups very often involves the study of cyclic *subgroups* of more complex groups, rather than of cyclic groups in their own right.

3.2 Classification of Cyclic Groups

Our first goal is to describe all cyclic groups.

Lemma 3.3. *Every cyclic group is abelian.*

Proof. Let $G = \langle g \rangle$. Then any two elements of G can be written g^k, g^l for some $k, l \in \mathbb{Z}$. But then

$$g^k g^l = g^{k+l} = g^{l+k} = g^l g^k,$$

and so G is abelian. ∎

Note that the converse is false: the Klein 4-group V is abelian but not cyclic.

Before going any further, we need to distinguish between *finite* and *infinite* groups. To do this, suppose that $G = \langle g \rangle$ is cyclic, and consider the following set of natural numbers[17]

$$S = \{m \in \mathbb{N} : g^m = e\}$$

The distinction hinges on whether the set S is empty or not.

[17] Recall $\mathbb{N} = \{1, 2, 3, \ldots\}$.

Infinite Cyclic Groups

Theorem 3.4. *Suppose $G = \langle g \rangle$ is cyclic and that the set $S = \{m \in \mathbb{N} : g^m = e\}$ is* empty. *Then G is an infinite group and we have an isomorphism $G \cong \mathbb{Z}$ via*

$$\mu : \mathbb{Z} \to G : x \mapsto g^x$$

Proof. We simply check the properties of μ:

Injectivity WLOG assume that $x \geq y$. Then

$$\mu(x) = \mu(y) \implies g^x = g^y \implies g^{x-y} = e \implies x - y = 0 \implies x = y$$

since $S = \emptyset$. Thus μ is 1–1.

Surjectivity μ is onto by definition: every element of G has the form g^x for some $x \in \mathbb{Z}$.

Homomorphism $\mu(x + y) = g^{x+y} = g^x g^y = \mu(x)\mu(y)$.

■

Finite Cyclic Groups

Theorem 3.5. *Suppose that $G = \langle g \rangle$ is cyclic and that $S = \{m \in \mathbb{N} : g^m = e\}$ is non-empty. By the well-ordering of $\mathbb{N}$, there exists a natural number $n = \min S$. Then $G \cong \mathbb{Z}_n$ via the isomorphism*[18]

$$\mu : \mathbb{Z}_n \to G : [x] \mapsto g^x$$

In particular, n is the order of G.

The proof is almost identical to that for infinite groups with two important differences: we need to check well-definition of μ since the domain is a set of equivalence classes, and we need to apply the division algorithm to invoke the injectivity argument.

Proof. Check the properties of μ.

Well-definition $[x] = [y] \implies y = x + \lambda n$ for some $\lambda \in \mathbb{Z}$. But then

$$\mu([x]) = g^x = g^y g^{\lambda n} = g^y = \mu([y])$$

since $g^n = e$.

Injectivity Suppose that $\mu([x]) = \mu([y])$. Then

$$g^x = g^y \implies g^{x-y} = e$$

Apply the division algorithm: $x - y = \lambda n + r$ for unique integers λ, r with $0 \leq r < n$. But then

$$e = g^{x-y} = g^{\lambda n} g^r = g^r \implies r = 0$$

since $r < n$. But then $x - y = \lambda n \implies [x] = [y]$.

Surjectivity This is by definition of μ.

Homomorphism As in the infinite case, $\mu([x + y]) = g^{x+y} = g^x g^y = \mu([x])\mu([y])$.

■

[18] We use the equivalence class notation $[x] = \{x + \lambda n : \lambda \in \mathbb{Z}\}$ to be clear regarding the nature of the elements of $\mathbb{Z}_n$. In particular, this stresses the fact that we need to check well-definition of μ.

Examples

1. The group of 7^{th} roots of unity $(U_7, \cdot)$ is isomorphic to $(\mathbb{Z}_7, +_7)$ via the isomorphism

$$\phi : \mathbb{Z}_7 \to U_7 : k \mapsto \zeta_7^k$$

2. The group $5\mathbb{Z} = \langle 5 \rangle$ is an infinite cyclic group. It is isomorphic to the integers via

$$\phi : (\mathbb{Z}, +) \cong (5\mathbb{Z}, +) : z \mapsto 5z$$

3. The real numbers $\mathbb{R}$ form an infinite group under addition. This *cannot* be cyclic because its cardinality $2^{\aleph_0}$ is larger than the cardinality $\aleph_0$ of the integers.

***The* cyclic group of order n?**

Given the Theorem, we see that all cyclic groups of order n are isomorphic. This is usually summarized by saying that there is exactly one cyclic group of order n (up to isomorphism). We label this *abstract* group C_n.

The fact that C_n is somewhat nebulous turns out to be convenient. For example: in some texts you may find $\mathbb{Z}_6$ referred to as *the* cyclic group of order 6. What, then, should we call the subgroup

$$\langle 2 \rangle = \{2, 4, 6, 8, 10, 0\} \leq (\mathbb{Z}_{12}, +)?$$

Certainly $\langle 2 \rangle$ is isomorphic to $\mathbb{Z}_6$ via $\phi : 2z \mapsto z$. It would be erroneous however to say that $\langle 2 \rangle$ *equals* $\mathbb{Z}_6$, since $\mathbb{Z}_6 = \{0, 1, 2, 3, 4, 5\}$ has *different elements.*
The notation C_6 is neutral: it's elements have no explicit interpretation. It is therefore a little safer to write $\langle 2 \rangle \cong C_6$.

3.3 Subgroups of cyclic groups

We can very straightforwardly classify all the subgroups of a cyclic group.

Theorem 3.6. *All subgroups of a cyclic group are themselves cyclic.*

Proof. Let $G = \langle g \rangle$ and let $H \leq G$. If $H = \{e\}$ is trivial, we are done. Otherwise, since all elements of H are in G, there must exist[19] a smallest natural number s such that $g^s \in H$. We claim that $H = \langle g^s \rangle$.
Let $g^m \in H$ be a general element of H. The division algorithm says that there exist unique integers q, r such that

$$m = qs + r \quad \text{and} \quad 0 \leq r < s$$

Therefore

$$g^m = g^{qs+r} = (g^s)^q g^r \implies g^r = (g^s)^{-q} g^m \in H$$

since H is closed under $\cdot$ and inverses. But this forces $r = 0$, since $r < s$.
In summary $g^m = (g^s)^q \in \langle g^s \rangle$ and we are done. ∎

[19] Well-ordering again…

Subgroups of infinite cyclic groups

If G is an infinite cyclic group, then any subgroup is itself cyclic and thus generated by some element. It is easiest to think about this for $G = \mathbb{Z}$. There are two cases:

- The trivial subgroup: $\langle 0 \rangle = \{0\} \leq \mathbb{Z}$.
- Every other subgroup: $\langle s \rangle = s\mathbb{Z} \leq \mathbb{Z}$ for $s \neq 0$. All these subgroups are isomorphic to $\mathbb{Z}$ via the isomorphism $\mu : \mathbb{Z} \to s\mathbb{Z} : x \mapsto sx$.

It should also be clear that $n\mathbb{Z} \leq m\mathbb{Z} \iff n \mid m$.

In the language of an abstract cyclic group $G = \langle g \rangle$ the non-trivial subgroups have the form

$$\langle g^s \rangle \cong G \quad \text{via} \quad \mu : G \to \langle g^s \rangle : g^x \mapsto g^{sx}$$

You should be comfortable comparing notations.

Subgroups of finite cyclic groups

As above, it is easier to consider the case where $G = \mathbb{Z}_n$ first. We state the general result afterwards.

Theorem 3.7. *Let $s \in \mathbb{Z}_n$. Then $\langle s \rangle \cong C_{\frac{n}{\gcd(s,n)}}$.*
More precisely, let $d = \gcd(s, n)$. Then $\langle s \rangle = \langle d \rangle$ as subgroups of $\mathbb{Z}_n$. Moreover, $\langle d \rangle \cong C_{\frac{n}{d}}$.

Proof. Let $d = \gcd(s, n)$. Since $d \mid s$ we see that $s \in \langle d \rangle \implies \langle s \rangle \leq \langle d \rangle$.
Conversely, by Bézout's identity, $d = \lambda s + \sigma n$ for some $\lambda, \sigma \in \mathbb{Z}$, from which $d \equiv \lambda s \mod n$. But then $d \in \langle s \rangle \implies \langle d \rangle \leq \langle s \rangle$.
Since $d \mid n$, there are precisely $\frac{n}{d}$ elements in $\langle d \rangle$, indeed

$$\langle d \rangle = \left\{0, d, 2d, \ldots, \left(\frac{n}{d} - 1\right) d\right\}$$

■

Corollary 3.8. *1. If $d \mid n$, then $\mathbb{Z}_n$ has precisely one subgroup of order d.*

2. If $G = \langle g \rangle$ has order n and $d \mid n$, then G has precisely one subgroup of order d. Indeed

$$\langle g^s \rangle = \langle g^t \rangle \iff \gcd(s, n) = \gcd(t, n)$$

and this subgroup has order $\frac{n}{\gcd(s,n)}$.

Summary

We now know everything there is to know about cyclic groups and their subgroups.

1. Is $G = \langle g \rangle$ infinite? If yes, then $G \cong \mathbb{Z}$ via $g^x \leftrightarrow x$. Every subgroup has the form $\langle g^s \rangle$: these are distinct for each s. A subgroup is trivial if $s = 0$ and isomorphic to G otherwise.
2. Is G finite? Then $G \cong \mathbb{Z}_n$ where $n = \min\{k \in \mathbb{N} : g^k = e\}$. There exists exactly one subgroup of G for each divisor d of n:

$$H = \langle g^s \rangle \leq G \text{ has } H \cong C_{\frac{n}{\gcd(s,n)}}$$

Armed with this information, it is easy to construct the complete subgroup diagrams for some cyclic groups. Indeed you will probably need to work several examples in order to *learn* and believe all these theorems!

Examples

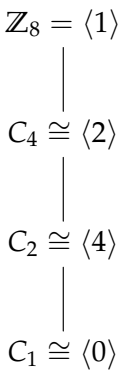
1. $\mathbb{Z}_8$ is generated by $1, 3, 5$ and 7, since these are precisely the elements $s \in \mathbb{Z}_8$ for which $\gcd(s, 8) = 1$. For example,

   $$\mathbb{Z}_8 = \langle 5 \rangle = \{5, 2, 7, 4, 1, 6, 3, 0\} \cong C_{\frac{8}{\gcd(5,8)}}$$

   The subgroup generated by 6 is

   $$\langle 6 \rangle = \{6, 4, 2, 0\}$$

   which has order $4 = \frac{8}{\gcd(6,8)}$ in accordance with the Theorem. This subgroup is also generated by 2. The complete collection of subgroups and their generators is shown in the table, and the subgroup diagram is also drawn.

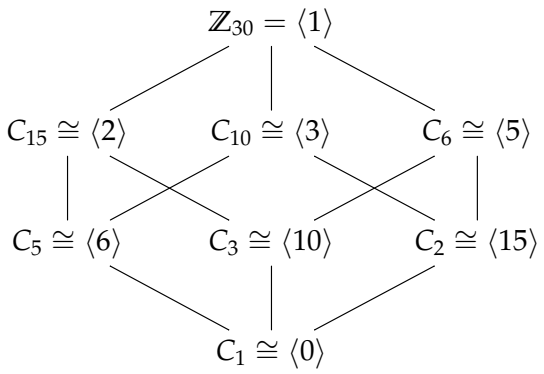


x	$\gcd(x, 8)$	$8/\gcd(x, 8)$	subgroup generated $\langle x \rangle$
$0(8)$	$0(8)$	1	C_1
4	4	2	C_2
$2, 6$	2	4	C_4
$1, 3, 5, 7$	1	8	$\mathbb{Z}_8$

2. Here we find all the subgroups of $\mathbb{Z}_{30}$. Note that $30 = 2 \cdot 3 \cdot 5$. We list all the elements of $\mathbb{Z}_{30}$ according to their greatest common divisor with 30, and then the subgroup generated by each. According to the above results, each subgroup in the right column is generated by *any* of the numbers in the left column.

x	$\gcd(x, 30)$	$30/\gcd(x, 30)$	subgroup generated $\langle x \rangle$
$0(30)$	$0(30)$	1	C_1
15	15	2	C_2
$10, 20$	10	3	C_3
$6, 12, 18, 24$	6	5	C_5
$5, 25$	5	6	C_6
$3, 9, 21, 27$	3	10	C_{10}
$2, 4, 8, 14, 16, 22, 26, 28$	2	15	C_{15}
$1, 7, 11, 13, 17, 19, 23, 29$	1	30	$\mathbb{Z}_{30}$

Here is the subgroup diagram for $\mathbb{Z}_{30}$ with the obvious generator chosen for each subgroup.



3.4 Generating sets — non-examinable

Definition 3.9. If $X \subseteq G$ is a *subset* of a group G then the subgroup of G generated by X is the subgroup created by making all possible combinations of elements and inverses of elements in X. The subgroup generated by X will be written

$$\langle x \in X \rangle$$

G is *finitely generated* if there exists a finite subset of G which generates G.

The subgroup of G generated by X really is a subgroup: it is certainly a subset, so we need only check that it is closed under multiplication and inverses. However, the definition says that we keep throwing things into the subgroup so that it satisfies precisely these conditions!

Examples

1. $(\mathbb{Z}, +) = \langle 2, 3 \rangle$. The inverse of $2 = -2$ must lie in $\langle 2, 3 \rangle$. But then $3 + (-2) = 1 \in \langle 2, 3 \rangle$. Since 1 generates $\mathbb{Z}$, we are done.

2. In general if $m, n \in \mathbb{Z}$ then the subgroup $\langle m, n \rangle = \{\lambda m + \mu n : \lambda, \mu \in \mathbb{Z}\}$ is $\langle d \rangle = d\mathbb{Z}$ where $d = \gcd(m, n)$.

3. The dihedral group of rotations and reflections of a regular n-gon can be seen to be generated by the 1-step rotation ρ_1 and *any* reflection μ: that is $D_n = \langle \rho_1, \mu \rangle$.

4. $(\mathbb{Q}, +) = \left\langle \frac{1}{n} : n \in \mathbb{Z}^+ \right\rangle$. $(\mathbb{Q}, +)$ is not finitely generated: there exists no finite subset which generates $\mathbb{Q}$. To see this, consider the subgroup generated by some finite set $X = \{\frac{m_i}{n_i}\}_{i=1}^{k}$.Now let p be a prime which does not divide *any* of the denominators n_i (there are infinitely many primes and each n_i can have only finitely many divisors…). It is then impossible to create the fraction $\frac{1}{p}$ from the set X.
   If this seems a little tricky, consider that if $X = \{\frac{1}{2}, \frac{1}{3}\}$, then

   $$\langle x \in X \rangle = \left\{ \frac{3m + 2n}{6} : m, n \in \mathbb{Z} \right\} = \left\{ \frac{k}{6} : k \in \mathbb{Z} \right\}$$

   for reasons similar to example 2. Clearly this subgroup does not contain $\frac{1}{5}$.

4 Direct products

4.1 Definition and Examples

Direct products are a straightforward way to define new groups from old. The simplest example is the Cartesian product $\mathbb{Z}_2 \times \mathbb{Z}_2$. Writing $\mathbb{Z}_2 = \{0, 1\}$, we see that

$$\mathbb{Z}_2 \times \mathbb{Z}_2 = \{(0,0), (0,1), (1,0), (1,1)\}$$

has four elements. This set can be given a *group structure* in an obvious way. Simply define

$$(p, q) + (r, s) := (p + r, q + s)$$

where $p + r$ and $q + s$ are computed in $\mathbb{Z}_2$. This is clearly a binary operation on $\mathbb{Z}_2 \times \mathbb{Z}_2$. It is straightforward to check that this operation *defines* a group. Indeed, we obtain the following Cayley table:

$+$	$(0,0)$	$(0,1)$	$(1,0)$	$(1,1)$
$(0,0)$	$(0,0)$	$(0,1)$	$(1,0)$	$(1,1)$
$(0,1)$	$(0,1)$	$(0,0)$	$(1,1)$	$(1,0)$
$(1,0)$	$(1,0)$	$(1,1)$	$(0,0)$	$(0,1)$
$(1,1)$	$(1,1)$	$(1,0)$	$(0,1)$	$(0,0)$

This should look familiar: it is exactly the Cayley table for the Klein 4-group: $\mathbb{Z}_2 \times \mathbb{Z}_2 \cong V$. This construction works in general.

Theorem 4.1. *Let $G_1, \ldots, G_n$ be multiplicative groups. The binary operation*

$$(a_1, \ldots, a_n) \cdot (b_1, \ldots, b_n) := (a_1 b_1, \ldots, a_n b_n)$$

induces a group structure on the set $G_1 \times \cdots \times G_n$.

Definition 4.2. The group $G_1 \times \cdots \times G_n$ is the *direct product* of the groups $G_1, \ldots, G_n$.

If the groups $G_1, \ldots, G_n$ are additive, then the operation will also be written additively.
It is immediate that a direct product has cardinality equal to the product of the cardinalities of $G_1, \ldots, G_n$.

Proof of Theorem. Simply check the group axioms.

Closure Since each $a_i b_i \in G_i$ this is immediate.

Associativity Each G_i is associative: it is a short calculation to see that the associativity condition on the whole direct product is equivalent to each individual G_i being associative.

Identity If e_i is the identity in G_i, then $(e_1, \ldots, e_n)$ is the identity in the direct product.

Inverse $(a_1, \ldots, a_n)^{-1} = (a_1^{-1}, \ldots, a_n^{-1})$.

■

The proof uses nothing beyond the fact that each factor G_i is a group in its own right—this should not be surprising as we have no other information to work with! In particular you should note that the individual groups G_i do not interact with each other.

Examples

1. $\mathbb{Z}_2 \times \mathbb{Z}_3 = \{(0,0), (0,1), (0,2), (1,0), (1,1), (1,2)\}$ under addition $(+_2, +_3)$. Observe that if we choose $a = (1,1)$, then the group can be written (in the above order) as $\{e, 4a, 2a, 3a, a, 5a\}$. Thus $\mathbb{Z}_2 \times \mathbb{Z}_3$ is generated by a and is therefore cyclic. Being a cyclic group of order 6, we necessarily have $\mathbb{Z}_2 \times \mathbb{Z}_3 \cong \mathbb{Z}_6$.

2. The direct sum of vector spaces $W = U \oplus V$ is a more general example. Indeed in linear algebra it is typical to use direct sum notation rather than Cartesian products. For example the direct sum of n copies of the real line $\mathbb{R}$ is the familiar vector space

$$\mathbb{R}^n = \bigoplus_{i=1}^{n} \mathbb{R} = \mathbb{R} \oplus \cdots \oplus \mathbb{R}$$

4.2 Orders of elements in direct products

In $\mathbb{Z}_{12}$ the element 10 has order $6 = \frac{12}{\gcd(10,12)}$, while in $\mathbb{Z}_8$ the element 2 has order 4. What is the order of the element $(10,2) \in \mathbb{Z}_{12} \times \mathbb{Z}_8$? Simply compute the cyclic group generated by this element:

$$\langle (10,2) \rangle = \Big\{ (10,2), (8,4), (6,6), (4,0), (2,2), (0,4), (10,6), (8,0), (6,2), (4,4), (2,6), (0,0) \Big\}$$

The order is therefore 12. If you consider what happens to each of the entries of each pair, it should be obvious that the order is the *least common multiple* of the orders of the originals: $12 = \text{lcm}(6,4)$. In general we have the following.

Theorem 4.3. *Suppose that $a_i \in G_i$ has order r_i for each i. Then $(a_1, \ldots, a_n) \in G_1 \times \cdots \times G_n$ has order $\text{lcm}(r_1, \ldots, r_n)$.*

Proof. We simply compute the order:

$$\begin{aligned} (a_1, \ldots, a_n)^k = (a_1^k, \ldots, a_n^k) = (e_1, e_2, \ldots, e_n) &\iff \forall i,\ a_i^k = e_i \\ &\iff \forall i,\ r_i \mid k \end{aligned}$$

The order is the minimal positive integer k satisfying the above, which is precisely

$$k = \text{lcm}(r_1, \ldots, r_n)$$

■

Example What is the order of[20] $(1,4,3,2) \in \mathbb{Z}_4 \times \mathbb{Z}_7 \times \mathbb{Z}_5 \times \mathbb{Z}_{20}$?
Recalling that the order of $x \in \mathbb{Z}_n$ is $\frac{n}{\gcd(x,n)}$ we see that the above elements have orders 4, 7, 5 and 10 respectively. Thus the order of $(1,4,3,2)$ is $\text{lcm}(4,7,5,10) = 140$.

4.3 Finite(ly generated) abelian groups

We have already seen that all finite cyclic groups are isomorphic to some $\mathbb{Z}_n$. As we shall see in a moment, all *finite abelian* groups are isomorphic to direct products of these.
We have already seen that $\mathbb{Z}_2 \times \mathbb{Z}_3 \cong \mathbb{Z}_6$ but that $\mathbb{Z}_2 \times \mathbb{Z}_2 \ncong \mathbb{Z}_4$. What is the pattern here? Your gut should suspect that it has something to do with the fact that 2 and 3 are *relatively prime.*

Theorem 4.4. *$\mathbb{Z}_m \times \mathbb{Z}_n$ is cyclic $\iff$ $\gcd(m,n) = 1$, specifically,*

$$\mathbb{Z}_m \times \mathbb{Z}_n \cong \mathbb{Z}_{mn} \iff \gcd(m,n) = 1$$

More generally,

$$\mathbb{Z}_{m_1} \times \cdots \times \mathbb{Z}_{m_k} \cong \mathbb{Z}_{m_1 \cdots m_k} \iff \gcd(m_i, m_j) = 1,\ \forall i \neq j$$

Moreover if $n = p_1^{r_1} \cdots p_k^{r_k}$ is the unique prime factorization of an integer n, then

$$\mathbb{Z}_n \cong \mathbb{Z}_{p_1^{r_1}} \times \cdots \times \mathbb{Z}_{p_k^{r_k}}$$

[20] Note that $(1,4,3,2)$ is really a quadruple of *equivalence classes* $([1]_4, [4]_7, [3]_5, [2]_{20})$.

