WIKIPEDIA

# Quotient group

A **quotient group** or **factor group** is a mathematical group obtained by aggregating similar elements of a larger group using an equivalence relation that preserves the group structure. For example, the cyclic group of addition modulo *n* can be obtained from the integers by identifying elements that differ by a multiple of *n* and defining a group structure that operates on each such class (known as a congruence class) as a single entity. It is part of the mathematical field known as group theory.

In a quotient of a group, the equivalence class of the identity element is always a normal subgroup of the original group, and the other equivalence classes are precisely the cosets of that normal subgroup. The resulting quotient is written *G* / *N*, where *G* is the original group and *N* is the normal subgroup. (This is pronounced "*G* mod *N*", where "mod" is short for modulo.)

Much of the importance of quotient groups is derived from their relation to homomorphisms. The first isomorphism theorem states that the image of any group *G* under a homomorphism is always isomorphic to a quotient of *G*. Specifically, the image of *G* under a homomorphism $\varphi$: $G \to H$ is isomorphic to *G* / ker($\varphi$) where ker($\varphi$) denotes the kernel of $\varphi$.

The dual notion of a quotient group is a subgroup, these being the two primary ways of forming a smaller group from a larger one. Any normal subgroup has a corresponding quotient group, formed from the larger group by eliminating the distinction between elements of the subgroup. In category theory, quotient groups are examples of quotient objects, which are dual to subobjects. For other examples of quotient objects, see quotient ring, quotient space (linear algebra), quotient space (topology), and quotient set.

## Contents

**Definition and illustration**
- Definition
- Example: Addition modulo 6

**Motivation for the name "quotient"**

**Examples**
- Even and odd integers
- Remainders of integer division
- Complex integer roots of 1
- Sums of integers and real numbers
- Matrices of real numbers
- Integer modular arithmetic
- Integer multiplication

**Properties**

**Quotients of Lie groups**

**See also**

**Notes**

**References**

## Definition and illustration

Given a group *G* and a subgroup *H*, and an element *a* in *G*, one can consider the corresponding left coset: $aH := \{\ ah : h \text{ in } H\ \}$. Cosets are a natural class of subsets of a group; for example consider the abelian group *G* of integers, with operation defined by the usual addition, and the subgroup *H* of even integers. Then there are exactly two cosets: $0 + H$, which are the even integers, and $1 + H$, which are the odd integers (here we are using additive notation for the binary operation instead of multiplicative notation).

For a general subgroup $H$, it is desirable to define a compatible group operation on the set of all possible cosets, { $aH$ : $a$ in $G$ }. This is possible exactly when $H$ is a normal subgroup, as we will see below. A subgroup $N$ of a group $G$ is normal if and only if the coset equality $aN = Na$ holds for all $a$ in $G$. A normal subgroup of $G$ is denoted $N \lhd G$.

### Definition

Let $N$ be a normal subgroup of a group $G$. We define the set $G/N$ to be the set of all left cosets of $N$ in $G$, i.e., $G/N = \{ aN : a \in G \}$. Define an operation on $G/N$ as follows. For each $aN$ and $bN$ in $G/N$, the product of $aN$ and $bN$ is $(aN)(bN)$. This defines an operation on $G/N$ if we impose $(aN)(bN) = (ab)N$, because $(ab)N$ does not depend on the choice of the representatives $a$ and $b$: if $xN = aN$ and $yN = bN$ for some $x$, $y$ in $G$, then

$$(ab)N = a(bN) = a(yN) = a(Ny) = (aN)y = (xN)y = x(Ny) = x(yN) = (xy)N.$$

Here we have used in an important way that $N$ is a normal subgroup. One checks that this operation on $G/N$ is associative, has identity element $N$, and the inverse of an element $aN$ of $G/N$ is $a^{-1}N$. Therefore, the set $G/N$ together with the operation defined above forms a group; this is known as the **quotient group** of $G$ by $N$.