Proof. This is merely a corollary of Theorem 4.3. For brevity we just prove the first part: the remainder follows by induction.
If $\gcd(m,n) = 1$, then the element $(1,1) \in \mathbb{Z}_m \times \mathbb{Z}_n$ has order

$$\operatorname{lcm}(m,n) = \frac{mn}{\gcd(m,n)}$$

Hence $(1,1)$ is a generator of $\mathbb{Z}_m \times \mathbb{Z}_n$, which is then *cyclic*.
Conversely, suppose $\gcd(m,n) = d \geq 2$. Then the maximum order of an element $(p,q) \in \mathbb{Z}_m \times \mathbb{Z}_n$ is

$$\operatorname{lcm}(m,n) = \frac{mn}{\gcd(m,n)} = \frac{mn}{d} < mn$$

It follows that $\mathbb{Z}_m \times \mathbb{Z}_n$ is not cyclic.

■

Example Is $\mathbb{Z}_5 \times \mathbb{Z}_{12} \times \mathbb{Z}_{43}$ cyclic? The Theorem says yes, since no pairs of the numbers 5, 12, 43 have any common factors. It is ghastly to write out, but there are 15 different ways (up to reordering) of expressing this group!

$$\begin{aligned}
\mathbb{Z}_{2580} &\cong \mathbb{Z}_3 \times \mathbb{Z}_{860} \cong \mathbb{Z}_4 \times \mathbb{Z}_{645} \cong \mathbb{Z}_5 \times \mathbb{Z}_{516} \cong \mathbb{Z}_{43} \times \mathbb{Z}_{60} \\
&\cong \mathbb{Z}_{12} \times \mathbb{Z}_{215} \cong \mathbb{Z}_{15} \times \mathbb{Z}_{172} \cong \mathbb{Z}_{20} \times \mathbb{Z}_{129} \\
&\cong \mathbb{Z}_3 \times \mathbb{Z}_4 \times \mathbb{Z}_{215} \cong \mathbb{Z}_3 \times \mathbb{Z}_5 \times \mathbb{Z}_{172} \cong \mathbb{Z}_3 \times \mathbb{Z}_{20} \times \mathbb{Z}_{43} \\
&\cong \mathbb{Z}_4 \times \mathbb{Z}_5 \times \mathbb{Z}_{129} \cong \mathbb{Z}_4 \times \mathbb{Z}_{15} \times \mathbb{Z}_{43} \cong \mathbb{Z}_5 \times \mathbb{Z}_{12} \times \mathbb{Z}_{43} \\
&\cong \mathbb{Z}_3 \times \mathbb{Z}_4 \times \mathbb{Z}_5 \times \mathbb{Z}_{43}
\end{aligned}$$

Direct products of cyclic groups have a universal application here. As the next Theorem shows, *every* finitely generated abelian group is isomorphic to a direct product of cyclic groups.

Theorem 4.5 (Fundamental Theorem of finitely generated Abelian groups)**.** *Every finitely generated abelian group is isomorphic to a group of the form*

$$\mathbb{Z}_{p_1^{r_1}} \times \cdots \times \mathbb{Z}_{p_n^{r_n}} \times \mathbb{Z} \times \cdots \times \mathbb{Z}$$

where the p_i are (not necessarily distinct) primes, the r_i are positive integers and there are finitely many factors of $\mathbb{Z}$.

The proof is far too difficult for this course. Its purpose here is to allow us to classify finite abelian groups up to isomorphism. Recall the optional section on *generating sets* to remind yourself of what *finitely generated* means: the above direct product is only a finite group if it has no factors of $\mathbb{Z}$.

Example Find, up to isomorphism, all abelian groups of order 450. First note that $450 = 2 \cdot 3^2 \cdot 5^2$. Now apply the fundamental theorem to see that the complete list is

1. $\mathbb{Z}_{450} \cong \mathbb{Z}_2 \times \mathbb{Z}_{3^2} \times \mathbb{Z}_{5^2}$
2. $\mathbb{Z}_2 \times \mathbb{Z}_3 \times \mathbb{Z}_3 \times \mathbb{Z}_{5^2}$
3. $\mathbb{Z}_2 \times \mathbb{Z}_{3^2} \times \mathbb{Z}_5 \times \mathbb{Z}_5$

4. $\mathbb{Z}_2 \times \mathbb{Z}_3 \times \mathbb{Z}_3 \times \mathbb{Z}_5 \times \mathbb{Z}_5$

Theorem 4.6. *If m is a square free integer ($\nexists k \in \mathbb{Z}_{\geq 2}$ such that $k^2 \mid m$) then there is only one abelian group of order m (up to isomorphism).*

Proof. By the Fundamental Theorem such a group G must be isomorphic to some $\mathbb{Z}_{p_1^{r_1}} \times \cdots \times \mathbb{Z}_{p_n^{r_n}}$ with $m = p_1^{r_1} \cdots p_n^{r_n}$. But m being square free implies that every exponent s_i is equal to 1 and all the primes p_i are distinct. By Theorem 4.4 we have $G \cong \mathbb{Z}_{p_1 \cdots p_n} = \mathbb{Z}_m$. ∎

All groups of small order

As examples of the above we list all the groups of orders 1 through 15 and the abelian groups of order 16 up to isomorphism. The Fundamental Theorem gives us all abelian groups. In particular observe where Theorem 4.6 applies. There are three groups we haven't previously encountered: the *Quaternion group* Q_8, the *Alternating group* A_4, and the *Dicyclic group* Dic_3. We will consider the alternating group properly later, the others you can look up if you're interested. There are *nine* non-abelian groups of order 16 up to isomorphism, six of which we have no notation for in this class! You may be suspicious from looking at the table that there are no non-abelian groups of any odd order. This is not so, but you need to go to order 21 before you find one.

Order	Abelian	Non-Abelian
1	$\mathbb{Z}_1$	
2	$\mathbb{Z}_2$	
3	$\mathbb{Z}_3$	
4	$\mathbb{Z}_4,\ V \cong \mathbb{Z}_2 \times \mathbb{Z}_2$	
5	$\mathbb{Z}_5$	
6	$\mathbb{Z}_6 \cong \mathbb{Z}_2 \times \mathbb{Z}_3$	$D_3 \cong S_3$
7	$\mathbb{Z}_7$	
8	$\mathbb{Z}_8,\ \mathbb{Z}_2 \times \mathbb{Z}_4,\ \mathbb{Z}_2 \times \mathbb{Z}_2 \times \mathbb{Z}_2$	$D_4,\ Q_8 \cong Dic_2$
9	$\mathbb{Z}_9,\ \mathbb{Z}_3 \times \mathbb{Z}_3$	
10	$\mathbb{Z}_{10} \cong \mathbb{Z}_2 \times \mathbb{Z}_5$	D_5
11	$\mathbb{Z}_{11}$	
12	$\mathbb{Z}_{12} \cong \mathbb{Z}_3 \times \mathbb{Z}_4,\ \mathbb{Z}_2 \times \mathbb{Z}_6 \cong \mathbb{Z}_2 \times \mathbb{Z}_2 \times \mathbb{Z}_3$	$D_6,\ A_4,\ Dic_3$
13	$\mathbb{Z}_{13}$	
14	$\mathbb{Z}_{14} \cong \mathbb{Z}_2 \times \mathbb{Z}_7$	D_7
15	$\mathbb{Z}_{15} \cong \mathbb{Z}_3 \times \mathbb{Z}_5$	
16	$\mathbb{Z}_{16},\ \mathbb{Z}_4 \times \mathbb{Z}_4,\ \mathbb{Z}_2 \times \mathbb{Z}_8,\ \mathbb{Z}_2 \times \mathbb{Z}_2 \times \mathbb{Z}_4,\ \mathbb{Z}_2 \times \mathbb{Z}_2 \times \mathbb{Z}_2 \times \mathbb{Z}_2$	Many

5 Permutations and Orbits

In the earliest conceptions of group theory, all groups were considered *permutation groups.* Essentially a group was a collection of ways in which one could rearrange some set or object: for example, each 'rearrangement' of an equilateral triangle corresponds to one of its *symmetries.* It was Arthur Cayley, of Cayley-table fame, who formulated the group axioms we now use. Importantly, he also proved what is now known as *Cayley's Theorem:* that the old definition and the new are identical.

5.1 The Symmetric Group

So what, first, is a permutation?

Definition 5.1. A *permutation* of a set A is a bijection $\varphi : A \to A$.

Theorem 5.2. *If A is any set, then the set of permutations S_A of A forms a group under composition.*

Proof. We check the axioms:

Closure If φ, ψ are bijective then so is the composition $\varphi \circ \psi$. ✓

Associativity Permutations are functions, the composition of which we know to be associative. ✓

Identity The *identity function* id_A maps all elements of A to themselves: $\mathrm{id}_A : x \mapsto x$. This is certainly bijective. ✓

Inverse If φ is a permutation then it is a bijection, whence the *function* φ^{-1} exists and is also a bijection. ✓

■

Definition 5.3. The *symmetric group on n-letters* S_n is the group of permutations of any[21] set A of n elements. Typically we choose $A = \{1, 2, \ldots, n\}$.

Basic combinatorics should make the following obvious:

Lemma 5.4. *S_n has $n!$ elements.*[22]

To describe a group as a *permutation group* simply means that each element of the group is being viewed as a permutation of some set. As the following result shows, all groups are permutation groups, although sadly not in a particularly useful way!

Theorem 5.5 (Cayley's Theorem)**.** *Every group G is isomorphic to a group of permutations.*

Proof. For each element $a \in G$, let $\rho_a : G \to G$ be the function $\rho_a : g \mapsto ag$ (i.e. left multiplication by a). We make two claims:

1. Each ρ_a is a permutation of G.
2. $\big(\{\rho_a : a \in G\}, \circ\big)$ forms a group isomorphic to G.

The first claim is straightforward. $\rho_{a^{-1}}$ is the inverse function to ρ_a:

$$\forall g \in G, \quad (\rho_{a^{-1}} \circ \rho_a)(g) = a^{-1}ag = g = \mathrm{id}_G(g)$$

whence each ρ_a is a bijection.
Now define a map $\phi : G \to \{\rho_a\}$ by $\phi(a) = \rho_a$. We claim this is an isomorphism:

1–1 $\phi(a) = \phi(b) \implies \rho_a = \rho_b \implies \forall g \in G,\ ag = bg \implies a = b$. ✓

Onto Certainly every permutation ρ_a is in the image of ϕ. ✓

Homomorphism If $a, b \in G$, then

$$\phi(a) \circ \phi(b) : g \mapsto \rho_a(\rho_b(g)) = abg = \rho_{ab}(g)$$

from which $\phi(ab) = \phi(a) \circ \phi(b)$.

■

Note that Cayley's Theorem is *not* saying that every group is isomorphic to some S_n. It is saying that every group G is isomorphic to some *subgroup* of S_G.

[21] S_n is the *explicit* group of permutations of $\{1, 2, \ldots, n\}$ or the *abstract* group of permutations of any set with n elements.
[22] In contrast to C_n or $\mathbb{Z}_n$ where the subscript is the order of the group.

Three notations for permutations

Standard notation Suppose that $\sigma \in S_4$ is the following map

$$\sigma : \begin{pmatrix} 1 \\ 2 \\ 3 \\ 4 \end{pmatrix} \mapsto \begin{pmatrix} 3 \\ 1 \\ 4 \\ 2 \end{pmatrix}, \quad \text{i.e.} \quad \sigma(1) = 3,\ \sigma(2) = 1,\ \sigma(3) = 4,\ \sigma(4) = 2$$

We could then write

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

where you read down columns to find where σ maps an element in the top row. Composition is read in the usual way for functions, do the right permutation first. Thus if

$$\rho = \begin{pmatrix} 1 & 2 & 3 & 4 \\ 1 & 4 & 3 & 2 \end{pmatrix} \quad \text{then} \quad \sigma\rho = \begin{pmatrix} 1 & 2 & 3 & 4 \\ 3 & 1 & 4 & 2 \end{pmatrix} \begin{pmatrix} 1 & 2 & 3 & 4 \\ 1 & 4 & 3 & 2 \end{pmatrix} = \begin{pmatrix} 1 & 2 & 3 & 4 \\ 3 & 2 & 4 & 1 \end{pmatrix} \qquad (*)$$

Matrix Notation σ can also be viewed as acting on the vector $(1, 2, 3, 4)^T$, which suggests a matrix method for encoding elements of S_n. For example, our permutation σ may be written

$$\sigma = \begin{pmatrix} 0 & 0 & 1 & 0 \\ 1 & 0 & 0 & 0 \\ 0 & 0 & 0 & 1 \\ 0 & 1 & 0 & 0 \end{pmatrix}$$

as a *permutation matrix:* multiplying on the left by such a matrix permutes the entries of vectors.

Definition 5.6. A *permutation matrix* is an $n \times n$ matrix with exactly one entry of 1 in each row and column and the remaining entries 0.

Indeed we may conclude:

Theorem 5.7. *The set of $n \times n$ permutation matrices forms a group under multiplication which is isomorphic to S_n. By Cayley's Theorem, every finite group of permutations is isomorphic to a group of matrices.*

Cycle notation Our example permutation can be more compactly written as $\sigma = (1\,3\,4\,2)$. We read from left to right, looping back to 1 at the end, each entry telling us where the previous is mapped to. Thus $(1\,3\,4\,2)$ maps

$$1 \mapsto 3 \mapsto 4 \mapsto 2 \mapsto 1$$

We have shorter cycles if some of the elements are fixed; for example in our two notations

$$(1\,3) = \begin{pmatrix} 1 & 2 & 3 & 4 \\ 3 & 2 & 1 & 4 \end{pmatrix} \in S_4$$

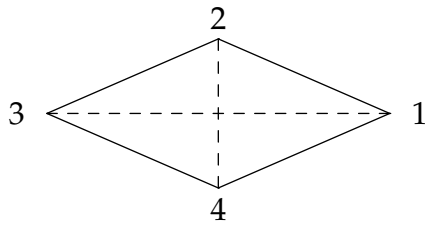
Juxtaposition is used for composition:

$$(1\,3\,4\,2)(2\,4) = (1\,3\,4)$$

(compare with $(*)$ above).
Remember that multiplication of cycles is really composition of functions: although each *cycle* is read from left to right when determining how it acts on elements of $\{1, 2, \ldots, n\}$, we multiply cycles by considering the *rightmost* cycle first. For example, in S_5,

$$(1\,3\,5\,4)(2\,3\,4) : \begin{cases} 1 \mapsto 3 \\ 2 \mapsto 3 \mapsto 5 \\ 3 \mapsto 4 \mapsto 1 \\ 4 \mapsto 2 \\ 5 \mapsto 4 \end{cases} \implies (1\,3\,5\,4)(2\,3\,4) = (1\,3)(2\,5\,4) \qquad (\dagger)$$

This notation can be used to describe non-symmetric groups: e.g. if we label the corners of a rhombus, the Klein 4-group V can be written in terms of cycles as a subgroup of S_4.



$$V = \{e, (1\,3), (2\,4), (1\,3)(2\,4)\}$$

Definition 5.8. Suppose that $k \leq n$. A *k-cycle* in S_n is an element $(a_1\, a_2 \cdots a_k)$.
Cycles $(a_1 \cdots a_k)$ and $(b_1 \cdots b_l)$ are *disjoint* if no element appears in both cycles: that is, if

$$\{a_1, \ldots, a_k\} \cap \{b_1, \ldots, b_l\} = \emptyset$$

The identity element is the only 0-cycle. It is sometimes written $()$, if not otherwise denoted by e.

As the example $(\dagger)$ illustrates, when computing the product of several cycles, the result will typically be a product of disjoint cycles. This will prove very useful in the next section when we discuss *orbits*.

Subgroup relations between symmetric groups It is easy to see that $S_m \leq S_n \iff m \leq n$. For example, fix the final $n - m$ elements of $\{1, \ldots, n\}$ so that

$$S_m = \{\sigma \in S_n : \sigma(i) = i,\ \forall i > m\}.$$

In fact S_m is a subgroup of S_n in precisely $\binom{n}{m}$ different ways: each copy of S_m arises by fixing $n - m$ elements of the set $\{1, \ldots, n\}$: there are precisely $\binom{n}{n-m} = \binom{n}{m}$ ways of choosing these fixed elements.

5.2 Dihedral groups

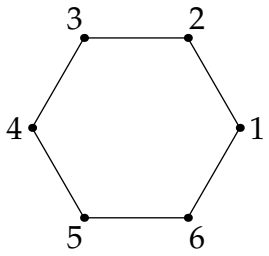
Definition 5.9. The *dihedral group* D_n is the group of symmetries of the regular n-gon (polygon with n sides).

Group? Now that we have defined permutation groups it is very easy to see that the dihedral groups are indeed groups. Observe that a symmetry of an n-gon can be viewed as a permutation of the corners of the n-gon for which 'neighborliness' is preserved. This is similar to how we viewed the Klein 4-group above.

For example, if we label the corners of the regular hexagon 1 through 6 then we see that D_6 is the set of $\sigma \in S_6$ such that $\sigma(1)$ is always next to $\sigma(6)$ and $\sigma(2)$, etc.

Clearly this says that $D_6 \subseteq S_6$.

To see that D_6 is a subgroup of S_6, we need only note that the composition of two neighbor-preserving transforms must also preserves neighbors, as does the inverse of such a map.



Elements of D_n The regular n-gon has $2n$ distinct symmetries and so $|D_n| = 2n$. These consist of:

n rotations For each $j = 0, \ldots, n-1$, let ρ_j be rotation counter-clockwise by $\frac{2\pi j}{n}$ radians.

n reflections Let μ_j be reflection across the line making angle $\frac{\pi j}{n}$ with the positive x-axis (make sure you put one of the corners of the n-gon on the x-axis!).[23]

Remarks Some authors write D_{2n} instead of D_n precisely because $|D_n| = 2n$: in this course, D_n will *always* mean the symmetries of the n-gon.

Every dihedral group D_n is a subgroup of the orthogonal group $\mathrm{O}_2(\mathbb{R})$. The correspondence is:

$$\rho_j = \begin{pmatrix} \cos\left(\frac{2\pi j}{n}\right) & -\sin\left(\frac{2\pi j}{n}\right) \\ \sin\left(\frac{2\pi j}{n}\right) & \cos\left(\frac{2\pi j}{n}\right) \end{pmatrix} \qquad \mu_j = \begin{pmatrix} \cos\left(\frac{2\pi j}{n}\right) & \sin\left(\frac{2\pi j}{n}\right) \\ \sin\left(\frac{2\pi j}{n}\right) & -\cos\left(\frac{2\pi j}{n}\right) \end{pmatrix}$$

It is a good exercise to convince yourself that these matrices really do correspond to the rotations and reflections claimed. In particular multiply any two of them together and see what you get…

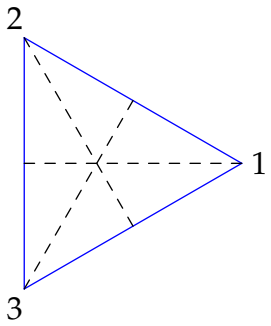
Subgroup relations between dihedral groups

$D_m \leq D_n \iff m \mid n$. Recall the discussion of geometric proofs earlier where we saw that $D_3 \leq D_6$. For instance, we can join every $(n/m)^{\text{th}}$ vertex of a regular n-gon to obtain a regular m-gon. Every symmetry of the m-gon is then a symmetry of the n-gon.

[23] For *even*-sided polygons these are often labelled differently, and split into two subsets of $\frac{n}{2}$ reflections each. The reflections μ_i are those which move *all* the corners of the n-gon, while δ_i refers to a reflection across a *diagonal.* We will see this in our treatment of D_4 below. In the abstract, is is simpler not to distinguish between these reflections.

Explicit descriptions of D_3 and D_4

D_3 is the group of symmetries of an equilateral triangle. If we label the corners as in the picture, we can easily define the elements of the group.



- ρ_0 the identity
- ρ_1 rotate counter-clockwise by $\frac{2\pi}{3}$ radians
- ρ_2 rotate clockwise by $\frac{2\pi}{3}$ radians
- μ_i reflect in the altitude through i

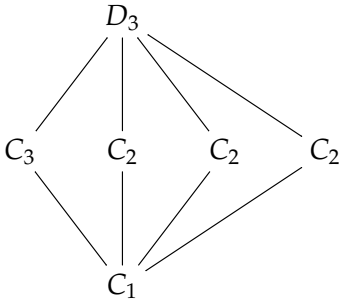
Here we write all the elements in permutation notation ad give the Cayley table.

$\circ$	ρ_0	ρ_1	ρ_2	μ_1	μ_2	μ_3
ρ_0	ρ_0	ρ_1	ρ_2	μ_1	μ_2	μ_3
ρ_1	ρ_1	ρ_2	ρ_0	μ_3	μ_1	μ_2
ρ_2	ρ_2	ρ_0	ρ_1	μ_2	μ_3	μ_1
μ_1	μ_1	μ_2	μ_3	ρ_0	ρ_1	ρ_2
μ_2	μ_2	μ_3	μ_1	ρ_2	ρ_0	ρ_1
μ_3	μ_3	μ_1	μ_2	ρ_1	ρ_2	ρ_0

Element		Standard notation	Cycle notation
Rotations	ρ_0	$\begin{pmatrix}1&2&3\\1&2&3\end{pmatrix}$	$e = ()$
	ρ_1	$\begin{pmatrix}1&2&3\\2&3&1\end{pmatrix}$	(123)
	ρ_2	$\begin{pmatrix}1&2&3\\3&1&2\end{pmatrix}$	(132)
Reflections	μ_1	$\begin{pmatrix}1&2&3\\1&3&2\end{pmatrix}$	(23)
	μ_2	$\begin{pmatrix}1&2&3\\3&2&1\end{pmatrix}$	(13)
	μ_3	$\begin{pmatrix}1&2&3\\2&1&3\end{pmatrix}$	(12)

It should be immediately obvious that all the permutations of $\{1,2,3\}$ are elements of D_3, and so $D_3 \cong S_3$. Now we consider all the subgroups of D_3 and its subgroup diagram.

Subgroup	Isomorph	Generating sets
$\{\rho_0\}$	C_1	$\{\rho_0\}$
$\{\rho_0, \mu_1\}$	C_2	$\{\mu_1\}$
$\{\rho_0, \mu_2\}$	C_2	$\{\mu_2\}$
$\{\rho_0, \mu_3\}$	C_2	$\{\mu_3\}$
$\{\rho_0, \rho_1, \rho_2\}$	C_3	$\{\rho_1\}$, or $\{\rho_2\}$
D_3	S_3	any pair $\{\rho_i, \mu_j\}$ where $i = 1,2$ and $j = 1,2,3$

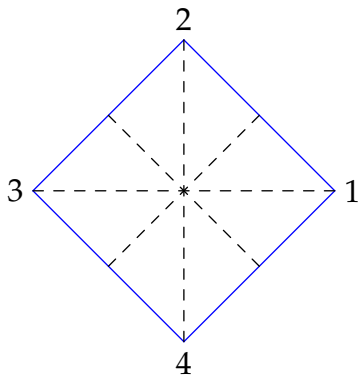


How can we be certain that there are no other subgroups of D_3? A careful consideration of generating sets should convince you. For example, suppose that a subgroup contains two reflections: WLOG suppose these are μ_1, μ_2. We compute the subgroup generated by $\{\mu_1, \mu_2\}$. It must include

$$\mu_1\mu_2 = \rho_1, \qquad \rho_1^2 = \rho_2 \qquad \mu_1\rho_1 = \mu_3$$

and thus the entire group.

D_4 is the group of symmetries of the square. It consists of four rotations and four reflections: the notation δ_j for reflection across a diagonal is used here, rather than labelling all reflections μ_j.



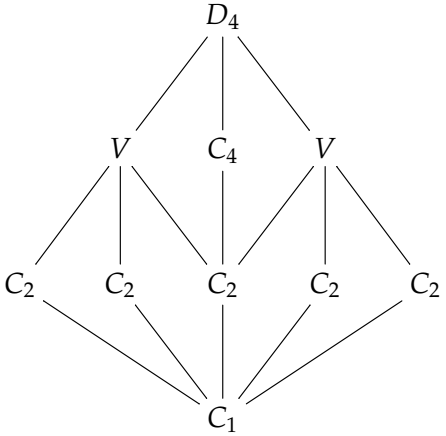
- ρ_0 the identity
- ρ_1 rotate counter-clockwise by $\frac{\pi}{2}$ radians
- ρ_2 rotate counter-clockwise by π radians
- ρ_3 rotate counter-clockwise by $\frac{3\pi}{2}$ radians
- μ_i reflect across midpoints of sides
- δ_i reflect across diagonals

$\circ$	ρ_0	ρ_1	ρ_2	ρ_3	μ_1	μ_2	δ_1	δ_2
ρ_0	ρ_0	ρ_1	ρ_2	ρ_3	μ_1	μ_2	δ_1	δ_2
ρ_1	ρ_1	ρ_2	ρ_3	ρ_0	δ_2	δ_1	μ_1	μ_2
ρ_2	ρ_2	ρ_3	ρ_0	ρ_1	μ_2	μ_1	δ_2	δ_1
ρ_3	ρ_3	ρ_0	ρ_1	ρ_2	δ_1	δ_2	μ_2	μ_1
μ_1	μ_1	δ_1	μ_2	δ_2	ρ_0	ρ_2	ρ_1	ρ_3
μ_2	μ_2	δ_2	μ_1	δ_1	ρ_2	ρ_0	ρ_3	ρ_1
δ_1	δ_1	μ_2	δ_2	μ_1	ρ_3	ρ_1	ρ_0	ρ_2
δ_2	δ_2	μ_1	δ_1	μ_2	ρ_1	ρ_3	ρ_2	ρ_0

Element		Standard notation	Cycle notation
Rotations	ρ_0	$\begin{pmatrix}1&2&3&4\\1&2&3&4\end{pmatrix}$	$e = ()$
	ρ_1	$\begin{pmatrix}1&2&3&4\\2&3&4&1\end{pmatrix}$	(1234)
	ρ_2	$\begin{pmatrix}1&2&3&4\\3&4&1&2\end{pmatrix}$	$(13)(24)$
	ρ_3	$\begin{pmatrix}1&2&3&4\\4&1&2&3\end{pmatrix}$	(1432)
Reflections	μ_1	$\begin{pmatrix}1&2&3&4\\2&1&4&3\end{pmatrix}$	$(12)(34)$
	μ_2	$\begin{pmatrix}1&2&3&4\\4&3&2&1\end{pmatrix}$	$(14)(23)$
	δ_1	$\begin{pmatrix}1&2&3&4\\1&4&3&2\end{pmatrix}$	(24)
	δ_2	$\begin{pmatrix}1&2&3&4\\3&2&1&4\end{pmatrix}$	(13)

All the subgroups are summarised in the following table. In particular, note that $D_4 \ncong S_4$: the latter has many more elements!

Subgroup	Isomorph	Generating sets
$\{\rho_0\}$	C_1	$\{\rho_0\}$
$\{\rho_0, \mu_i\}$	C_2	$\{\mu_i\}$ for each i
$\{\rho_0, \delta_i\}$	C_2	$\{\delta_i\}$ for each i
$\{\rho_0, \rho_2\}$	C_2	$\{\rho_2\}$
$\{\rho_0, \rho_1, \rho_2, \rho_3\}$	C_4	$\{\rho_1\}$ or $\{\rho_3\}$
$\{\rho_0, \mu_1, \mu_2, \rho_2\}$	V	$\{\mu_1, \mu_2\}$, $\{\mu_1, \rho_2\}$ or $\{\mu_2, \rho_2\}$
$\{\rho_0, \delta_1, \delta_2, \rho_2\}$	V	$\{\delta_1, \delta_2\}$, $\{\delta_1, \rho_2\}$ or $\{\delta_2, \rho_2\}$
D_4	D_4	any pair $\{\rho_i, \mu_j\}$ or $\{\rho_i, \delta_j\}$ where $i = 1, 3$ and $j = 1, 2$ or any pair $\{\mu_k, \delta_l\}$ where $k, l = 1, 2$



In the subgroup diagram, the middle C_2 is $\{\rho_0, \rho_2\}$ while the two copies on each side contain either the reflections δ_i or μ_i.

5.3 Orbits

In this section we continue the idea of a group being a set of permutations. In particular, we will see how any element $\sigma \in S_n$ partitions the set $\{1, 2, \ldots, n\}$. This concept will be generalized later when we consider group actions.

Definition 5.10. The *orbit* of $\sigma \in S_n$ containing $j \in \{1, 2, \ldots, n\}$ is the *set*

$$\text{orb}_j(\sigma) = \{\sigma^k(j) : k \in \mathbb{Z}\} \subseteq \{1, 2, \ldots, n\}$$

Observe that $\text{orb}_{\sigma^k(j)}(\sigma) = \text{orb}_j(\sigma)$ for *any* $k \in \mathbb{Z}$.
Be careful: each orbit is a subset of the set $\{1, 2, \ldots, n\}$, *not* of the group S_n.

Examples If $\sigma \in S_n$ is written in cycle notation (recall Definition 5.8) using *disjoint cycles,* then the cycles are the orbits! For example, in S_5,

Orbits of (134) are $\{1, 3, 4\}, \{2\}, \{5\}$
Orbits of $(12)(45)$ are $\{1, 2\}, \{3\}, \{4, 5\}$

The same does not hold if the cycles are not disjoint. For example, $\sigma = (13)(234) \in S_4$ maps

$$1 \mapsto 3 \mapsto 4 \mapsto 2 \mapsto 1$$

so there is only one orbit: $\text{orb}_j(\sigma) = \{1, 2, 3, 4\}$ for any j. In fact, $\sigma = (1234)$, from which the orbit is obvious.

Given that disjoint cycle notation is so useful for reading orbits, it is a natural question to ask if *any* permutation σ can be written as a product of disjoint cycles. The answer, of course, is yes, with the disjoint cycles turning out to be precisely the orbits of σ!

Theorem 5.11. *The orbits of any $\sigma \in S_n$ partition $X = \{1, 2, \ldots, n\}$.*

Proof. Define $\sim$ on $X = \{1, 2, \ldots, n\}$ by

$$x \sim y \iff y \in \text{orb}_x(\sigma)$$

We claim that $\sim$ is an equivalence relation.

Reflexivity $x \sim x$ since $x = \sigma^0(x)$. ✓

Symmetry $x \sim y \implies y = \sigma^k(x)$ for some $k \in \mathbb{Z}$. But then $x = \sigma^{-k}(y) \implies y \sim x$. ✓

Transitivity Suppose that $x \sim y$ and $y \sim z$. Then $y = \sigma^k(x)$ and $z = \sigma^l(y)$ for some $k, l \in \mathbb{Z}$. But then $z = \sigma^{k+l}(x)$ and so $x \sim z$. ✓

The equivalence classes of $\sim$ are clearly the orbits of σ, which therefore partition X. ∎

Corollary 5.12. *Every permutation can be written as a product of disjoint cycles.*

Proof. Write out each of the orbits of $\sigma \in S_n$ in order, placing each orbit in parentheses ( ). Since the orbits of σ partition $X = \{1, 2 \ldots, n\}$ the cycles obtained are disjoint.
More concretely,

$$\text{orb}_1(\sigma) = \{1, \sigma(1), \sigma^2(1), \ldots\}$$

If this orbit is the entirity of X, then we are finished. Otherwise, let

$$x_1 = \min\{x : x \notin \text{orb}_1(\sigma)\}$$

and construct its orbit:

$$\text{orb}_{x_1}(\sigma) = \{x_1, \sigma(x_1), \sigma^2(x_1), \ldots\}$$

This orbit must be disjoint with $\text{orb}_1(\sigma)$. Now repeat. It is immediate from the construction that

$$\sigma = \Big(1\ \sigma(1)\ \sigma^2(1)\ \cdots\Big)\Big(x_1\ \sigma(x_1)\ \sigma^2(x_1)\ \cdots\Big)\Big(\cdots\cdots\Big)$$

■

Examples If you mechanically follow the algorithm for multiplying cycles (see the previous section) you will automatically end up with a product of disjoint cycles:

1. $(13)(234)(1432) = (123)$
2. $(13)(24)(12)(34) = (14)(23)$

Note that disjoint cycles commute! E.g. $(14)(23) = (23)(14)$.

Now that we are able to write any permutation as a product of disjoint cycles, we are able to compute much more easily. For example:

Theorem 5.13. *The order of a permutation σ is the least common multiple of the lengths of its disjoint cycles.*

Proof. Write σ as a product of disjoint cycles $\sigma = \sigma_1 \cdots \sigma_m$. Since disjoint cycles commute, it it immediate that

$$\sigma^n = \sigma_1^n \cdots \sigma_m^n$$

Moreover, since the terms σ_j^n permute disjoint sets, it follows that

$$\sigma^n = e \iff \forall j,\ \sigma_j^n = e$$

A k-cycle clearly has order k (the least positive integer l such that $(a_1 \cdots a_k)^l = e$). If the orbits of σ have lengths $\alpha_j \in \mathbb{N}$ respectively, it follows that

$$\sigma_j^n = e \iff \alpha_j \mid n$$

Thus n must be a multiple of α_j for all j. The least such n is clearly $\text{lcm}\{\alpha_j\}$.

■

Example The order of $\sigma = (145)(3627)(89) \in S_9$ is $\text{lcm}(3,4,2) = 12$.
We can easily calculate σ^{3465} for the above σ. Since $3465 = 12 \cdot 288 + 9$ we have

$$\sigma^{3465} = (\sigma^{12})^{288}\sigma^9 = \sigma^9 = (145)^9(3627)^9(89)^9 = (3627)(89)$$

since (145), (3627) and (89) have orders 3, 4 and 2 respectively.

5.4 Transpositions

Instead of breaking a permutation σ into disjoint cycles, we can consider a permutation as being constructed from only the simplest bijections.

Definition 5.14. A 2-cycle (a_1a_2) is also known as a *transposition,* since it swaps two elements of $\{1, 2, \ldots, n\}$ and leaves the rest untouched.

Theorem 5.15. *Every $\sigma \in S_n$ is the product of transpositions.*

Proof. There are many, many ways to write out a single permutation as a product of transpositions. One method is to first write σ as a product of disjoint cycles, then write each cycle as follows:

$$(a_1 \cdots a_k) = (a_1a_k)(a_1a_{k-1}) \cdots (a_1a_2)$$

Just look carefully to see that this works!

■

Example $(17645) = (15)(14)(16)(17)$

Definition 5.16. A permutation $\sigma \in S_n$ is *even/odd* if it can be written as the product of an even/odd number of transpositions.

Theorem 5.17. *The concepts of even/odd are well-defined: every permutation is either even or odd, and not both.*

Proof. Recall that any permutation $\sigma \in S_n$ can be written as an $n \times n$ permutation matrix (Definition 5.6). A 2-cycle is a permutation matrix which swaps two rows: it therefore differs from the $n \times n$ identity matrix only in that two of its rows are swapped. For example

$$(24) = \begin{pmatrix} 1 & 0 & 0 & 0 \\ 0 & 0 & 0 & 1 \\ 0 & 0 & 1 & 0 \\ 0 & 1 & 0 & 0 \end{pmatrix} \in S_4$$

From linear algebra we have that swapping two rows of a matrix changes the sign of its determinant. Hence $\det(\text{2-cycle}) = -1$. It follows that

$$\det(\sigma) = \begin{cases} 1 \text{ if } \sigma \text{ is the product of an even number of 2-cycles,} \\ -1 \text{ if } \sigma \text{ is the product of an odd number of 2-cycles.} \end{cases}$$

In particular σ cannot be both odd and even.

■

5.5 The Alternating Groups

The concept of even permutations leads us to the definition of a new collection of groups.

Definition 5.18. The alternating group A_n ($n \geq 2$) is the group of even permutations in S_n.

Theorem 5.19. *A_n has exactly half the elements of S_n: that is $|A_n| = \frac{n!}{2}$.*

Proof. Since $n \geq 2$, we have $(12) \in S_n$. Define $\phi : A_n \to \{\text{odd permutations}\}$ by $\phi(\sigma) = (12)\sigma$. We claim that this is a bijection

1–1 $\phi(\sigma) = \phi(\tau) \implies (12)\sigma = (12)\tau \implies \sigma\tau$. ✓

Onto If ρ is an odd permutation, then $(12)\rho$ is even and so in A_n. Therefore $\rho = \phi((12)\rho)$. ✓

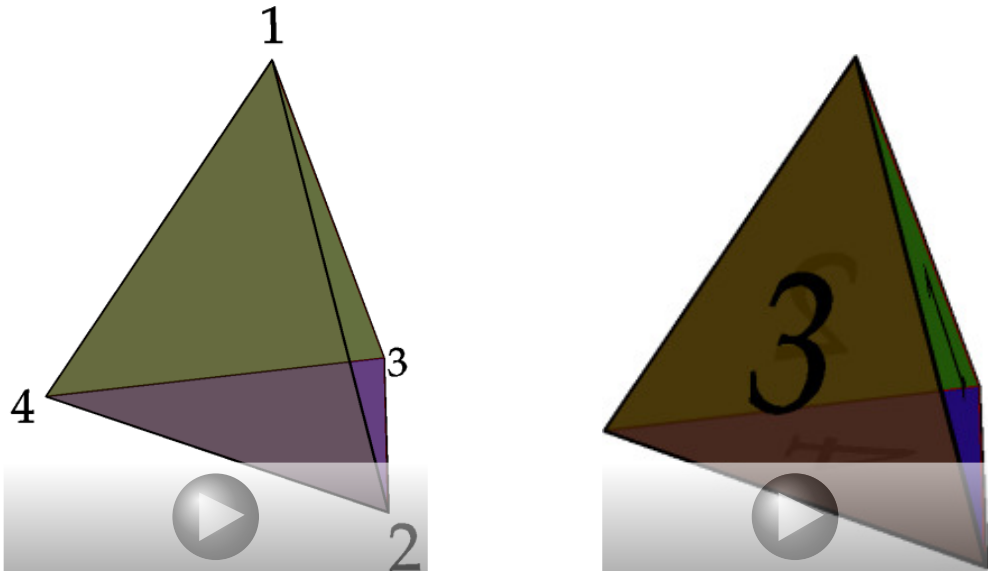
Since ϕ is a bijection, it follows that there are exactly the same number of even and odd permutations in S_n. Exactly half of them are therefore even. ∎

Examples: small alternating groups

1. $A_2 = \{e\}$ is extremely boring!
2. $A_3 = \{e, (13)(12), (12)(13)\} = \{e, (123), (132)\}$ is simply the cyclic group of order 3.
3. $A_4 = \{e, (123), (132), (124), (142), (134), (143), (234), (243), (12)(34), (13)(24), (14)(23)\}$ is the first genuinely new group in the alternating family. It has order 12 and is non-Abelian: for example

   $$(123)(124) = (13)(24) \neq (14)(23) = (124)(123)$$

   We already know of one non-Abelian group of order 12: the dihedral group D_6. But we can quickly see that A_4 is non-isomorphic to D_6: all elements of A_4 have order 1, 2 or 3, while D_6, being the symmetries of a hexagon, contains a rotation of order 6.
   A concrete appearance of A_4 can be seen as the group of rotations of a tetrahedron. Either label the corners of a tetrahedron, or the faces, with the numbers 1, 2, 3, 4. Can you visualize how each element of A_4 transforms each tetrahedron?



6 Cosets & Factor Groups

The course becomes markedly more abstract at this point. Our primary goal is to break apart a group into subsets such that the set of subsets inherits a natural group structure. This sounds strange, but it is *precisely* what you've already encountered when constructing a natural addition on the set of remainders modulo n: in $\mathbb{Z}_6$, when we write $3+5=2$, we really mean $[3]+[5]=[2]$, where

$$[3] = \{3+6n : n \in \mathbb{Z}\}$$

is the *set* of integers whose remainder is 3 when divided by 6. We shall call this set a *coset* to indicate that it is related to a *subgroup* of the integers, namely $3\mathbb{Z}$. That the above addition of sets makes sense and defines a group structure is merely an example of a more general construction.

6.1 Lagrange's Theorem

Before properly defining cosets, we state what you should already have hypothesized, given the huge number of examples you've now seen. Cosets will turn out to provide a simple proof. Review any of the subgroup relations we've already seen and observe that the order of a subgroup is a divisor of the order of its parent group. This is a general result.

Theorem 6.1 (Lagrange)**.** *Suppose that G is a finite group. The order of any subgroup $H \leq G$ divides the order of G. Otherwise said*

$$H \leq G \implies |H| \,\Big|\, |G|$$

We have already proved the special case for subgroups of cyclic groups:[24]

> If G is a cyclic group of order n, then, for every divisor d of n, G has exactly one subgroup of order d. More precisely, if $G = \langle g \rangle$ has order n, then
>
> - $\langle g^k \rangle \cong C_d \quad \text{where} \quad d = \frac{n}{\gcd(n,k)}$
> - $\langle g^k \rangle = \langle g^l \rangle \iff \gcd(n,k) = \gcd(n,l)$

We shall prove the full theorem shortly. For such a simple result, Lagrange's Theorem is extremely powerful. For instance, you may have observed that there is only one group structure, up to isomorphism, of prime orders 2, 3, 5 and 7. This is also a general result.

Corollary 6.2. *There is only one group (up to isomorphism) of each prime order p, namely C_p.*

Proof. Let p be prime and suppose that G is a group with $|G| = p$. Since $p \geq 2$, we may choose some element $x \in G \setminus \{e\}$. Consider the cyclic subgroup generated by x, namely $\langle x \rangle \leq G$.
Lagrange $\implies$ $|\langle x \rangle|$ divides p $\implies$ $\langle x \rangle = 1$ or p. Since $\langle x \rangle$ has at least two elements, its order must therefore be p, from which $G = \langle x \rangle$ is cyclic.
Finally, recall that there is only one cyclic group of each order up to isomorphism, so $G = C_p$. ∎

[24] Lagrange's Theorem is sometimes misremembered as 'the order of an element divides the order of a group.' This is really only a statement about the *cyclic subgroups* of a group G and is not as general as Lagrange-proper.

6.2 Cosets and Normal Subgroups

The idea for the proof of Lagrange's Theorem is very simple. Given a subgroup $H \leq G$, partition G into several subsets, each with the same cardinality as H. We call these subsets the *cosets* of H.

Definition 6.3. Let $H \leq G$ and choose $g \in G$. The subsets of G defined by

$$gH := \{gh : h \in H\} \qquad \text{and} \qquad Hg := \{hg : h \in H\}$$

are (respectively) the *left* and *right cosets* of H containing g.
If the left- and right- cosets of H containing g are always equal ($\forall g \in G,\ gH = Hg$) we say that H is a *normal subgroup* of G, and write $H \triangleleft G$.
If G is written additively, the left and right cosets of H containing g are

$$g + H := \{g + h : h \in H\} \qquad \text{and} \qquad H + g := \{h + g : h \in H\}$$

Even though our ultimate purpose is to prove Lagrange's Theorem (a statement about *finite* groups), the concept of cosets is perfectly well-defined for any group. Before seeing some examples, we state a straightforward lemma giving some conditions for identifying normal subgroups.