Because of the normality of $N$, the left cosets and right cosets of $N$ in $G$ are equal, and so we could have instead defined $G/N$ to be the set of right cosets of $N$ in $G$.

### Example: Addition modulo 6

For example, consider the group with addition modulo 6: $G = \{0, 1, 2, 3, 4, 5\}$. Consider the subgroup $N = \{0, 3\}$, which is normal because $G$ is abelian. Then the set of (left) cosets is of size three:

$$G/N = \{ a+N : a \in G \} = \{ \{0, 3\}, \{1, 4\}, \{2, 5\} \} = \{ 0+N , 1+N, 2+N \}.$$

The binary operation defined above makes this set into a group, known as the quotient group, which in this case is isomorphic to the cyclic group of order 3.

# Motivation for the name "quotient"

The reason $G/N$ is called a quotient group comes from division of integers. When dividing 12 by 3 one obtains the answer 4 because one can regroup 12 objects into 4 subcollections of 3 objects. The quotient group is the same idea, although we end up with a group for a final answer instead of a number because groups have more structure than an arbitrary collection of objects.

To elaborate, when looking at $G/N$ with $N$ a normal subgroup of $G$, the group structure is used to form a natural "regrouping". These are the cosets of $N$ in $G$. Because we started with a group and normal subgroup, the final quotient contains more information than just the number of cosets (which is what regular division yields), but instead has a group structure itself.

# Examples

### Even and odd integers

Consider the group of integers **Z** (under addition) and the subgroup 2**Z** consisting of all even integers. This is a normal subgroup, because **Z** is abelian. There are only two cosets: the set of even integers and the set of odd integers; therefore, the quotient group **Z**/2**Z** is the cyclic group with two elements. This quotient group is isomorphic with the set { 0, 1 } with addition modulo 2; informally, it is sometimes said that **Z**/2**Z** *equals* the set { 0, 1 } with addition modulo 2.

**Example further explained...**

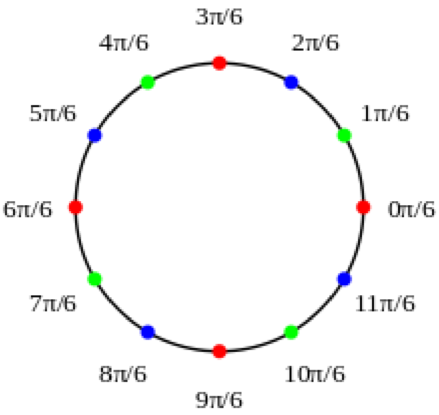
Let $\gamma(m)=$ remainders of $m\in\mathbb{Z}$ when dividing by $2$.
Then $\gamma(m)=0$ when $m$ is even and $\gamma(m)=1$ when $m$ is odd.
By definition of $\gamma$, the kernel of $\gamma$,
$\ker(\gamma)=\{m\in\mathbb{Z}:\gamma(m)=0\}$, is the set of all even integers.
Let $H=\ker(\gamma)$.
Then $H$ is a subgroup, because the identity in $\mathbb{Z}$, which is $0$, is in $H$,
the sum of two even integers is even and hence if $m$ and $n$ are in $H$, $m+n$ is in $H$ (closure)
and if $m$ is even, $-m$ is also even and so $H$ contains its inverses.
Define $\mu:\mathbb{Z}/\mathrm{H}\rightarrow\mathbb{Z}_2$ as $\mu(aH)=\gamma(a)$ for $a\in\mathbb{Z}$
and $\mathbb{Z}/\mathrm{H}$ is the quotient group of left cosets; $\mathbb{Z}/\mathrm{H}=\{H,1+H\}$.
By the way we have defined $\mu$, $\mu(aH)$ is $1$ if $a$ is odd and $0$ if $a$ is even.
Thus, $\mu$ is an isomorphism from $\mathbb{Z}/\mathrm{H}$ to $\mathbb{Z}_2$.