Lemma 6.4. *1. Every subgroup of an abelian group G is normal.*

2. A subgroup H is normal in G if and only if $\forall g \in G,\ \forall h \in H,\ ghg^{-1} \in H$.

For non-abelian groups, most subgroups are typically *not* normal (although see example 3 below).

Proof. Part 1. should be obvious. For part 2., note first that

$$H \triangleleft G \implies \forall g \in G,\ h \in H, gh \in Hg \implies \forall g \in G,\ h \in H,\ ghg^{-1} \in H$$

Conversely, $ghg^{-1} \in H \implies gh \in Hg \implies gH \subseteq Hg$. If this holds for *all* $g \in G$ and $h \in H$, then it certainly applies for g^{-1}, whence

$$g^{-1}hg \in H \implies hg \in gH \implies Hg \subseteq gH$$

We conclude that $gH = Hg$ for all $g \in G$ and so H is normal in G. ∎

Examples

1. Consider the subgroup of $\mathbb{Z}_{12}$ generated by 4. This subgroup is cyclic of order 3:

   $$H = \langle 4 \rangle = \{0, 4, 8\} \cong C_3$$

   Since the group operation is addition, we write cosets additively: for example, the left coset of $\langle 4 \rangle$ containing $x \in \mathbb{Z}_{12}$ is the subset

   $$x + \langle 4 \rangle = \{x + n : n \in \langle 4 \rangle\} = \{x, x + 4, x + 8\}$$

where we might have to reduce $x+4$ and $x+8$ modulo 12. The distinct left cosets of $\langle 4\rangle$ are as follows:

$$\begin{aligned}
0+\langle 4\rangle &= \{0,4,8\} &&= 4+\langle 4\rangle = 8+\langle 4\rangle && \text{(usually written } \langle 4\rangle\text{, dropping the zero)}\\
1+\langle 4\rangle &= \{1,5,9\} &&= 5+\langle 4\rangle = 9+\langle 4\rangle &&\\
2+\langle 4\rangle &= \{2,6,10\} &&= 6+\langle 4\rangle = 10+\langle 4\rangle &&\\
3+\langle 4\rangle &= \{3,7,11\} &&= 7+\langle 4\rangle = 11+\langle 4\rangle &&
\end{aligned}$$

There are only four distinct cosets: notice that each has the *same* number of elements (three) as the subgroup $\langle 4\rangle$, and that $\frac{|\mathbb{Z}_{12}|}{|\langle 4\rangle|} = \frac{12}{3} = 4$. The cosets have *partitioned* $\mathbb{Z}_{12}$ into equal-sized subsets. This is crucial for the proof of Lagrange's Theorem.
Observe also that the right cosets of $\langle 4\rangle$ are the same as the left cosets, in accordance with Lemma 6.4).
Observe finally that *only one* of the cosets is a *subgroup*, the others are merely *subsets* of $\mathbb{Z}_{12}$.

2. Recall the multiplication table for D_3. With a little work, you should be able to compute that the left and right cosets of the subgroup $H = \{e, \mu_1\}$ are as follows:

Left cosets	Right cosets
$eH = \mu_1 H = H = \{e, \mu_1\}$	$He = H\mu_1 = H = \{e, \mu_1\}$
$\rho_1 H = \mu_3 H = \{\rho_1, \mu_3\}$	$H\rho_1 = H\mu_2 = \{\rho_1, \mu_2\}$
$\rho_2 H = \mu_2 H = \{\rho_2, \mu_2\}$	$H\rho_2 = H\mu_3 = \{\rho_1, \mu_3\}$

This time the left and right cosets of H are different (H is *not* a normal subgroup of D_3), but all cosets still have the same cardinality.

3. Recall how we proved that the alternating subgroup $A_n \leq S_n$ has cardinality $|A_n| = \frac{1}{2}|S_n|$. Generalizing this approach, it should be clear that, for any $\alpha \in A_n$ and $\sigma \in S_n$, we have

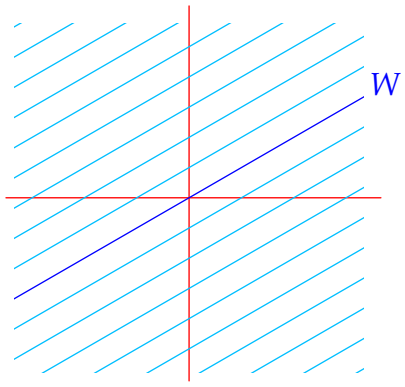
$$\alpha\sigma \text{ even} \iff \sigma \text{ even} \iff \sigma\alpha \text{ even}$$

Otherwise said, for any $\sigma \in S_n$, the cosets of A_n contiaining σ are

$$\sigma A_n = A_n \sigma = \begin{cases} A_n & \text{if } \sigma \text{ even} \\ B_n & \text{if } \sigma \text{ odd} \end{cases}$$

where B_n is the set of odd permutations in S_n. Note that A_n is a normal subgroup of S_n.

4. The vector space $\mathbb{R}^2$ is an Abelian group under addition. The real line $\mathbb{R}$ identified with the x-axis, is a subgroup. The cosets of $\mathbb{R}$ in $\mathbb{R}^2$ are all the sets $\mathbf{v} + \mathbb{R}$ which are horizontal lines.
More generally, if W is a subspace of a vector space V, then the cosets $\mathbf{v} + W$ form sets parallel to W: only the zero coset $W = \mathbf{0} + W$ is a sub*space*.
In the picture, W is line through the origin in $\mathbb{R}^2$; its cosets comprise all the lines in $\mathbb{R}^2$ parallel to W (including W itself!).



The examples should have suggested the following Theorem.

Theorem 6.5. *The left cosets of H partition G.*

Before reading the proof, look at each of the above examples and convince yourself that the result is satisfied in each case. The strategy is to define an equivalence relation, the equivalence classes of which are precisely the left cosets of H.

Proof. Define a relation $\sim$ on G by $x \sim y \iff x^{-1}y \in H$. We claim that $\sim$ is an equivalence relation.

Reflexivity $x \sim x$ since $x^{-1}x = e \in H$. ✓

Symmetry $x \sim y \implies x^{-1}y \in H \implies (x^{-1}y)^{-1} \in H$, since H is a subgroup. But then

$$y^{-1}x \in H \implies y \sim x. \quad \checkmark$$

Transitivity If $x \sim y$ and $y \sim z$ then $x^{-1}y \in H$ and $y^{-1}z \in H$. But H is closed, whence

$$x^{-1}z = (x^{-1}y)(y^{-1}z) \in H \implies x \sim z. \quad \checkmark$$

The equivalence classes of $\sim$ therefore partition G. We claim that these are precisely the left cosets of H. Specifically, we claim that

$$x \sim y \iff x \text{ and } y \text{ lie in the same left coset of } H \iff xH = yH$$

However, note that $x \sim y \iff x^{-1}y \in H \iff y \in xH$. It follows that $yH \subseteq xH$.
By symmetry, $x \sim y \iff y^{-1}x \in H \iff xH \subseteq yH$. We conclude that

$$x \sim y \iff xH = yH$$

as required. ∎

Aside: Partitions and Subgroups Each of the three conditions that $\sim$ be an equivalence relation corresponds to one of the properties characterizing H as a *subgroup* of G:

Reflexivity H contains the identity.

Symmetry H is closed under inverses.

Transitivity H is closed under the group operation.

It is precisely the fact that H is a subgroup which guarantees a partition. For example, if H is merely the *subset* $H = \{0, 1\}$ of $|Z_3 = \{0, 1, 2\}$, then its left 'cosets' are

$$0 + \{0,1\} = \{0,1\}, \quad 1 + \{0,1\} = \{1,2\}, \quad 2 + \{0,1\} = \{2,1\},$$

which do not partition $\mathbb{Z}_3$.

Proof of Lagrange's Theorem. Suppose that $H \leq G$ and $g \in G$ is a fixed element. Then the function

$$\phi : H \to gH : h \mapsto gh$$

is a bijection (its inverse is $\phi^{-1} : gh \mapsto g$). It follows that every left coset of H has the same cardinality as H. Therefore

$$|G| = (\text{number of left cosets of } H) \cdot |H|$$

whence $|H|$ divides $|G|$.

■

You should now revisit the proof that $|A_n| = \frac{1}{2}|S_n|$: it is nothing but a special case of Theorem 6.5 and the proof of Lagrange.

The right cosets of a subgroup H also partition G although, in general, they do this in a *different* way to the left cosets: observe the earlier example of the cosets of the subgroup $\{e, \mu_1\} \leq D_3$. The proof of Lagrange's Theorem could also be argued with right cosets.

6.3 Indices

The proof of Lagrange's Theorem in fact tells us that the number of left and right cosets of H in G is *identical:* both are equal to the quotient $\frac{|G|}{|H|}$. This leads us to the following definition.

Definition 6.6. If $H \leq G$ then the *index* of H in G, written $(G : H)$, is the number of left (or right) cosets of H in G. Strictly, the index is the cardinality of the set of left cosets:

$$(G : H) = |\{gH : g \in G\}|$$

If G is finite $(G : H) = \frac{|G|}{|H|}$ and the index is simple to calculate. It is more difficult to consider the situation when G is *infinite,* although the concept is well-defined (the cardinalities of the sets of left and right cosets are identical).

Theorem 6.7. *If $K \leq H \leq G$ is a sequence of subgroups then*

$$(G : K) = (G : H)(H : K)$$

If G is a *finite* group then the result is essentially trivial:

$$(G : K) = \frac{|G|}{|K|} = \frac{|G|}{|H|} \cdot \frac{|H|}{|K|} = (G : H)(H : K)$$

However, the Theorem is more general, for it applies also to *infinite* groups.[25]

[25]Even when dealing with infinite groups, we will only think about examples where *indices* are finite so that their multiplication makes sense. If you are comfortable multiplying infinite cardinals then there is no problem removing this restriction and our proof works even in the general case.

Proof. Given $K \leq H \leq G$ choose a single element g_i from each left coset of H in G and a single element k_j from each left coset of K in H. Clearly

$$(G : H) = |\{g_i\}| \qquad \text{and} \qquad (H : K) = \big|\{h_j\}\big|$$

We claim that the left cosets of K in G are precisely the sets $(g_i h_j)K$. Certainly each set $(g_i h_j)K$ is a coset of K in G: our goal is to show that these sets *partition* G, whence the collection $\{(g_i h_j)K\}$ comprises *all* the left cosets of K in G. The partition conditions are confirmed below:

- Every $g \in G$ lies in some left coset of H, so $\exists g_i \in G$ such that $g \in g_i H$. But then $g_i^{-1} g \in H$.
  Every $h \in H$ lies in some left coset of K in H, so $\exists h_j \in H$ such that $g_i^{-1} g \in h_j K$.
  But then $g \in (g_i h_j)K$ so that every $g \in G$ lies in at least one set $(g_i h_j)K$.
- Suppose $y \in g_i h_j K \cap g_\alpha h_\beta K$. Since the left cosets of H partition G, we have

  $$y \in g_i H \cap g_\alpha H \implies g_\alpha = g_i$$

  But then $g_i^{-1} y \in h_j K \cap h_\beta K \implies h_\beta = h_j$ similarly, since the left cosets of K in H partition H. It follows that the sets $(g_i h_j)K$ are disjoint.

Since the left cosets of K in G are given by $\{(g_i h_j)K\}$, it is immediate that[26]

$$(G : K) = \big|\{g_i h_j\}\big| = \big|\{g_i\} \times \{h_j\}\big| = (G : H)(H : K)$$

■

Examples

1. Consider $G = \mathbb{Z}_{20}$ with its subgroups $H = \langle 2 \rangle$ and $K = \{10\}$. Certainly

   $$K = \{0, 10\} \leq H = \{0, 2, 4, \ldots, 18\} \leq G = \{0, 1, 2, 3, \ldots\}$$

   There are two (left)[27] cosets of H in G, namely

   $$H = \{0, 2, 4, \ldots, 18\} \quad \text{and} \quad 1 + H = \{1, 3, 5, \ldots, 19\}$$

   whence the index is $(G : H) = 2$. Indeed, in the language of the proof, we could choose representatives $g_1 = 0$ and $g_2 = 1$.
   Meanwhile, K has five cosets in H:

   $$K = \{0, 10\}, \quad 2 + K = \{2, 12\}, \quad 4 + K = \{4, 14\}, \quad 6 + K = \{6, 16\}, \quad 8 + K = \{8, 18\}$$

   so that $(H : K) = 5$. We could choose representatives $h_1 = 0$, $h_2 = 2$, $h_3 = 4$, $h_4 = 6$, $h_5 = 8$.
   There are ten cosets of K in G, in accordance with $(G : K) = (G : H)(H : K)$:

   $$K = \{0, 10\}, \quad 1 + K = \{1, 11\}, \quad 2 + K = \{2, 12\}, \quad \ldots, \quad 9 + K = \{9, 19\}$$

   In the language of the Theorem, these can be written

   $$K = (g_1 + h_1) + K, \quad 1 + K = (g_2 + h_1) + K, \quad 2 + K = (g_1 + h_2) + K, \quad \ldots$$
   $$\ldots, \quad 8 + K = (g_1 + h_4) + K, \quad 9 + K = (g_2 + h_4) + K$$

[26] The fact that $\big|\{g_i h_j\}\big| = \big|\{g_i\} \times \{h_j\}\big|$ follows from the second bullet-point.

[27] The example is Abelian so left and right cosets are identical.

2. We consider the cosets for the sequence of subgroups

$$C_3 \leq S_3 \leq S_4$$

where $C_3 = \{e, (123), (132)\}$ and $S_3 = \{\sigma \in S_4 : \sigma(4) = 4\}$. The left cosets for C_3 in S_3 are

$$eC_3 = C_3 = \{e, (123), (132)\} \quad \text{and} \quad (12)C_3 = \{(12), (23), (13)\}$$

reflecting the fact that $(S_3 : C_3) = 2$. In the language of the Theorem, $g_0 = e$ and $g_1 = (12)$. Similarly, the left cosets for S_3 in S_4 are

$$\begin{aligned}
eS_3 &= S_3 = \{e, (123), (132), (12), (23), (13)\} \\
(14)S_3 &= S_3 = \{(14), (1234), (1324), (124), (14)(23), (134)\} \\
(24)S_3 &= S_3 = \{(24), (1423), (1342), (142), (234), (13)(24)\} \\
(34)S_3 &= S_3 = \{(34), (1243), (1432), (12)(34), (243), (143)\}
\end{aligned}$$

with $(S_4 : S_3) = 4$ and $h_0 = e, h_1 = (14), h_2 = (24), h_3 = (34)$. Finally, the left cosets of C_3 in S_4 are

$$\begin{aligned}
eC_3 &= C_3 = \{e, (123), (132)\} & (12)eC_3 &= (12)C_3 = \{(12), (23), (13)\} \\
(14)C_3 &= \{(14), (1234), (1324)\} & (12)(14)C_3 &= (124)C_3 = \{(124), (14)(23), (134)\} \\
(24)C_3 &= \{(24), (1423), (1342)\} & (12)(24)C_3 &= (142)C_3 = \{(142), (234), (13)(24)\} \\
(34)C_3 &= \{(34), (1243), (1432)\} & (12)(34)C_3 &= \{(12)(34), (243), (143)\}
\end{aligned}$$

in accordance with $(S_4 : C_3) = 8 = (S_4 : S_3) = (S_3 : C_3)$. There are patterns everywhere!

Aside: Indices in Infinite Groups It is more challenging to think about indices for infinite groups. Here are two classic examples:

1. $\mathrm{O}_2(\mathbb{R})$ is the set of rotations and reflections of the plane (or of the unit circle if you prefer). Its subgroup $\mathrm{SO}_2(\mathbb{R})$ is the set of rotations. Both groups are infinite (indeed uncountable), but we can compute the index:

   $$(\mathrm{O}_n(\mathbb{R}) : \mathrm{SO}_n(\mathbb{R})) = 2$$

   Intuitively this says that the rotations comprise half of group $\mathrm{O}_2(\mathbb{R})$. To prove this, one performs what should be a now-familiar trick: the function

   $$\phi : \mathrm{SO}_2(\mathbb{R}) \to \mathrm{O}_2(\mathbb{R}) \setminus \mathrm{SO}_2(\mathbb{R}) : A \mapsto \begin{pmatrix} 1 & 0 \\ 0 & -1 \end{pmatrix} A$$

   is a bijection...

2. The sets $\mathbb{Q}$ and $\mathbb{Z}$ are both groups under addition. Their index is countably infinite!

   $$(\mathbb{Q} : \mathbb{Z}) = \aleph_0$$

   To see this, note that

   $$p + \mathbb{Z} = q + \mathbb{Z} \iff p - q \in \mathbb{Z}$$

   so that there is precisely one coset of $\mathbb{Z}$ in $\mathbb{Q}$ for every rational number in the interval $[0, 1)$, a denumerable set.

6.4 Factor Groups

The idea of factor groups is very simple, if abstract. Given a subgroup $H \leq G$ we may consider the *set of left cosets*

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

The question for this section is whether the set of left cosets has any *interesting structure*: that is, *can we view* G/H *as a group in a natural way?*[28] To see how this might work, let us recall the first two examples of cosets starting on page 49.

Turning the set of left cosets into a group Consider $H \leq \mathbb{Z}_{12}$ where $H = \langle 4 \rangle = \{0, 4, 8\}$, with (left) cosets

$$H, \quad 1 + H, \quad 2 + H, \quad 3 + H$$

The set of left cosets is then

$$\mathbb{Z}_{12}/H = \{H,\ 1 + H,\ 2 + H,\ 3 + H\} = \Big\{\{0,4,8\}, \{1,5,9\}, \{2,6,10\}, \{3,7,11\}\Big\}$$

There is a nice pattern here: x and y are members of the same coset if and only if $x \equiv y \pmod 4$. Moreover, there are four cosets. Can we view $\mathbb{Z}_{12}/H$ as merely the cyclic group $\mathbb{Z}_4$ in disguise? The answer, of course, is yes.

To do this, we need to define a binary operation on $\mathbb{Z}_{12}/H$: we need to see how to combine cosets to create new ones. The obvious thing to do is to use the addition in $\mathbb{Z}_{12}$ that we already have: thus define

$$(a + H) \oplus (b + H) := (a + b) + H$$

The binary operation $\oplus$ on the set $\mathbb{Z}_{12}/H$ comes naturally from the existing addition on $\mathbb{Z}_{12}$: we haven't created anything new, just using what we've been given.

There is a potential problem however: the *freedom of choice* built into the definition. Computing $(a + H) \oplus (b + H)$ requires three steps:

Choose representatives Make a choice of elements a and b in the respective cosets.

Add in the original group Compute $a + b \in \mathbb{Z}_{12}$.

Take the coset Return the left coset $(a + b) + H$.

[28] There are typically *many* operations one could define on a set which would define a group structure. We want the structure to be *natural*: this means that it should appear without choice or imposition, and be inherited from the pre-existing structure on G. In this way the structure will encode some information about G itself.

If $\oplus$ is to make any sense at all, then the result $(a+b)+H$ must be *independent of the choices* we made in the first step.[29] In this case there is no problem, as you can tediously check for yourself. For example, to compute

$$(1+H)\oplus(2+H)$$

there are *nine* possibilities:

$$\begin{aligned}
1+2=3 &\implies (1+H)\oplus(2+H)=3+H\\
1+6=7 &\implies (1+H)\oplus(2+H)=7+H=3+H\\
1+10=11 &\implies (1+H)\oplus(2+H)=11+H=3+H\\
5+2=7 &\implies (1+H)\oplus(2+H)=7+H=3+H\\
5+6=11 &\implies (1+H)\oplus(2+H)=11+H=3+H\\
5+10=15 &\implies (1+H)\oplus(2+H)=15+H=3+H\\
9+2=11 &\implies (1+H)\oplus(2+H)=11+H=3+H\\
9+6=15 &\implies (1+H)\oplus(2+H)=15+H=3+H\\
9+10=19 &\implies (1+H)\oplus(2+H)=19+H=3+H
\end{aligned}$$

Thankfully all nine results are the same! The other possibilities for adding cosets can be similarly checked (we'll do this in general in a moment). It is not hard to produce a table for the binary operation $\oplus$ on the set $\mathbb{Z}_{12}\big/_{H}$:

$\oplus$	H	$1+H$	$2+H$	$3+H$
H	H	$1+H$	$2+H$	$3+H$
$1+H$	$1+H$	$2+H$	$3+H$	H
$2+H$	$2+H$	$3+H$	H	$1+H$
$3+H$	$3+H$	H	$1+H$	$2+H$

This table should look very familiar: if you delete all the H expressions (so that $H = 0+H$ becomes 0), we recover precisely the Cayley table for the cyclic group $\mathbb{Z}_4$. Indeed we have proved the following:

Proposition 6.8. *The set of left cosets* $\mathbb{Z}_{12}\big/_{H} = \{H,\ 1+H,\ 2+H,\ 3+H\}$ *forms a group under the operation* $\oplus$*, which is moreover isomorphic to* $\mathbb{Z}_4$*. We will shortly refer to this as a* factor group.

It would be very nice if this sort of behavior were universal. Unfortunately it isn't.

When cosets fail to form a group Let us repeat the process with the subgroup $H=\{e,\mu_1\}\leq D_3$. Recall that its left cosets are

$$eH=\mu_1H=H=\{e,\mu_1\},\qquad \rho_1H=\mu_3H=\{\rho_1,\mu_3\},\qquad \rho_2H=\mu_2H=\{\rho_2,\mu_2\}$$

In the same way as above, we define the 'natural' operation on the set $D_3\big/_{H}$ of left cosets:[30]

$$aH\otimes bH := (ab)H$$

[29] Strictly speaking we require that $\oplus : \mathbb{Z}_{12}\big/_{H}\times\mathbb{Z}_{12}\big/_{H}\to\mathbb{Z}_{12}\big/_{H}$ be a *well-defined function.*

[30] Again, the 'operation' on the set of left cosets comes directly from the group operation on D_3.

This time there is a problem. Suppose we want to compute $\rho_1 H \otimes \rho_1 H$. There are *four choices*:[31]

$$\rho_1 H \otimes \rho_1 H = \rho_1^2 H = \rho_2 H$$
$$\rho_1 H \otimes \mu_3 H = \rho_1 \mu_3 H = \mu_2 H = \rho_2 H$$
$$\mu_3 H \otimes \rho_1 H = \mu_3 \rho_1 H = \mu_1 H = H$$
$$\mu_3 H \otimes \mu_3 H = \mu_3^2 H = eH = H$$

Exercising the freedom of choice in the definition of $\otimes$ leads to different outcomes: it follows that $\otimes$ is *not well-defined.* There is nothing stopping us from defining a group structure on D_3/H, but any such definition must involve a *choice* on our part: we would be *imposing* structure rather that observing structure that occured naturally.

Well-definition of the natural group structure The above discussion can be generalized. Clearly some subgroups $H \leq G$ behave better than others when considering the set G/H of left cosets. How can we tell which subgroups?

Let H be a subgroup of G and define the natural operation on G/H:

$$aH \cdot bH := (ab)H$$

This is well-defined if and only if

$$\forall a, b \in G,\ \forall x \in aH,\ y \in bH, \quad \text{we have} \quad aH \cdot bH = xH \cdot yH$$

Let us trace through what this means for the subgroup H.

$$x \in aH \iff \exists h \in H \quad \text{such that} \quad x = ah$$

The operation on G/H is therefore well-defined if and only if

$$\begin{aligned}
&\forall a, b \in G, \quad \forall h_1, h_2 \in H, \quad (ah_1bh_2)H = (ab)H \\
\iff &\forall a, b \in G, \quad \forall h \in H, \quad (ahb)H = (ab)H && \text{(since } h_2H = H \text{ for all } h_2 \in H\text{)} \\
\iff &\forall a, b \in G, \quad \forall h \in H, \quad (ab)^{-1}(ahb) \in H \\
\iff &\forall b \in G, \quad \forall h \in H, \quad b^{-1}hb \in H \\
\iff &H \triangleleft G && \text{(recall Lemma 6.4)}
\end{aligned}$$

We've therefore proved the critical part of the following:

Theorem 6.9. *Suppose that H is a subgroup of G. The set of (left) cosets G/H forms a group under the natural operation*

$$aH \cdot bH := (ab)H$$

if and only if H is a normal subgroup of G.

[31] Write these as cycles if you're having trouble computing: e.g. $\rho_1 = (123)$, $\mu_1 = (23)$, etc.

Proof. The above discussion proves the $\Rightarrow$ direction: if G/H forms a group then the operation is certainly well-defined, whence H is normal.
For the converse, we check the group axioms.

Closure By the above discussion, $H \triangleleft G \implies$ the natural operation is well-defined. Certainly $aH \cdot bH = (ab)H$ is a coset, whence $\left(G/H, \cdot\right)$ is closed. ✓

Associativity $aH \cdot (bH \cdot cH) = aH \cdot (bc)H = a(bc)H$. Similarly $(aH \cdot bH) \cdot cH = (ab)cH$. By the associativity of G these are identical. ✓

Identity $eH \cdot aH = (ea)H = aH$ therefore $eH = H$ is the identity. ✓

Inverse $a^{-1}H \cdot aH = (a^{-1}a)H = eH = H$, therefore $(aH)^{-1} = a^{-1}H$. ✓

■

Definition 6.10. If H is a normal subgroup of G, then G/H is called a *factor group.*

Warning! Because the group structure on a factor group G/H comes naturally from the group structure on G, we typically use the *same notation* for the operation. Thus if $(G, +)$ is a group, we also use $+$ for the operation on G/H. Similarly $(G, \cdot)$ will have factor groups $\left(G/H, \cdot\right)$ written multiplicatively. Make sure you know to *which group* an operation refers! The symbols $\oplus, \otimes$ in the above examples were used only to help you keep the operations separate.

6.5 Factor Groups: Examples and Calculations

There are many nice examples of factor groups. The main question we are concerned with is how to *identify* a given factor group G/H: by this we mean that we want to find a well-understood group K which is isomorphic to G/H. We start with a general example which is important enough to merits a full discussion. This should, however, be a revision of material from a previous class.

Factor Groups of Infinite Cyclic Groups: The Group $\mathbb{Z}_m$

For each integer m, its integer multiples $m\mathbb{Z} = \langle m \rangle$ form a subgroup of $\mathbb{Z}$. Since $\mathbb{Z}$ is abelian, $m\mathbb{Z}$ is a normal subgroup. Observe that

$$x + m\mathbb{Z} = y + m\mathbb{Z} \iff x - y \in m\mathbb{Z} \iff x \equiv y \mod m$$

whence there is precisely one coset for each remainder modulo m. We may therefore write the cosets of $m\mathbb{Z}$ as

$$\mathbb{Z}/m\mathbb{Z} = \{0 + m\mathbb{Z},\ 1 + m\mathbb{Z},\ \ldots,\ (m-1) + m\mathbb{Z}\}$$

Addition in the factor group is natural:

$$\Big(x + m\mathbb{Z}\Big) + \Big(y + m\mathbb{Z}\Big) = (x + y) + m\mathbb{Z}$$

This looks suspiciously like addition modulo m! Indeed we have the following:

Theorem 6.11. $\mu : \mathbb{Z}/m\mathbb{Z} \to \mathbb{Z}_m : x + m\mathbb{Z} \mapsto x \pmod{m}$ *is an isomorphism.*

Proof. We've already seen most of the relevant calculations!

Well-definition and Injectivity Note that

$$\begin{aligned} x + m\mathbb{Z} = y + m\mathbb{Z} &\iff x - y \in m\mathbb{Z} \iff x - y \equiv 0 \pmod{m} \\ &\iff x = y \quad (\text{in } \mathbb{Z}_m) \\ &\iff \mu(x + m\mathbb{Z}) = \mu(y + m\mathbb{Z}) \end{aligned}$$

Surjectivity Given any $x \in \mathbb{Z}_m$, we have $x = \mu(x + m\mathbb{Z})$.

Homomorphism For all $x + m\mathbb{Z},\ y + m\mathbb{Z} \in \mathbb{Z}/m\mathbb{Z}$, we have

$$\begin{aligned} \mu\Big((x + m\mathbb{Z}) + (y + m\mathbb{Z})\Big) &= \mu\Big((x + y) + m\mathbb{Z}\Big) = x + y \pmod{m} \\ &= \mu\big(x + m\mathbb{Z}\big) + \mu\big(y + m\mathbb{Z}\big) \pmod{m} \end{aligned}$$

■

By this argument, algebraists often take the factor group $\mathbb{Z}/m\mathbb{Z}$ to be the *definition* of the group $\mathbb{Z}_m$.

Factor Groups of Finite Cyclic Groups

We've already seen the example $\mathbb{Z}_{12}/\langle 4\rangle \cong \mathbb{Z}_4$ (Proposition 6.8). We can, in fact, identify all factor groups of finite cyclic groups.

Recall that $\mathbb{Z}_n$ has a single subgroup of order $\frac{n}{d}$ for each divisor d of n, namely[32]

$$\langle d\rangle = \Big\{0, d, 2d, \ldots, \Big(\frac{n}{d} - 1\Big)\, d\Big\}$$

Theorem 6.12. *If $d \mid n$, then $\mu : \mathbb{Z}_n/\langle d\rangle \to \mathbb{Z}_d : x + \langle d\rangle \mapsto x \pmod{d}$ is an isomorphism.*

Try proving this yourself: it should be very similar to the proof of Theorem 6.11.

Example $\langle 5\rangle = \{0, 5, 10, 15\} \leq \mathbb{Z}_{20}$ has factor group

$$\mathbb{Z}_{20}/\langle 5\rangle = \{0 + \langle 5\rangle\,,\ 1 + \langle 5\rangle\,,\ 2 + \langle 5\rangle\,,\ 3 + \langle 5\rangle\,,\ 4 + \langle 5\rangle\}$$

This is isomorphic to $\mathbb{Z}_5$ under the isomorphism

$$\mu : \mathbb{Z}_{20}/\langle 5\rangle \to \mathbb{Z}_5 : x + \langle 5\rangle \mapsto x \pmod{5}$$

[32] Recall that $\langle s\rangle = \langle d\rangle \iff \gcd(s, n) = \gcd(d, n) = d$.

Factor Groups of Finite Abelian Groups

If G is a finite abelian group with subgroup H, then G/H is also a finite abelian group. According to the Fundamental Theorem of Finitely Generated Abelian Groups, the means that

$$G/H \cong \mathbb{Z}_{m_1} \times \mathbb{Z}_{m_k}$$

for some $m_1, \ldots, m_k \in \mathbb{N}$ which satisfy $m_1 \cdots m_k = (G : H) = \frac{|G|}{|H|}$. Our goal in the following examples is to *identify* G/H by finding the relevant m_k.

Examples

1. Identify the factor group $G/H = (\mathbb{Z}_4 \times \mathbb{Z}_8)/\langle (0,1) \rangle$ in terms of the Fundamental Theorem of Finitely Generated Abelian Groups.

   First consider the elements of the cyclic subgroup:

   $$H = \langle (0,1) \rangle = \{(0,0), (0,1), (0,2), (0,3), (0,4), (0,5), (0,6), (0,7)\}$$

   This has order 8 whence the number of cosets is index of H in G, namely $(G : H) = \frac{4 \cdot 8}{8}$. We can easily compute the cosets: recall that

   $$(x,y) + H = (v,w) + H \iff (x,y) - (v,w) = (x - v, y - w) \in H \iff x = v$$

   It follows that there is a unique element in each coset of the form $(x,0)$, where $x \in \mathbb{Z}_4$. Indeed the factor group may be written

   $$G/H = \Big\{ H,\ (1,0) + H,\ (2,0) + H,\ (3,0) + H \Big\}$$

   The factor group is abelian of order 4. We therefore have two possibilities: $G/H \cong \mathbb{Z}_4$ or $G/H \cong \mathbb{Z}_2 \times \mathbb{Z}_2$. Which is it?

   A straightforward answer comes by observing that the factor group is generated by the coset $(1,0) + H$, indeed

   $$\langle (1,0) + H \rangle = \{ H,\ (1,0) + H,\ (2,0) + H,\ (3,0) + H \} = G/H$$

   The factor group is cyclic and is therefore isomorphic to $\mathbb{Z}_4$.

   If you want to be more explicit, observe that the function

   $$\psi : \mathbb{Z}_4 \to G/H : x \mapsto (x,0) + H$$

   is an isomorphism.

2. We can do something similar for $G/H = (\mathbb{Z}_4 \times \mathbb{Z}_8)/\langle(0,2)\rangle$. This time the cyclic subgroup $H = \{0,0),(0,2),(0,4),(0,6)\}$ has order 4. As with the previous example, the elements of of the cyclic subgroup only influce the second factor $\mathbb{Z}_8$ of G, and we therefore expect to see

$$(\mathbb{Z}_4 \times \mathbb{Z}_8)/\langle(0,2)\rangle \cong \mathbb{Z}_4 \times \mathbb{Z}_8/\langle 2\rangle \cong \mathbb{Z}_4 \times \mathbb{Z}_2$$

Indeed this is what we find, for the function

$$\psi : \mathbb{Z}_4 \times \mathbb{Z}_2 \to G/H : (x,y) \mapsto (x,y) + H$$

is an isomorphism.

If the above seems too, fast, try counting cosets. Clearly $\left|G/H\right| = \frac{4\cdot 8}{4} = 8$, whence the quotient group is abelian of order 8. There are three non-isomorphic possibilities:

$$G/H \cong \mathbb{Z}_8, \quad \mathbb{Z}_4 \times \mathbb{Z}_2, \quad \mathbb{Z}_2 \times \mathbb{Z}_2 \times \mathbb{Z}_2$$

To distinguish these, consider the possible orders of elements in each group:

Group	Possible orders of elements
$\mathbb{Z}_8$	$1,2,4,8$
$\mathbb{Z}_4 \times \mathbb{Z}_2$	$1,2,4$
$\mathbb{Z}_2 \times \mathbb{Z}_2 \times \mathbb{Z}_2$	$1,2$

Observe:

- $(1,0) + H$ has order 4, since $\langle(1,0) + H\rangle = \{H, (1,0) + H, (2,0) + H, (3,0) + H\}$
- *All* elements of the factor group have order dividing 4:

$$4\big((x,y) + H\big) = (4x,4y) + H = (0,4y) + H = 2y\big((0,2) + H\big) = H$$

It follows that the factor group must be isomorphic to $\mathbb{Z}_4 \times \mathbb{Z}_2$.

3. This time we identify[33] $G/H = (\mathbb{Z}_4 \times \mathbb{Z}_8)/\langle(2,4)\rangle$. As ever, first compute the subgroup:

$$H = \{(0,0),(2,4)\}$$

has order 2. The factor group is therefore abelian of order $\frac{4\cdot 8}{2} = 16$. The Fundamental Theorem gives *five* distinct options for the factor group, namely

$$\mathbb{Z}_{16}, \quad \mathbb{Z}_2 \times \mathbb{Z}_8, \quad \mathbb{Z}_4 \times \mathbb{Z}_4, \quad \mathbb{Z}_2 \times \mathbb{Z}_2 \times \mathbb{Z}_4, \quad \mathbb{Z}_2 \times \mathbb{Z}_2 \times \mathbb{Z}_2 \times \mathbb{Z}_2$$

A little scratch work allows us to identify which is correct:

[33] The previous examples may have lulled you into a false sense of security: the answer to this question is *not*

$$\mathbb{Z}_4/\langle 2\rangle \times \mathbb{Z}_8/\langle 4\rangle \cong \mathbb{Z}_2 \times \mathbb{Z}_2$$

Indeed by counting the *sixteen* cosets, we see immediately see that this is impossible!

- If $x = 2n$ is even, then $(x, y) + H = (2n, y) + H = (0, y - 4n) + H$.
- If $x = 2n + 1$ is odd, then $(x, y) + H = 1, y - 4n) + H$.
- It follows that there is precisely one representative of each coset whose first entry is either 0 or 1, whence the following sixteen elements lie in distinct cosets of $\langle(2, 4)\rangle$:

$$(0,0),\ (0,1),\ \ldots,\ (0,7),\ (1,0),\ \ldots,\ (1,7)$$

- It now seems reasonable to conjecture that the factor group is isomorphic to $\mathbb{Z}_2 \times \mathbb{Z}_8$.

Here are two possible ways to prove this:

(a) Observe that the coset $(0, 1) + H$ has order 8 in the factor group. This narrows our choice to $\mathbb{Z}_{16}$ or $\mathbb{Z}_2 \times \mathbb{Z}_8$. Now check that *all* cosets have order at most 8:

$$8\Big((x, y) + H\Big) = (8i, 8j) + H = (0, 0) + H$$

There are no elements of order 16 whence we can rule out $\mathbb{Z}_{16}$ as a candidate. The only possibility remaining is $\mathbb{Z}_2 \times \mathbb{Z}_8$.

(b) We can define an explicit isomorphism:

$$\psi : \mathbb{Z}_2 \times \mathbb{Z}_8 \to {}^{\mathbb{Z}_4 \times \mathbb{Z}_8}\Big/_{\langle(2,4)\rangle} : (x, y) \mapsto (x \mod 2, y - 4x) + \langle(2, 4)\rangle$$

We leave it as an exercise to check that ψ is a well-defined isomorphism: it requires some creativity to invent such a function from nothing! In practice, method (a) is generally easier for us.

Other Examples

There are many other examples of factor groups. Often these have to be considered individually.

1. Let $H = \{2\pi n : n \in \mathbb{Z}\}$. This is a subgroup of the abelian group of $(\mathbb{R}, +)$. Can we identify the factor group ${}^{\mathbb{R}}\Big/_{H}$?

   It should be clear that in any given coset there is a unique element x such that $0 \leq x < 2\pi$ (this is like taking the remainder of x modulo 2π!). It follows that

$${}^{\mathbb{R}}\Big/_{H} = \{x + H : x \in [0, 2\pi)\}$$

   Indeed, you can check that the function

$$\psi : {}^{\mathbb{R}}\Big/_{H} \to S^1 : x + H \mapsto e^{ix}$$

   is a well-defined group isomorphism! The factor group construction therefore corresponds to wrapping the real line infinitely many times around a circle of circumference 2π.

2. Recall the description of the alternating group A_4. It can be (tediously) checked that

$$V = \{e, (12)(34), (13)(24), (14)(23)\}$$

is a normal subgroup of A_4 which is moreover isomorphic to the Klein 4-group. In this case, the factor group A_4/V has order $\frac{12}{4} = 3$ and so must be isomorphic to $\mathbb{Z}_3$: can you find an explicit isomorphism?

3. A similar analysis may be performed to see that $S_4/V \cong S_3$. See the homework.

Aside: An factor group of an *infinite* cyclic group As a final example we do something far more difficult: nothing this tricky is examinable!

Identify $G/H = (\mathbb{Z}_{10} \times \mathbb{Z}_6 \times \mathbb{Z})/\langle (4,2,3) \rangle$.

The challenge is that both G and H are *infinite,* whence we cannot simply use the index formula to count the number of cosets. Here is a way round the problem.

- Let $z = 3q + r$ be the result of the division algorithm applied to $z \in \mathbb{Z}$, where $r = 0, 1$ or 2. Then

$$(x, y, z) + H = (x, y, z) - q(4, 2, 3) + H = (x - 4q, y - 2q, r) + H$$

It follows that in every coset $(x, y, z) + H$, there is precisely one element (x, y, z) with $z = 0, 1$ or 2.

- The elements $(x, y, 0)$ where $x \in \mathbb{Z}_{10}$ and $y \in \mathbb{Z}_6$ all lie in different cosets: if two such were in the same coset, then

$$\begin{aligned}(x_1, y_1, 0) - (x_2, y_2, 0) \in H &\iff (x_1 - x_2, y_1 - y_2, 0) \in H \\ &\iff \begin{cases} x_1 \equiv x_2 \pmod{10} \\ \quad \text{and} \\ y_1 \equiv y_2 \pmod{6} \end{cases}\end{aligned}$$

Similarly all the elements $(x, y, 1)$ and $(x, y, 2)$ lie in different cosets.

- It follows that the elements $(x, y, 0)$, $(x, y, 1)$ and $(x, y, 2)$ are representatives of different cosets, and that all cosets have one such representative. There are therefore $10 \cdot 6 \cdot 3 = 180$ distinct cosets whence the factor group G/H is abelian of order 180.

- The prime decomposition of 180 is $2^2 \cdot 3^2 \cdot 5$: there are, up to isomorphism, *four* abelian groups of order 180, namely

$$\begin{aligned}&\mathbb{Z}_4 \times \mathbb{Z}_9 \times \mathbb{Z}_5 \cong \mathbb{Z}_{180} \\ &\mathbb{Z}_2 \times \mathbb{Z}_2 \times \mathbb{Z}_9 \times \mathbb{Z}_5 \cong \mathbb{Z}_2 \times \mathbb{Z}_{90} \\ &\mathbb{Z}_4 \times \mathbb{Z}_3 \times \mathbb{Z}_3 \times \mathbb{Z}_5 \cong \mathbb{Z}_3 \times \mathbb{Z}_{60} \\ &\mathbb{Z}_2 \times \mathbb{Z}_2 \times \mathbb{Z}_3 \times \mathbb{Z}_3 \times \mathbb{Z}_5 \cong \mathbb{Z}_6 \times \mathbb{Z}_{30}\end{aligned}$$

How do we distinguish between these? As before, we look for elements of a particular order (lots of scratch work may be required in general!).

- Compute the order of the coset $(1,1,1)+H$. Certainly its order must be divisible by 3, since the third entry of

  $$n(1,1,1) = (n,n,n) \in H$$

  requires $3 \mid n$. Thus let $n = 3k$. Now

  $$\begin{aligned} 3k(1,1,1)+H &= (3k,3k,3k)+H = (3k,3k,3k) - k(4,2,3) + H \qquad \text{(since } (4,2,3) \in H\text{)} \\ &= (-k,k,0)+H \\ &= H \iff 10 \mid k \text{ and } 6 \mid k \iff 30 \mid k \iff 90 \mid n \end{aligned}$$

  Since $G\Big/_H$ contains an element of order 90, our choices are narrowed to $\mathbb{Z}_{180}$ and $\mathbb{Z}_2 \times \mathbb{Z}_{90}$.

- We show that *every* element of $G\Big/_H$ has order dividing 90:

  $$\begin{aligned} 90\big((x,y,z)+H\big) &= (90x,90y,90z) - 30z(4,2,3) + H = (90x-120z, 90y-60z, 0) + H \\ &= (0,0,0)+H \end{aligned}$$

  We conclude that $G\Big/_H \cong \mathbb{Z}_2 \times \mathbb{Z}_{90}$. Phew!

You can check (it's hard!) that the function

$$\psi : \mathbb{Z}_2 \times \mathbb{Z}_{90} \to (\mathbb{Z}_{10} \times \mathbb{Z}_6 \times \mathbb{Z})\Big/_{\langle (4,2,3) \rangle} : (x,y) \mapsto (y, 3x+y, y) + H$$

is an isomorphism, though you'd have to be truly inspired to conjecture this out of thin air!

7 Homomorphisms and the First Isomorphism Theorem

In each of our examples of factor groups, we not only computed the factor group but identified it as isomorphic to an already well-known group. Each of these examples is a special case of a very important theorem: the *first isomorphism theorem.* This theorem provides a universal way of defining and identifying factor groups. Moreover, it has versions applied to all manner of algebraic structures, perhaps the most famous being the rank–nullity theorem of linear algebra. In order to discuss this theorem, we need to consider two subgroups related to any group homomorphism.

7.1 Homomorphisms, Kernels and Images

Definition 7.1. Let $\phi : G \to L$ be a homomorphism of multiplicative groups. The *kernel* and *image* of ϕ are the sets

$$\ker\phi = \{g \in G : \phi(g) = e_L\} \qquad \operatorname{Im}\phi = \{\phi(g) : g \in G\}$$

Note that $\ker\phi \subseteq G$ while $\operatorname{Im}\phi \subseteq L$.

Similar notions The image of a function is simply its range $\operatorname{Im}\phi = \operatorname{range}\phi$, so this is nothing new. You saw the concept of *kernel* in linear algebra. For example if $A \in M_{3\times 2}(\mathbb{R})$ is a matrix, then we can define the linear map

$$L_A : \mathbb{R}^2 \to \mathbb{R}^3 : \mathbf{x} \mapsto A\mathbf{x}$$

In this case, the kernel of L_A is precisely the *nullspace* of A. Similarly, the image of L_A is the *column-space* of A. All we are doing in this section is generalizing an old discussion from linear algebra.

Theorem 7.2. *Suppose that $\phi : G \to L$ is a homomorphism. Then*

1. $\phi(e_G) = e_L$
2. $\forall g \in G,\ (\phi(g))^{-1} = \phi(g^{-1})$
3. $\ker\phi \triangleleft G$
4. $\operatorname{Im}\phi \leq L$

Proof. 1. Suppose that $g \in G$. Then

$$\phi(g) = \phi(ge_G) = \phi(g)\phi(e_G) \implies e_L = \phi(e_G)$$

by the left cancellation law.

2. Suppose that $g \in G$. Then

$$e_L = \phi(e_G) = \phi(gg^{-1}) = \phi(g)\phi(g^{-1}) \implies (\phi(g))^{-1} = \phi(g^{-1})$$

3. First suppose that $k_1, k_2 \in \ker\phi$. Then

$$\phi(k_1k_2) = \phi(k_1)\phi(k_2) = e_L \implies k_1k_2 \in \ker\phi$$

and

$$\phi(k_1^{-1}) = (\phi(k_1))^{-1} = e_L \implies k_1^{-1} \in \ker\phi$$

It follows that $\ker\phi$ is a subgroup of G. To see that $\ker\phi$ is normal, recall, let $g \in G$ and $k \in \ker\phi$, then

$$\phi(gkg^{-1}) = \phi(g)\phi(k)\phi(g)^{-1} = e_L \implies gkg^{-1} \in \ker\phi$$

This is one of the conditions equaivalent to $\ker\phi \triangleleft G$.

4. Let $\phi(g_1), \phi(g_2) \in \operatorname{Im}\phi$. Then

$$\phi(g_1)\phi(g_2) = \phi(g_1g_2) \in \operatorname{Im}\phi$$

and

$$(\phi(g_1))^{-1} = \phi(g_1^{-1}) \in \operatorname{Im}\phi$$

Thus $\operatorname{Im}\phi$ is a subgroup of L.

■

Examples

1. Recall that the trace function $\operatorname{tr} : M_n(\mathbb{R}) \to \mathbb{R}$ is a homomorphism of additive groups. These are Abelian groups and so the kernel of tr is automatically normal without needing the above Theorem. The additive group of trace-free matrices[34] is a normal subgroup of $(M_n(\mathbb{R}), +)$:

$$\ker \operatorname{tr} = \{A \in M_n(\mathbb{R}) : \operatorname{tr} A = 0\} \triangleleft M_n(\mathbb{R})$$

2. Let $\phi : \mathbb{Z}_{36} \to \mathbb{Z}_{20}$ be defined by $\phi(n) = 5n \pmod{20}$. The kernel of ϕ is the subgroup

$$\ker \phi = \{n : 5n \equiv 0 \pmod{20}\} = \{0, 4, 8, 12, 16\} \triangleleft \mathbb{Z}_{36}$$

   This is simply the cyclic group C_5.

3. The map $\operatorname{sgn} : S_n \to \{1, -1\}$ given by $\operatorname{sgn}(\sigma) = \begin{cases} 1 & \text{if } \sigma \text{ even,} \\ -1 & \text{if } \sigma \text{ odd,} \end{cases}$ is a homomorphism of groups. Here $\{1, -1\}$ is a group under multiplication. Since the identity in the target group is 1, we have $\ker \operatorname{sgn} = A_n$, the alternating group of even permutations in S_n. Indeed $A_n \triangleleft S_n$.

4. $\det : \mathrm{GL}_n(\mathbb{R}) \to \mathbb{R}^\times$ is a homomorphism and so $\ker \det = \mathrm{SL}_n(\mathbb{R})$ is a normal subgroup $\mathrm{SL}_n(\mathbb{R}) \triangleleft \mathrm{GL}_n(\mathbb{R})$. Compare this with example 1.

All these examples should suggest an idea to you. Not only is every kernel a normal subgroup, the converse is also true: *any* normal subgroup is the kernel of some homomorphism. This (loosely) is the 1st isomorphism Theorem to which we will come shortly. It may seem counter-intuiutive, but the homomorphism approach actually makes calculations with factor groups easier! As the next lemma shows, there is a very easy correspondence between the cosets of the kernel of a homomorphism, and the elements of the image.

Lemma 7.3. *Suppose that $\phi : G \to L$ is a homomorphism. Then*

$$g_1 \ker \phi = g_2 \ker \phi \iff \phi(g_1) = \phi(g_2)$$

Proof. For all $g_1, g_2 \in G$, we have

$$\begin{aligned} g_1 \ker \phi = g_2 \ker \phi &\iff g_2^{-1} g_1 \in \ker \phi \\ &\iff \phi(g_2^{-1} g_1) = e_L \\ &\iff \phi(g_2)^{-1} \phi(g_1) = e_L \\ &\iff \phi(g_1) = \phi(g_2) \end{aligned}$$

■

The lemma tells us there is a bijective correspondence between the factor group $G/\ker \phi$ and the image $\operatorname{Im} \phi$. In the next theorem, we put this to use to help us determine what can possibly be a homomorphism.

Theorem 7.4. *Let $\phi : G \to L$ be a homomorphism.*

[34] This kernel is often written $\mathfrak{sl}_n(\mathbb{R})$ (for the *special-linear algebra*), and is very much related to the special linear group $\mathrm{SL}_n(\mathbb{R})$. Indeed the expression $\det e^A = e^{\operatorname{tr} A}$ shows that matrix exponentiation is a map $\exp : \mathfrak{sl}_n(\mathbb{R}) \to \mathrm{SL}_n(\mathbb{R})$.

1. *If G is a finite group then* $\operatorname{Im}\phi$ *is a finite subgroup of L and its order divides that of G. More succinctly:* $|G| < \infty \implies |\operatorname{Im}\phi| \,\Big|\, |G|$.

2. *Similarly,* $|L| < \infty \implies |\operatorname{Im}\phi| \,\Big|\, |L|$.

Note that we are only assuming one of the groups to be finite in each case.

Proof. 1. If G is a finite group, then $\operatorname{Im}\phi$ is a finite subgroup of L. Lemma 7.3 tells us that

$$\phi(g_1) = \phi(g_2) \iff g_1 \ker\phi = g_2 \ker\phi$$

whence there are precisely as many elements of $\operatorname{Im}\phi$ as there are distinct cosets of $\ker\phi$ in G. But this is the definition of the index:

$$|\operatorname{Im}\phi| = (G : \ker\phi)$$

Given that G is finite, the discussion following Lagrange's Theorem quickly says that

$$|G| = |\operatorname{Im}\phi| \cdot |\ker\phi| \implies |\operatorname{Im}\phi| \,\Big|\, |G|$$

2. This is immediate from Lagrange's Theorem: $\operatorname{Im}\phi$ is a subgroup of a finite group L and so the order of $\operatorname{Im}\phi$ divides the order of L.

■

Examples

1. Suppose that $|G| = 17$ and $|L| = 13$. How many distinct homomorphisms are there $\phi : G \to L$? If ϕ were such a homomorphism, the Theorem says that $|\operatorname{Im}\phi|$ divides both $|G|$ and $|L|$. But the only such positive integer is 1. Since the image of any homomorphism always contains the identity ($\phi(e_G) = e_L$), it follows that there is only one homomorphism! ϕ must be the function defined by $\phi(g) = e_L$, $\forall g \in G$.
   More generally, if $\gcd(|G|, |L|) = 1$, then the only homomorphism $\phi : G \to L$ is the trivial function $\phi : g \mapsto e_L$.

2. How many homomorphisms are there $\phi : \mathbb{Z}_4 \to S_3$? Again the Theorem tells us that $|\operatorname{Im}\phi|$ divides $4 = |\mathbb{Z}_4|$ and $6 = |S_3|$: thus $|\operatorname{Im}\phi|$ is either 1 or 2. If $|\operatorname{Im}\phi| = 2$ then $\operatorname{Im}\phi$ is a subgroup of order 2 of S_3. There are exactly 3 of these: $\{e, \mu_i\}$ for each $i = 1, 2, 3$. Since a homomorphism must map the identity to the identity we therefore have the homomorphisms

$$\phi_1 : \begin{pmatrix}0\\1\\2\\3\end{pmatrix} \mapsto \begin{pmatrix}e\\\mu_1\\e\\\mu_1\end{pmatrix}, \qquad \phi_2 : \begin{pmatrix}0\\1\\2\\3\end{pmatrix} \mapsto \begin{pmatrix}e\\\mu_2\\e\\\mu_2\end{pmatrix}, \qquad \phi_3 : \begin{pmatrix}0\\1\\2\\3\end{pmatrix} \mapsto \begin{pmatrix}e\\\mu_3\\e\\\mu_3\end{pmatrix}.$$

   Finally if $\operatorname{Im}\phi$ has one element then ϕ is the trivial homomorphism $\phi(z) = e$, $\forall z \in \mathbb{Z}_4$. There are therefore 4 distinct homomorphisms.

Theorem 7.5. *There are exactly $d = \gcd(m, n)$ distinct homomorphisms $\phi : \mathbb{Z}_m \to \mathbb{Z}_n$, defined by*

$$\phi(x) = k\frac{n}{d}x \pmod{n} \quad \textit{where} \quad k = 0, \ldots, d-1$$

There are several ways of proving this: one is in the homework. We use the above discussion on the cardinality of the image.

Proof. Suppose $\phi : \mathbb{Z}_m \to \mathbb{Z}_n$ is a homomorphism and $d = \gcd(m, n)$. Then $|\operatorname{Im}\phi| \,\Big|\, d$. However $\operatorname{Im}\phi$ is a subgroup of $\mathbb{Z}_n$ which is necessarily cyclic. Recalling the structure of cyclic groups[35] we see that must be a subgroup of the *unique* cyclic subgroup of order d in $\mathbb{Z}_n$. This is generated by $\frac{n}{d}$. The only possible choices for our homomorphisms are therefore[36]

$$\phi_k(x) = k\frac{n}{d}x \pmod{n}$$

for each $k = 0, 1, 2, \ldots, d-1$. It remains only to check that these are well-defined functions. For this, note that for any $j \in \mathbb{Z}$ we have,

$$\begin{aligned}\phi_k(x + jm) &= k\frac{n}{d}(x + jm) \equiv k\frac{n}{d}x + knj\frac{m}{d} \equiv k\frac{n}{d}x \pmod{n} && \text{(since } \tfrac{m}{d} \in \mathbb{Z}\text{)}\\ &= \phi_k(x)\end{aligned}$$

■

Example Suppose that $\phi : \mathbb{Z}_{12} \to \mathbb{Z}_{20}$ is a homomorphism. Since $\gcd(12, 20) = 4$, the image of ϕ must be a subgroup of $C_4 = \langle 5 \rangle \leq \mathbb{Z}_{20}$. There are four choices:

$$\phi_0(x) = 0, \qquad \phi_1(x) = 5x, \qquad \phi_2(x) = 10x, \qquad \phi_3(x) = 15x \pmod{20}$$

Reversing the argument, we see that there are also four distinct homomorphisms $\psi : \mathbb{Z}_{20} \to \mathbb{Z}_{12}$, namely

$$\psi_0(x) = 0, \qquad \psi_1(x) = 3x, \qquad \psi_2(x) = 6x, \qquad \psi_3(x) = 9x \pmod{12}$$

7.2 The 1st Isomorphism Theorem

We have seen that all kernels of group homomorphisms are normal subgroups. In fact *all* normal subgroups are the kernel of some homomorphism. We state this in two parts.

Theorem 7.6 (1st Isomorphism Theorem)**.** *Let G be a group.*

1. *Let $H \triangleleft G$. Then $\gamma : G \to {}^{G}\!/_{H}$ defined by $\gamma(g) = gH$ is a homomorphism with $\ker\gamma = H$.*
2. *If $\phi : G \to L$ is a homomorphism with kernel H, then $\mu : {}^{G}\!/_{H} \to \operatorname{Im}\phi$ defined by $\mu(gH) = \phi(g)$ is an isomorphism.*

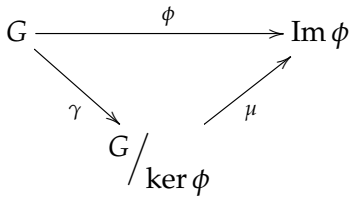
The Theorem can be summarised by the following formula,

$${}^{G}\!/_{\ker\phi} \cong \operatorname{Im}\phi.$$

[35] Recall that a cyclic group $\mathbb{Z}_n$ has exactly one subgroup, which is itself cyclic, of each order d which divides n. Therefore if $\operatorname{Im}\phi$ is a subgroup of $\mathbb{Z}_n$, then it is cyclic. Since its order divides d, it must also be a subgroup of the unique $C_d \leq \mathbb{Z}_n$.

[36] We may choose $\phi_k(1)$ for each k. If these are homomorphisms, then $\phi_k(2) = \phi_k(1) + \phi_k(1)$, etc.

The notion of a *commutative diagram* is often useful for summarizing theorems. To say that a diagram commutes means that if there are multiple paths from one side of the diagram to the other, they both give the same result. In this case one can travel from G to $\operatorname{Im}\phi$ in two ways. For the 1st isomorphism theorem, this means $\phi = \mu \circ \gamma$.



Definition 7.7. Given a normal subgroup $H \triangleleft G$, the function $\gamma : G \to {}^{G}\!/_{H} : g \mapsto gH$ is called the *canonical* or *fundamental homomorphism*.

Proof of Theorem. We check that the functions γ and μ have the properties we claim.

1. γ is certainly a well-defined function: we need only check that it is a homomorphism with $\ker\gamma = H$. However

   $$\gamma(g_1)\gamma(g_2) = g_1H \cdot g_2H = (g_1g_2)H = \gamma(g_1g_2)$$

   by the definition of multiplication in a factor group. Moreover, the identity in the factor group is H, whence

   $$\ker\gamma = \{g \in G : \gamma(g) = H\}$$

   Thus $g \in \ker\gamma \iff gH = H \iff g \in H$, whence the kernel of γ is H, as claimed.

2. Clearly $H \triangleleft G$ (Theorem 7.2) and so the factor group ${}^{G}\!/_{H}$ is well-defined. We need to check that $\mu : {}^{G}\!/_{H} \to \operatorname{Im}\phi$ defined by $\mu(gH) = \phi(g)$ is an isomorphism.

   Well-definition and Bijectivity These are immediate from Lemma 7.3.

   Homomorphism For all $g_1H, g_2H \in {}^{G}\!/_{H}$, we have

   $$\begin{aligned}\mu(g_1H \cdot g_2H) &= \mu(g_1g_2H) = \phi(g_1g_2)\\ &= \phi(g_1)\phi(g_2) && \text{(since } \phi \text{ is a homomorphism)}\\ &= \mu(g_1H)\mu(g_2H)\end{aligned}$$

   μ is a well-defined, bijective homomorphism and is therefore an isomorphism.

∎

Examples Here are two examples where we can calculate all the pieces in the Theorem.

1. Let $\phi : \mathbb{Z}_{10} \to \mathbb{Z}_{20}$ be the homomorphism with $\phi(1) = 4$. Then, by the homomorphism property, $\phi(x) = 4x \pmod{20}$. In particular

   $$\begin{aligned}&\ker\phi = \{x \in \mathbb{Z}_{10} : 4x \equiv 0 \pmod{20}\} = \{0,5\} \quad \text{and,}\\ &\operatorname{Im}\phi = \{4x \pmod{20} : x \in \mathbb{Z}_{10}\} = \{0,4,8,12,16\}\end{aligned}$$

   Observe that $\ker\phi = \langle 5\rangle \leq \mathbb{Z}_{10}$ is isomorphic to C_2 and $\operatorname{Im}\phi = \langle 4\rangle \leq \mathbb{Z}_{20}$ is isomorphic to C_5. The factor group is

   $${}^{\mathbb{Z}_{10}}\!/_{\ker\phi} = \Big\{\{0,5\},\{1,6\},\{2,7\},\{3,8\},\{4,9\}\Big\}$$

The function

$$\mu : \mathbb{Z}_{10}\Big/_{\ker\phi} \to \operatorname{Im}\phi : \begin{pmatrix} \{0,5\} \\ \{1,6\} \\ \{2,7\} \\ \{3,8\} \\ \{4,9\} \end{pmatrix} \mapsto \begin{pmatrix} 0 \\ 4 \\ 8 \\ 12 \\ 16 \end{pmatrix} \qquad \text{i.e.} \qquad \mu(x + \ker\phi) = 4x \pmod{20}$$

is the isomorphism from the Theorem.

2. Rather than starting with a homomorphism, suppose we simply wanted to identify the factor group $\mathbb{Z}_{10}\Big/_{H}$ with a well-known group (here $H = \{0,5\}$ is our normal subgroup from before). We might search for a homomorphism $\psi : \mathbb{Z}_{10} \to L$ whose kernel is H. Since $\mathbb{Z}_{10}\Big/_{H}$ clearly has 5 elements (5 cosets of H in $\mathbb{Z}_{10}$), the obvious thing to do is search for a homomorphism

   $$\psi : \mathbb{Z}_{10} \to \mathbb{Z}_5 \quad \text{with} \quad \ker\psi = H$$

   It should be clear that $\psi(x) = x \pmod 5$ is such a homomorphism! Since $\operatorname{Im}\psi = \mathbb{Z}_5$, the first isomorphism theorem says that $\mathbb{Z}_{10}\Big/_{H} \cong \mathbb{Z}_5$. The isomorphism μ in this case is simply

   $$\mu(x + H) = x \pmod 5$$

The point of these examples is that the Theorem can be used in two ways, both of which help us find alternative descriptions of factor groups.

- Start with a homomorphism $\phi : G \to L$ and build an isomorphism $\mu : G\Big/_{\ker\phi} \cong \operatorname{Im}\phi$.
- Start with a normal subgroup $H \triangleleft G$ and construct a homomorphism ϕ with $H = \ker\phi$. Then $G\Big/_{H} \cong \operatorname{Im}\phi$.

Direct product problems

We quickly refresh the examples we saw in the last section in the language of the first isomorphism theorem.

1. Given $G\Big/_{H} = (\mathbb{Z}_4 \times \mathbb{Z}_8)\Big/_{\langle(0,1)\rangle}$, define

   $$\phi : \mathbb{Z}_4 \times \mathbb{Z}_8 \to \mathbb{Z}_4 : (x,y) \mapsto x$$

   This is clearly a homomorphism, with $\ker\phi = \{(0,1)\}$. Indeed ϕ is also *surjective.* It follows that

   $$(\mathbb{Z}_4 \times \mathbb{Z}_8)\Big/_{\langle(0,1)\rangle} \cong \operatorname{Im}\phi = \mathbb{Z}_4$$

   The explicit isomorphism is

   $$\mu : (x,y) + H \mapsto x$$

   This is precisely the *inverse* of the isomorphism ψ we stated when originally considering this example.

In the first example, we pulled ϕ out of thin air, and it worked! In general, it is often a good idea to search for a homomorphism $\phi : G \to G$ with $\ker\phi = H$: this typically gives you more room with wich to work. This is what we do in the next example.

2. For ${}^{G}\!/_{H} = {}^{(\mathbb{Z}_4 \times \mathbb{Z}_8)}\!/_{\langle(0,2)\rangle}$, we search for a homomorphism

   $$\phi : \mathbb{Z}_4 \times \mathbb{Z}_8 \to \mathbb{Z}_4 \times \mathbb{Z}_8$$

   with $\ker\phi = \langle(0,2)\rangle$. It should seem reasonable to try[37]

   $$\phi(x,y) = (x,4y)$$

   Certainly $(x,y) \in \ker\phi \iff x = 0 \in \mathbb{Z}_4$ and $4y = 0 \in \mathbb{Z}_8$. This is if and only if $2 \mid y$, whence $\ker\phi = \{(0,2)\}$. The 1st isomorphism theorem says that

   $${}^{(\mathbb{Z}_4 \times \mathbb{Z}_8)}\!/_{\langle(0,2)\rangle} \cong \operatorname{Im}\phi = \{(x,4y) \in \mathbb{Z}_4 \times \mathbb{Z}_8\}$$

   via the isomorphism

   $$\mu((x,y) + H) = (x,4y)$$

   The result is clearly isomorphic to $\mathbb{Z}_4 \times \mathbb{Z}_2$ via $(x,4y) \mapsto (x,y)$.

3. We play the same game with ${}^{G}\!/_{H} = {}^{(\mathbb{Z}_4 \times \mathbb{Z}_8)}\!/_{\langle(2,4)\rangle}$, defining

   $$\phi : \mathbb{Z}_4 \times \mathbb{Z}_8 \to \mathbb{Z}_4 \times \mathbb{Z}_8 : (x,y) \mapsto (2x, y-2x)$$

   Certainly $\phi(x,y) = (0,0) \iff 2x = 0 \in \mathbb{Z}_4$ and $y = 2x \in \mathbb{Z}_8$. Thus $x = 2k$ is even, and $y = 4k \in \mathbb{Z}_8$ is the corresponding multiple of 4. We therefore have a homomorphism with $\ker\phi = \langle(2,4)\rangle$, whence

   $${}^{(\mathbb{Z}_4 \times \mathbb{Z}_8)}\!/_{\langle(2,4)\rangle} \cong \operatorname{Im}\phi = \{(2x, y-2x)\} = \{0,2\} \times \mathbb{Z}_8 \cong \mathbb{Z}_2 \times \mathbb{Z}_8$$

Here are two further examples written in this language.

1. Let $H = \langle 2\pi\rangle \leq \mathbb{R}$ and define $\phi : \mathbb{R} \to (\mathbb{C}^\times, \cdot)$ by $\phi(x) = e^{ix}$. Clearly ϕ is a homomorphism with

   $$\ker\phi = \{x \in \mathbb{R} : e^{ix} = 1\} = H$$

   It follows that

   $${}^{\mathbb{R}}\!/_{H} \cong \operatorname{Im}\phi = S^1 = \{e^{ix}\}$$

   Indeed $\mu(x + \langle 2\pi\rangle) = e^{ix}$ is the isomorphism guaranteed by the 1st isomorphism theorem.

2. Let $\phi : S^1 \to S^1 : e^{i\theta} \mapsto e^{2i\theta}$. Clearly ϕ is a homomorphism with $\ker\phi = \{1,-1\}$. It follows that

   $${}^{S^1}\!/_{\{1,-1\}} \cong \operatorname{Im}\phi = S^1$$

In general, it can be very difficult to *construct* a simple homomorphim with the correct kernel. The primary application of the theorem comes when starting with a given homomorphism.

[37] We need $\phi(0,2) = (0,0)$. Moreover, if $\phi(1,0) = (a,b)$ and $\phi(0,1) = (c,d)$, then we must have $\phi(x,y) = (ax+cy, bx+dy)$, so any possible homomorphism must look like a *linear* map.

8 Conjugation, Centers and Automorphisms

In this section we describe another equivalence relation on a group, that of *conjugacy*. Conjugacy is the group theory abstraction of the idea of *similarity* from linear algebra: two square matrices A and B are said to be similar if there exists some invertible matrix S for which $B = SAS^{-1}$. You should recall that such matrices have the same eigenvalues and, essentially, 'do the same thing' with respect to different bases.

Definition 8.1. Let G be a group and $g_1, g_2 \in G$. We say that g_1 is *conjugate to* g_2 if

$$\exists h \in G \quad \text{such that} \quad g_2 = hg_1h^{-1}$$

Conjugation is intimately related to the concept of normal subgroup. Recall that a subgroup $H \leq G$ is normal if and only if

$$\forall g \in G, h \in H, \quad ghg^{-1} \in H$$

A normal subgroup can therefore be defined as a subgroup which is closed under conjugation.

Theorem 8.2. *Conjugacy is an equivalence relation.*

The proof is an exercise.

Definition 8.3. The equivalence classes of a group G under conjugacy are termed the *conjugacy classes* of G.

Examples

1. If G is Abelian then every conjugacy class contains only one element. Observe that g_1 and g_2 are conjugate if and only if

$$\exists h \in G \quad \text{such that} \quad g_2 = hg_1h^{-1} = g_1hh^{-1} = g_1$$

2. The smallest non-Abelian group is $D_3 \cong S_3$. Its conjugacy classes are

$$\{e\}, \quad \{\rho_1, \rho_2\}, \quad \{\mu_1, \mu_2, \mu_3\}$$

This can be computed directly, but it follows immediately from...

Theorem 8.4. *The conjugacy classes of S_n are the* cycle types.

The concept of cycle type is straightforward: for example $(123)(45)$ has the same cycle type as $(156)(23)$, but not the same as $(12)(34)$. Just write an element of S_n as a product of disjoint cycles and its cycle type is clear. The proof involves some messy notation, so you may want to avoid on a first reading.
In the above example, e is a 0-cycle, ρ_1, ρ_2 are 3-cycles and μ_1, μ_2, μ_3 are 2-cycles: these form the conjugacy classes by the Theorem.

Proof. Suppose that $(a_1 \cdots a_k) \in S_n$ is a k-cycle and $\rho \in S_n$ is any element. It is easy to see that

$$\rho(a_1 \cdots a_k)\rho^{-1} = (\rho(a_1) \cdots \rho(a_k))$$

is also a k-cycle, since the elements $\rho(a_i)$ must be distinct. Now let $\tau \in S_n$ be written as the product of disjoint cycles $\tau = \tau_1 \cdots \tau_l$. Then

$$\rho\tau\rho^{-1} = (\rho\tau_1\rho^{-1})(\rho\tau_2\rho^{-1}) \cdots (\rho\tau_l\rho^{-1})$$

which has the same cycle type as τ (again ρ permutes the elements of $\{1, 2, \ldots, n\}$) Thus conjugation preserves cycle type.
Conversely, let $\sigma = \sigma_1 \cdots \sigma_l$ and $\tau = \tau_1 \cdots \tau_l$ be elements of S_n with the same cycle type; otherwise said, σ_i and τ_i are k-cycles for the *same* k. Define a permutation π by writing σ and τ one on top of the other in standard notation:

$$\pi = \begin{pmatrix} \sigma_1 & \sigma_2 & \cdots & \sigma_l & s_1 & s_2 & \cdots \\ \tau_1 & \tau_2 & \cdots & \tau_l & t_1 & t_2 & \cdots \end{pmatrix},$$

where we write each of the elements of the cycle σ_i in a row and s_i, t_i are the remaining elements of the set $\{1, 2, \ldots, n\}$ missing from each row, written in any order. We claim that $\tau = \pi\sigma\pi^{-1}$. If $\sigma_{i,j}$ and $\tau_{i,j}$ refer to the j^{th} element of the orbits σ_i and τ_i respectively, then

$$\pi\sigma\pi^{-1}(\tau_{i,j}) = \pi\sigma(\sigma_{i,j}) = \pi\sigma_{i,j+1} = \tau_{i,j+1} = \tau(\tau_{i,j})$$

If $t = t_i$ for some i, then $\pi\sigma\pi^{-1}(t_i) = \pi\sigma(s_i) = \pi(s_i) = t_i$. Either way, $\pi\sigma\pi^{-1} = \tau$, as required. ∎

Examples

1. If $\sigma = (13)(24)$ and $\rho = (124)$ in S_4, then

   $$\sigma\rho\sigma^{-1} = \big(\sigma(1)\,\sigma(2)\,\sigma(4)\big) = (342) = (234) \qquad \text{and,}$$
   $$\rho\sigma\rho^{-1} = \big(\rho(1)\,\rho(3)\big)\big(\rho(2)\,\rho(4)\big)(23)(41) = (14)(23)$$

2. According to the Theorem, the permutations $(145)(627)$ and $(165)(234)$ in S_7 are conjugate by the permutation

   $$\pi = \begin{pmatrix} 1 & 4 & 5 & 6 & 2 & 7 & 3 \\ 1 & 6 & 5 & 2 & 3 & 4 & 7 \end{pmatrix} = \begin{pmatrix} 1 & 2 & 3 & 4 & 5 & 6 & 7 \\ 1 & 3 & 7 & 6 & 5 & 2 & 4 \end{pmatrix} = (23746)$$

   Indeed

   $$\pi(145)(627)\pi^{-1} = (23746)(145)(627)(26473) = (165)(234)$$

   There are other possible choice of π, for example by writing the orbits in different orders.

3. Recall earlier when we claimed that $V = \{e, (12)(34), (13)(24), (14)(23)\}$ is a normal subgroup of A_4. While one still has to check to V is a subgroup, the normality is now clear since V contains all the elements in A_4 of the cycle type $(ab)(cd)$ which is preserved by conjugation.

Thus A_4/V is a factor group of order $\frac{12}{4} = 3$ which must therefore be isomorphic to C_3. Indeed the cosets of V may be written[38]

$$A_4/V = \{V, (123)V, (132)V\}$$

An example isomorphism $\mu : A_4/V \to C_3$ from the first isomorphism theorem is then

$$\mu : \begin{pmatrix} V \\ (123)V \\ (132)V \end{pmatrix} = \begin{pmatrix} e \\ (123) \\ (132) \end{pmatrix}$$

where we view C_3 in a natural way as a subgroup of S_4.

Automorphisms

Conjugation by a fixed element of a group is a special case of a general structure-preserving transformation.

Definition 8.5. An *automorphism* of a group G is an isomorphism of G with itself. The set of such is labelled $\operatorname{Aut} G$. The *inner automorphisms* of G are the conjugations

$$\operatorname{Inn} G = \{c_h : G \to G \text{ where } c_h(g) = hgh^{-1}\}$$

Examples

1. Consider the automorphisms of $\mathbb{Z}_4$. To define a homomorphism $\phi : \mathbb{Z}_4 \to \mathbb{Z}_4$, it is enough to choose the value of $\phi(1)$. Indeed, to obtain a bijection, we need to map 1 (a generator) to a generator. There are therefore two choices:

   $$\phi_0(x) = x \mod 4 \qquad \phi_1(x) = -x \mod 4$$

   Observe that the set $\operatorname{Aut}(\mathbb{Z}_4) = \{\phi_0, \phi_1\}$ forms a group (necessarily isomorphic to C_2) under composition of functions.
   There is only one inner automorphism of $\mathbb{Z}_4$, since $\mathbb{Z}_4$ is abelian.

2. Find the automorphisms of S_3 is a little harder. First observe that if $\phi \in \operatorname{Aut}(S_3)$, then

   $$(\phi(x))^n = e \iff \phi(x^n) = e \iff x^n = e$$

   so that the orders of x and $\phi(x)$ are identical. The group S_3 is generated by two elements: $\mu := (12)$ and $\rho := (123)$, where $\rho\mu = \mu\rho^2$;

   $$e = \rho^3, \quad (132) = \rho^2, \quad (13) = \rho\mu, \quad (23) = \rho^2\mu$$

[38] In fact $(123)V = (134)V = (243)V = (142)V$ and $(132)V = (143)V = (234)V = (124)V$.

We therefore have a maximum of *six* possible choices of automorphism: $\phi(\mu)$ is either $\mu, \rho\mu$ or $\rho^2\mu$ and $\phi(\rho) = \rho$ or ρ^2. A little thinking shows that *all of these* functions are in fact automorphisms! Moreover, $\mathrm{Aut}(G)$ is a group of order 6 which is easily seen to be non-abelian, whence $\mathrm{Aut}(S_3) \cong S_3$. In fact, each of these functions is conjugation by some element of S_3: explicitly

$$c_e : \begin{pmatrix} e \\ \rho \\ \rho^2 \\ \mu \\ \rho\mu \\ \rho^2\mu \end{pmatrix} \mapsto \begin{pmatrix} e \\ \rho \\ \rho^2 \\ \mu \\ \rho\mu \\ \rho^2\mu \end{pmatrix} \qquad c_\rho : \begin{pmatrix} e \\ \rho \\ \rho^2 \\ \mu \\ \rho\mu \\ \rho^2\mu \end{pmatrix} \mapsto \begin{pmatrix} e \\ \rho \\ \rho^2 \\ \rho^2\mu \\ \mu \\ \rho\mu \end{pmatrix} \qquad c_{\rho^2} : \begin{pmatrix} e \\ \rho \\ \rho^2 \\ \mu \\ \rho\mu \\ \rho^2\mu \end{pmatrix} \mapsto \begin{pmatrix} e \\ \rho \\ \rho^2 \\ \rho\mu \\ \rho^2\mu \\ \mu \end{pmatrix}$$

$$c_\mu : \begin{pmatrix} e \\ \rho \\ \rho^2 \\ \mu \\ \rho\mu \\ \rho^2\mu \end{pmatrix} \mapsto \begin{pmatrix} e \\ \rho^2 \\ \rho \\ \mu \\ \rho^2\mu \\ \rho\mu \end{pmatrix} \qquad c_{\rho\mu} : \begin{pmatrix} e \\ \rho \\ \rho^2 \\ \mu \\ \rho\mu \\ \rho^2\mu \end{pmatrix} \mapsto \begin{pmatrix} e \\ \rho^2 \\ \rho \\ \rho^2\mu \\ \rho\mu \\ \mu \end{pmatrix} \qquad c_{\rho^2\mu} : \begin{pmatrix} e \\ \rho^2 \\ \rho \\ \mu \\ \rho\mu \\ \rho^2\mu \end{pmatrix} \mapsto \begin{pmatrix} e \\ \rho \\ \rho^2 \\ \rho\mu \\ \mu \\ \rho^2\mu \end{pmatrix}$$

It follows that $\mathrm{Inn}(S_3) = \mathrm{Aut}(S_3) \cong S_3$.

Indeed we have a general result here:

Theorem 8.6. *The sets* Aut G *and* Inn G *form groups under composition. Moreover* Inn G *is a subgroup of* Aut G.

Proof. We sketch the argument for Aut G first.

Closure It is straightforward to check that composition of two isomorphisms is an isomorphism.

Associativity Aut G consists of functions under composition.

Identity $\mathrm{id} : g \mapsto g$ is clearly an automorphism and moreover $\forall \psi \in \mathrm{Aut}(G),\ \psi \circ \mathrm{id} = \mathrm{id} \circ \psi = \psi$.

Inverse If $\phi \in$ Aut G it is also staightforward to check that the inverse function $\phi^{-1} : G \to G$ is automorphism.

For Inn G, note that each c_h is a homomorphism:

$$c_h(g_1g_2) = h(g_1g_2)h = (hg_1h^{-1})(hg_2h)^{-1} = c_h(g_1)c_h(g_2)$$

It also has inverse $c_h^{-1} = c_{h^{-1}}$ since

$$c_{h^{-1}}(c_h(g)) = h^{-1}(hgh^{-1})h = g \implies c_{h^{-1}} \circ c_h = \mathrm{id}$$

Thus each c_h is an automorphism of G and indeed Inn G is closed under inverses. Finally we check that Inn G is closed under composition:

$$(c_{g_1} \circ c_{g_2})(h) = g_1(g_2hg_2^{-1})g_1^{-1} = (g_1g_2)h(g_1g_2)^{-1} = c_{g_1g_2}(h) \qquad (c)$$

Inn G is therefore a subgroup of Aut G.

■

Theorem 8.7. $\operatorname{Inn} G \triangleleft \operatorname{Aut} G$.

Proof. Let $\tau \in \operatorname{Aut} G$ and $c_h \in \operatorname{Inn} G$. It is enough to see that $\tau c_h \tau^{-1} \in \operatorname{Inn} G$. Since $\tau c_h \tau^{-1}$ is a *function,* we compute what it does to a general element $g \in G$.

$$\begin{aligned}
(\tau c_h \tau^{-1})(g) &= \tau\Big(c_h\big(\tau^{-1}(g)\big)\Big) = \tau\big(h\tau^{-1}(g)h^{-1}\big) \\
&= \tau(h)\tau\big(\tau^{-1}(g)\big)\tau(h^{-1}) && \text{(since } \tau \text{ is a homomorphism)} \\
&= \tau(h)g\tau(h)^{-1} && \text{(again since } \tau \text{ is an homomorphism)} \\
&= c_{\tau(h)}(g)
\end{aligned}$$

Therefore $\tau c_h \tau^{-1} = c_{\tau(h)}$, which is an element of $\operatorname{Inn} G$. ∎

Since conjugation by an element $g \in G$ is an automorphism of G, conjugation must map subgroups of G to isomorphic subgroups. We also call such subgroups *conjugate.*

Example Let $H = \{e, \mu_1\} \leq D_3$. Then

$$c_{\rho_1} H = \rho_1 H \rho_1^{-1} = \{e, \rho_1\mu_1\rho_2\} = \{e, \mu_2\}$$

If we compute all six possible conjugations of H, we obtain

$$\begin{aligned}
\{e, \mu_1\} &= H = c_e H = c_{\mu_1} H, \\
\{e, \mu_2\} &= c_{\rho_1} H = c_{\mu_3} H \\
\{e, \mu_3\} &= c_{\rho_2} H = c_{\mu_2} H
\end{aligned}$$

These comprise all the two element subgroups of D_3.

Centers

We say that an element g in a group G *commutes* with another element $a \in G$ if the order of multiplication is irrelevant: i.e. if $ga = ag$. It is a natural question to ask if there are any elements in a group which commute with *all other elements.* There are two simple cases to consider:

- If G is abelian, then every element commutes with every other element!
- The identity e commutes with everything, regardless of the group.

In general, the set of such elements will fall somewhere between these extremes. This subset will turn out to form another normal subgroup of G.

Definition 8.8. The *center* of a group G is the subset of G defined by

$$Z(G) := \{g \in G : \forall h \in G,\ gh = hg\}$$

We will prove that $Z(G) \triangleleft G$ shortly, although a simple proof (check the axioms of a subgroup and that the left and right cosets are equal) is straightforward. Instead, here are a few examples.

Examples

1. $Z(G) = G \iff G$ is Abelian.
2. $Z(D_3) = \{e\}$. This is straightforward to check as there are only 6 elements!
3. In general $Z(D_{2n+1}) = \{e\}$ and $Z(D_{2n}) = \{e, \rho_{n/2}\}$, where $\rho_{n/2}$ is rotation by 180°.
   For example, it is easy to see in D_{2n+1} that any rotation and reflection fail to commute.
4. $Z(S_n) = \{e\}$ if $n \geq 3$.
5. $Z(\mathrm{GL}_n(\mathbb{R})) = \{\lambda I_n : \lambda \in \mathbb{R}^\times\}$.

The challenge with centers is that they are typically very difficult to compute, at least in part because we need to think about *non-abelian* groups in order to generate interesting examples. As an example we give an argument for computing $Z(\mathrm{GL}_n(\mathbb{R}))$.

Let $A \in \mathrm{GL}_n(\mathbb{R})$ be a matrix with only one eigenvector[39] $\mathbf{v}$, and let $Z \in Z(\mathrm{GL}_n(\mathbb{R}))$. Then

$$AZ\mathbf{v} = ZA\mathbf{v} = \lambda Z\mathbf{v}$$

where λ is the corresponding eigenvalue of A. It follows that $Z\mathbf{v}$ is an eigenvector of A, whence $Z\mathbf{v}$ is parallel to $\mathbf{v}$. Since our construction depended only on the initial choice of vector $\mathbf{v}$, it follows that $Z\mathbf{v}$ must be parallel to $\mathbf{v}$ for *every possible choice* of $\mathbf{v}$. The only such matrices are multiples of the identity.

Theorem 8.9. $Z(G) \triangleleft G$.

Proof. We have already done most of the work. Define $\phi : G \to \operatorname{Inn} G$ by $\phi(g) = c_g$. Thus each *element* $\phi(g)$ is the *function* 'conjugation by g.' We quickly see that ϕ is a homomorphism:

$$\begin{aligned}\phi(gh)(x) = c_{gh}(x) &= (gh)x(gh)^{-1} = g(hxh^{-1})g^{-1} = c_g(c_h(x)) \\ &= \Big(\phi(g) \circ \phi(h)\Big)(x)\end{aligned}$$

We compute the kernel of ϕ:

$$\begin{aligned}g \in \ker\phi &\iff c_g = \mathrm{id} \\ &\iff \forall h \in G, \quad ghg^{-1} = h \\ &\iff g \in Z(G)\end{aligned}$$

It follows that $\ker\phi = Z(G) \triangleleft G$. ∎

In fact $\phi : G \to \operatorname{Inn} G$ is a surjective homomorphism (every inner automorphism is a conjugation). The 1st isomorphism theorem tells us that

$$G\Big/_{Z(G)} \cong \operatorname{Inn} G$$

for any group G.

[39] Such A exist: extend $\mathbf{v}$ to an orthonormal basis $\mathbf{v}, \mathbf{v}_2, \ldots \mathbf{v}_n$ of $\mathbb{R}^n$ and let $A = I + \mathbf{v}(\mathbf{v}_2^T + \cdots + \mathbf{v}_n^T)$. With respect to this basis, A has 1's down the main diagonal and the diagonal immediately above the main, and zeros elsewhere: a classic Jordan form from linear algebra.

9 Group actions

For much of these notes, groups have been abstract objects. We have stated theorems in a general way so that a result may apply as widely as possible. While this approach certainly fits the general philosophy of pure mathematics, it doesn't leave one with the feeling that groups are *useful.* What is the point of groups, beyond providing a playground for mathematicians?

A simple answer is that groups are useful because of *how they transform sets.* This idea provided the first foundations of group theory: recall Cayley's Theorem that every group is a collection of permutations. But permuting *what?* This depends on the group and your own creativity: the possibilities are endless! Indeed we have presented several of our examples in this vein.

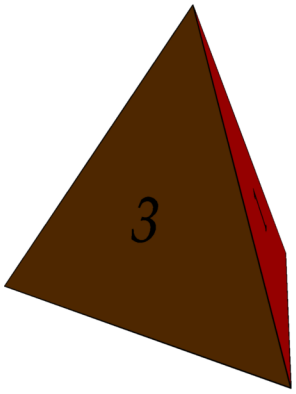
- The symmetric group S_n is described in terms of what its elements do to the set $\{1, \ldots, n\}$.
- The dihedral group D_n is presented as permuting the corners of a regular n-gon.

This is part of a general approach. Consider the following example as an illustration, where we use group theory to answer a concrete question: how many genuinely different tetrahedral dice are there?

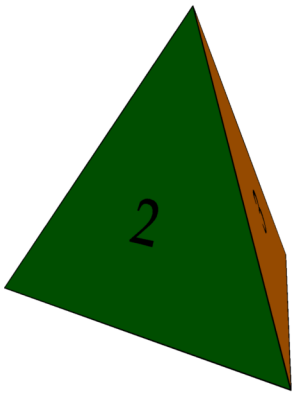
- We have four faces, and four numbers with which to label them. It follows that there are $4! = 24$ different ways of labelling the faces of a tetrahedron.
- However, dice roll! We will say that two *labellings* (i.e. dice) are identical if and only if one may be rotated into the other. Recall that the rotation group of a regular tetrahedron may be identified as the alternating group A_4. Therefore, two dice will be considered indistinguishable if they are related by an element of the group A_4.
- It seems reasonable, since $|A_4| = 12$, that the 24 possible dice are really split into two subsets of 12 dice each. Each subset consists of 12 dice which may be rotated into each other. There is something to prove here: since we want to argue that a set is *partitioned* into distinct subsets, we attempt to define an *equivalence relation.*
- Let $X = \{\text{all 24 tetrahedral dice}\}$. An element $g \in A_4$ will *act* on the set X by rotating all of the dice. If $x \in X$ is one die, we write $g \cdot x$ to denote the new, rotated, die. We define a relation $\sim$ on X by

  $$x \sim y \iff \exists g \in A_4 \text{ such that } y = g \cdot x$$

  It is easy to see that this is an equivalence relation on X, and that there are two equivalence classes, each containing 12 elements.
- It follows that there are really only *two* distinct 4-sided dice up to rotations.



A die $x \in X$



The resulting die $g \cdot x$, if $g = (123)$

Of course you don't need group theory to answer this question. You could argue that any die could be placed with the number 4 face down, and then rotated so that the number 3 is towards you. There

are then only 2 choices for labelling the other two faces: from left to right 1, 2 or 2, 1. But this is an *easy* problem. What if you had a cubic die? Or a 20-sided, icosahedral die? The beauty of the group theory approach is that it is *generalizable.* With such a goal in mind, here is the central definition.

Definition 9.1. Let X be a set and G a group. A map $\cdot : G \times X \to X$ is a (left) *action* of G on X if,

1. $\forall x \in X, \quad e \cdot x = x, \quad$ and,
2. $\forall x \in X,\ \forall g, h \in G, \quad g \cdot (h \cdot x) = (gh) \cdot x.$

Otherwise said, the map $G \to S_X : g \mapsto g\cdot$ is a homomorphism.

There is an analogous definition of a *right action*: in this course, all our actions will be left.

Examples

1. Any group G acts on itself by left multiplication. This is Cayley's Theorem.
2. As mentioned earlier, the symmetric S_n group acts on $X = \{1, 2, \ldots, n\}$.
3. Matrix groups act on vector spaces by matrix multiplication. For example

$$\cdot : \mathrm{GL}_2(\mathbb{R}) \times \mathbb{R}^2 \to \mathbb{R}^2 : (A, \mathbf{v}) \mapsto A\mathbf{v}$$

4. A group can act on many different sets. Here are three actions of the orthogonal group $\mathrm{O}_2(\mathbb{R})$.
   (a) $\mathrm{O}_2(\mathbb{R})$ acts on the set $X = \{1, -1\}$ via $A \cdot x := \det(A)x$.
   (b) $\mathrm{O}_2(\mathbb{R})$ acts on the set $X = \mathbb{R}^3$ via $A \cdot \mathbf{v} := A(v_1\mathbf{i} + v_2\mathbf{j}) + v_3\mathbf{k}$.
   (c) $\mathrm{O}_2(\mathbb{R})$ acts on the unit circle $X = S^1 \subseteq \mathbb{R}^2$ via matrix multiplication $A \cdot \mathbf{v} := A\mathbf{v}$.

The first two actions of $\mathrm{O}_2(\mathbb{R})$ should make you feel somewhat uncomfortable. In the first case, many matrices $A \in \mathrm{O}_2(\mathbb{R})$ act in exactly the same way. In essence, the set X is very small relative to the group: using the action as a description of the group means that we *lose information.*
In the second case, it feels like the set X is too large. The group acts via rotations and reflections, but only those which fix the z-axis. The action of $\mathrm{O}_2(\mathbb{R})$ doesn't do anything interesting to vertical vectors. This third action of $\mathrm{O}_2(\mathbb{R})$ on the circle feels nicely balanced: the set X is large enough so that the action fully describes the group, without being inefficiently large. These notions can be formalized.

Definition 9.2. Let $G \times X \to X$ be an action.

1. Let $g \in G$. The *fixed set* of g is the set

$$\mathrm{Fix}(g) = \{x \in X : g \cdot x = x\} \qquad \text{(also written } X_g\text{)}$$

2. Let $x \in X$. The *isotropy subgroup* or *stabilizer* of x is the set

$$\mathrm{Stab}(x) = \{g \in G : g \cdot x = x\} \qquad \text{(also written } G_x\text{)}$$

3. We say that the action is *faithful* if the only element of g which fixes everything is the identity. Equivalently

- $\text{Fix}(g) = X \iff g = e$.
- $\bigcap_{x \in X} \text{Stab}(x) = \{e\}$.

4. The action is *transitive* if one may use the action to transform any element of X to any other: that is

$$\forall x, y \in X,\ \exists g \in G \quad \text{such that} \quad y = g \cdot x.$$

Returning to our examples:

1. The left action of a group on itself is both transitive and faithful.
2. The action of S_n on $\{1, 2, \ldots, n\}$ is both faithful and transitive. For example, for any $a, b \in X$, the 2-cycle $(a\, b)$ maps $a \mapsto b$.
3. The action of matrix multiplication is faithful but not transitive: the zero vector cannot be transformed into any other vector. If we restricted the action of $\text{GL}_2(\mathbb{R})$ to the non-zero vectors $X = \mathbb{R}^2 \setminus \{\mathbf{0}\}$, then the action is both faithful and transitive. To see this, let V, W be matrices whose first columns are non-zero vectors $\mathbf{v}, \mathbf{w}$ respectively. Provided that the second column of each matrix is non-parallel to the first, these are invertible. Since $V\mathbf{i} = \mathbf{v}$ and $W\mathbf{i} = \mathbf{w}$, it is immediate that WV^{-1} is an invertible matrix whose action maps $\mathbf{v} \mapsto \mathbf{w}$.
4. (a) The action $A \cdot x = \det(A)x$ is transitive, but not faithful: indeed if A is any orthgonal matrix with determinant 1, then $\text{Fix}(A) = X$.
   (b) The action of $\text{O}_2(\mathbb{R})$ on $\mathbb{R}^3$ is faithful but not transitive. It is impossible to transform, say, the zero vector into anything else.
   (c) The action of $\text{O}_2(\mathbb{R})$ is both faithful and transitive.

Lemma 9.3. *As claimed in the definition,* $\text{Stab}(x)$ *is a subgroup of* G *for each* $x \in X$.

Proof. $\text{Stab}(x)$ is certainly a subset of G, so we must show that it is closed under multiplication and inverses. Let $g, h \in \text{Stab}(x)$, then

$$(gh) \cdot x = g \cdot (h \cdot x) = g \cdot x = x \implies gh \in \text{Stab}(x)$$

Moreover

$$\begin{aligned} g \cdot x = x &\implies g^{-1} \cdot (g \cdot x) = g^{-1} \cdot x \implies (g^{-1}g) \cdot x = g^{-1} \cdot x \\ &\implies e \cdot x = g^{-1} \cdot x \implies x = g^{-1} \cdot x. \end{aligned}$$

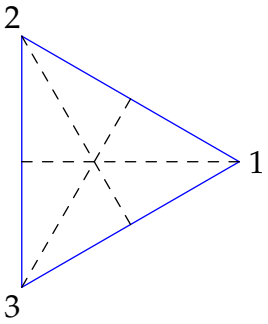
Hence $g^{-1} \in \text{Stab}(x)$.

■

Example The dihedral group D_3 acts on the set of corners of an equilateral triangle. Similarly D_4 acts on the set of corners of a square. We calculate the stabilizers of each corner under these actions. See earlier sections for the descriptions of each element.

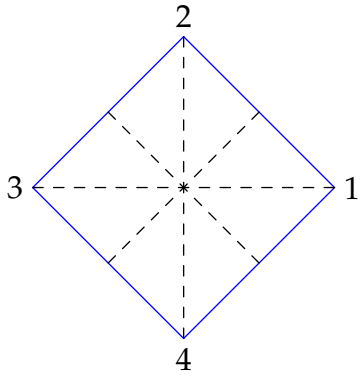
Given that the rotations ρ_1, ρ_2 move all the corners of the triangle, and that each reflection μ_i reflects across the altitude through the corner i, it is clear that the isotropy subgroup of the corner 1 is

$$\text{Stab}(1) = \{\rho_0, \mu_1\}.$$



Similarly $\text{Stab}(2) = \{\rho_0, \mu_2\}$ and $\text{Stab}(3) = \{\rho_0, \mu_3\}$.
D_3 also acts on the set of edges of the triangle $X = \{\{1,2\},\{1,3\},\{2,3\}\}$. Clearly

$$\text{Stab}(\{1,2\}) = \{\rho_0, \mu_3\}, \quad \text{etc.}$$



The rotations $\rho_1, \rho_2, \rho_3 \in D_4$ move all the corners of the square, the reflections μ_i reflect across the midpoints of edges and δ_i across diagonals. The stabilizers come in pairs:

$$\text{Stab}(1) = \text{Stab}(3) = \{\rho_0, \delta_1\}, \qquad \text{Stab}(2) = \text{Stab}(4) = \{\rho_0, \delta_2\}.$$

Acting on the set of edges of the square, we instead obtain

$$\text{Stab}(\{1,2\}) = \text{Stab}(\{3,4\}) = \{\rho_0, \mu_1\},$$
$$\text{Stab}(\{1,4\}) = \text{Stab}(\{2,3\}) = \{\rho_0, \mu_2\}.$$

Orbits

In order to address questions like the dice problem, we need to think about all the elements of a set X which can be transformed one to another under the action of G.

Definition 9.4. Let $G \times X \to X$ be an action. The *orbit* of $x \in X$ under G is the set

$$Gx = \{g \cdot x : g \in G\} \subseteq X$$

Theorem 9.5. *The orbits of an action partition X.*

Proof. Define $x \sim y \iff \exists g \in G$ such that $g \cdot x = y$ (i.e. x, y are in the same orbit). We claim that $\sim$ is an equivalence relation.

Reflexivity $x = e \cdot x \implies x \sim x$.

Symmetry $g \cdot x = y \implies x = g^{-1} \cdot y$, thus $x \sim y \implies y \sim x$.

Transitivity Let $y = g \cdot x$ and $z = h \cdot y$, then $z = (hg) \cdot x$, thus $x \sim y$ and $y \sim z$ together give $x \sim z$.

■

Observe that a transitive[40] action has only one orbit.

If X is the set $\{1, 2, \ldots n\}$ acted on by a cyclic group $G = \langle \sigma \rangle < S_n$, then the definition of orbits coincides with that given earlier in the course.

[40] Unhelpfully, we now have two distinct meanings of *transitive*; one for equivalence relations and one for actions.

Theorem 9.6. *The cardinality of the orbit containing $x \in X$ under the action of G is the index of the isotropy subgroup* $\mathrm{Stab}(x)$*:*

$$|Gx| = \big(G : \mathrm{Stab}(x)\big)$$

Proof. Observe that

$$g \cdot x = h \cdot x \iff h^{-1}g \cdot x = x \iff h^{-1}g \in \mathrm{Stab}(x) \iff g\,\mathrm{Stab}(x) = h\,\mathrm{Stab}(x)$$

Thus there are as many distinct elements of the set Gx as there are left cosets of $\mathrm{Stab}(x)$ in G. ∎

Burnside's formula

To solve combinatorial problems such as our dice problem, we need to be able to count the *number* of orbits of an action. At least when thinking about *finite* actions, this turns out to be possible in two different ways.

Theorem 9.7 (Burnside's formula)**.** *Let G be a finite group acting on a finite set X. Then the number of orbits in X under G satisfies*

$$\textit{number of orbits} = \frac{1}{|G|}\sum_{x\in X}|\mathrm{Stab}(x)| = \frac{1}{|G|}\sum_{g\in G}|\mathrm{Fix}(g)|\,.$$

Proof. G and X are finite, whence Theorem 9.6 tells us that the cardinality of the orbit of x is

$$|Gx| = \big(G : \mathrm{Stab}(x)\big) = \frac{|G|}{|\mathrm{Stab}(x)|}.$$

It follows that

$$\frac{1}{|G|}\sum_{x\in X}|\mathrm{Stab}(x)| = \sum_{x\in X}\frac{1}{|Gx|}. \qquad (*)$$

Now consider a fixed orbit Gy. Clearly $|Gx| = |Gy|$ for each $x \in Gy$, whence

$$\sum_{x\in Gy}\frac{1}{|Gx|} = \frac{|Gy|}{|Gy|} = 1.$$

The sum $(*)$ counts 1 for each distinct orbit in X and therefore returns the number of orbits.
For the second part of the formula, we compute the cardinality of the set

$$S = \{(g,x) \in G \times X : g \cdot x = x\}.$$

in two different ways.

- Suppose that $x \in X$ is constant. There are $|\mathrm{Stab}(x)|$ elements of G which satisfy $g \cdot x = x$. It follows that $|S| = \sum_{x\in X}\mathrm{Stab}(x)$.
- Now suppose that $g \in G$ is constant. There are $|\mathrm{Fix}(g)|$ elements of X which satisfy $g \cdot x = x$. It follows that $|S| = \sum_{g\in G}\mathrm{Fix}(g)$.

We conclude that $\sum_{x\in X}|\mathrm{Stab}(x)| = \sum_{g\in G}|\mathrm{Fix}(g)|$ and the proof is complete. ∎

Examples

1. Consider the set $X = \{1,2,3,4,5,6,7\}$ under the action of the cyclic group $G = \langle (14)(273) \rangle < S_7$. Since the orbits of a product of disjoint cycles are precisely the cycles, it is clear that wa have four orbits: $\{1,4\}, \{2,3,7\}, \{5\}, \{6\}$. We check Burnside's formula by computing the stabilizers and fixed sets. If $\sigma := (14)(273)$, then $|G| = 6$. Indeed

$$\sigma^2 = (237), \quad \sigma^3 = (14), \quad \sigma^4 = (273), \quad \sigma^5 = (14)(237), \quad \sigma^6 = e.$$

The stabilizers and fixed sets are summarized in the following tables

$x \in X$	$\mathrm{Stab}(x)$
1	$\{e, \sigma^2, \sigma^4\}$
2	$\{e, \sigma^3\}$
3	$\{e, \sigma^3\}$
4	$\{e, \sigma^2, \sigma^4\}$
5	$G = \{e, \sigma, \sigma^2, \sigma^3, \sigma^4, \sigma^5\}$
6	G
7	$\{e, \sigma^3\}$

$g \in G$	$\mathrm{Fix}(g)$
e	$X = \{1,2,3,4,5,6,7\}$
σ	$\{5,6\}$
σ^2	$\{1,4,5,6\}$
σ^3	$\{2,3,5,6,7\}$
σ^4	$\{1,4,5,6\}$
σ^5	$\{5,6\}$

In either case Burnside just sums the number of elements in all of the subsets in the right column:

$$\begin{aligned} 4 = \text{number of orbits} &= \frac{1}{|G|} \sum_{x \in X} |\mathrm{Stab}(x)| = \frac{1}{6}(3+2+2+3+6+6+2) \\ &= \frac{1}{|G|} \sum_{g \in G} |\mathrm{Fix}(g)| = \frac{1}{6}(7+2+4+5+4+2) \end{aligned}$$

2. The edges of an equilateral triangle are to be painted using any choice of colors from the rainbow set {red, orange, yellow, green, blue, indigo, violet}. How many distinct triangles are possible?

   This is a little tricky, since we have a lot of choice. We assume that D_3 acts on $X = \{\text{painted triangles}\}$. Clearly $|X| = 7^3 = 343$. It would be very time consuming to compute the stabilizer of each; fixed sets are easier.

   - $\mathrm{Fix}(e) = X$ is clear.
   - For each of the two rotations ρ_1, ρ_2, the set $\mathrm{Fix}(\rho_i)$ has 7 elements. If a color-scheme is to be fixed by ρ_1, then all pairs of adjacent edges must be the same color. The only color-schemes fixed by ρ_1 are therefore those where all sides have the same color.
   - For each reflection μ_i, the set $\mathrm{Fix}(\mu_i)$ has $7^2 = 49$ elements. This is since μ_i swaps two edges, which must be the same color in order to be fixed. We have 7 choices for the color of the pair of switched edges, and an independent choice of 7 colors for the other edge.

   It follows that the number of distinct color-schemes is

$$\frac{1}{|D_3|} \sum_{g \in D_3} |\mathrm{Fix}(g)| = \frac{1}{6}(7^3 + 7 + 7 + 49 + 49 + 49) = \frac{7}{6}(49 + 1 + 1 + 7 + 7 + 7) = 84$$

This question is tricky because we are allowing multiple sides to have the same color. A simpler question would restrict to the situation where all sides had to be different. In this case D_3 acts on a set of color schemes with cardinality $|X| = 7 \cdot 6 \cdot 5 = 210$. It is clear that only the identity has a non-empty fixed set, whence the number of orbits is $\frac{210}{6} = 35$.

3. A cuboid measuring $2 \times 2 \times 3$ cm is to be made into an extremely unfair die by painting the numbers 1 to 6, one on each face. If we assume that the orientation of the numbers on each face is irrelevant, how many distinct dice can we make?
   To apply Burnside we need a set X and group G acting on X such that the orbits of the action consist of indistinct dice. Thus let X be the set of all possible labelings of the faces and G be the group of rotations of the prism. There are clearly 6! possible ways to label the faces. The group of rotations is a little trickier. Consider one of the square faces. We can leave this face where it is by performing the identity of one of three rotations. Alternatively, we can swap this face with the other square face before rotating. The result is a rotation group[41] of order 8. learly the cyclic group of order 4, generated by a 90° rotation. Every face of a labelled cuboid has a different number, thus any element of the rotation group changes every labelling, with the exception of the identity which changes nothing. Therefore

$$\mathrm{Fix}(g) = \begin{cases} X, & \text{if } g = e, \\ \emptyset, & \text{if } g \neq e. \end{cases}$$

   It follows that the number of distinct dice is

$$\frac{1}{|G|} \sum_{g \in G} |\mathrm{Fix}(g)| = \frac{6!}{8} = 90.$$

   This question can also be answered very simply using combinatorics. There are $\binom{6}{2}$ choices for the pair of numbers to be painted on the square ends. Once these are chosen, there are 6 configurations of the remaining 4 numbers on the longer sides (up to rotation of the end squares). We therefore obtain $\binom{6}{2} \cdot 6 = 90$ distinct dice.

4. Our motivating tetrahedron example be extended to the point where combinatorial arguments are next to useless. How many dice there are for a given regular polyhedron?

   Let X be the set of labelings of the f faces of a polyhedron by the numbers $1, \ldots, f$. Clearly $|X| = f!$ Let G be the group of rotations of the polyhedron. While we many not be able to calculate this group directly, this doesn't matter as all we need is the order of the group. Suppose the polyhedron has f faces which are all the same shape. We may then find f elements $g_1 \ldots, g_f$ which each map a fixed starting face to one of the f distinct faces. Once there, we can apply the rotation group of each face. Thus $|G| = f\,|H|$ where H is the rotation group of the face. Since the polyhedron is regular, we have $H = C_n$ where n is the number of edges on each face. Moreover every element of the rotation group except for the identity moves every labeling (since it moves at least one numbered face). Hence $\mathrm{Fix}(e) = X$ and $\mathrm{Fix}(g) = \emptyset$ for $g \neq e$. The number of distinct dice for a regular polyhedron is therefore

$$\frac{f!}{fn} = \frac{(f-1)!}{n}$$

[41] We don't need to know G in terms of the standard lists, just its order. However, it isn't hard to see that the rotation group is isomorphic to D_4.

To summarize:

Polyhedron	f	n	# distinct dice
Tetrahedron	4	3	2
Cube	6	4	30
Octahedron	8	3	1,680
Dodecahedron	12	5	7,983,360
Icosahedron	20	3	40,548,366,802,944,000

The same game can be played with non-regular polyhedra. For example suppose you wanted to make a die out of a football[42] constructed from 20 regular hexagons and 12 regular pentagons, with a different number on each face.

Notice that five hexagons surround each pentagon. Here the rotation group has order $12 \cdot 5 = 60$ (move a pentagon to any other pentagon then rotate—this is isomorphic to the dodecahedron/icosahedron groups). It is therefore possible to construct $\frac{32!}{60} = 4.39 \times 10^{33}$ distinct dice!

Say instead that you had 20 different colored hexagonal patches and 12 different colored pentagonal patches. This time the set of possible footballs X has cardinality 20!12!, so that the number of distinct footballs is $\frac{20!12!}{60} = 1.94 \times 10^{25}$.

[42] Or a soccer ball for those who've never questioned why American football isn't played with the feet…This is also the shape of the famous Bucky-ball C_{60}-molecule with a carbon atom at each corner.