## Remainders of integer division

A slight generalization of the last example. Once again consider the group of integers **Z** under addition. Let *n* be any positive integer. We will consider the subgroup *n***Z** of **Z** consisting of all multiples of *n*. Once again *n***Z** is normal in **Z** because **Z** is abelian. The cosets are the collection {*n***Z**, 1+*n***Z**, ..., (*n*−2)+*n***Z**, (*n*−1)+*n***Z**}. An integer *k* belongs to the coset *r*+*n***Z**, where *r* is the remainder when dividing *k* by *n*. The quotient **Z**/*n***Z** can be thought of as the group of "remainders" modulo *n*. This is a cyclic group of order *n*.

## Complex integer roots of 1

The twelfth roots of unity, which are points on the complex unit circle, form a multiplicative abelian group *G*, shown on the picture on the right as colored balls with the number at each point giving its complex argument. Consider its subgroup *N* made of the fourth roots of unity shown as red balls. This normal subgroup splits the group into three cosets, shown in red, green and blue. One can check that the cosets form a group of three elements (the product of a red element with a blue element is blue, the inverse of a blue element is green, etc.). Thus, the quotient group *G*/*N* is the group of three colors, which turns out to be the cyclic group with three elements.



The cosets of the fourthroots of unity *N* in the twelfth roots of unity *G*.

## Sums of integers and real numbers

Consider the group of real numbers **R** under addition, and the subgroup **Z** of integers. The cosets of **Z** in **R** are all sets of the form *a*+**Z**, with 0 ≤ *a* < 1 a real number. Adding such cosets is done by adding the corresponding real numbers, and subtracting 1 if the result is greater than or equal to 1. The quotient group **R**/**Z** is isomorphic to the circle group $S^1$, the group of complex numbers of absolute value 1 under multiplication, or correspondingly, the group of rotations in 2D about the origin, i.e., the special orthogonal group SO(2). An isomorphism is given by *f*(*a*+**Z**) = exp(2*πia*) (see Euler's identity).

## Matrices of real numbers

If *G* is the group of invertible 3 × 3 real matrices, and *N* is the subgroup of 3 × 3 real matrices with determinant 1, then *N* is normal in *G* (since it is the kernel of the determinant homomorphism). The cosets of *N* are the sets of matrices with a given determinant, and hence *G*/*N* is isomorphic to the multiplicative group of non-zero real numbers. The group *N* is known as the special linear group SL(3).

## Integer modular arithmetic

Consider the abelian group $\mathbf{Z}_4 = \mathbf{Z}/4\mathbf{Z}$ (that is, the set { 0, 1, 2, 3 } with addition modulo 4), and its subgroup { 0, 2 }. The quotient group $\mathbf{Z}_4$/{ 0, 2 } is { { 0, 2 }, { 1, 3 } }. This is a group with identity element { 0, 2 }, and group operations such as { 0, 2 } + { 1, 3 } = { 1, 3 }. Both the subgroup { 0, 2 } and the quotient group { { 0, 2 }, { 1, 3 } } are isomorphic with $\mathbf{Z}_2$.

### Integer multiplication

Consider the multiplicative group $G = \mathbf{Z}^*_{n^2}$. The set $N$ of $n$th residues is a multiplicative subgroup isomorphic to $\mathbf{Z}^*_n$. Then $N$ is normal in $G$ and the factor group $G/N$ has the cosets $N$, $(1+n)N$, $(1+n)^2$N, ..., $(1+n)^{n-1}$N. The Paillier cryptosystem is based on the conjecture that it is difficult to determine the coset of a random element of $G$ without knowing the factorization of $n$.

# Properties

The quotient group $G/G$ is isomorphic to the trivial group (the group with one element), and $G/\{e\}$ is isomorphic to $G$.

The order of $G/N$, by definition the number of elements, is equal to $|G : N|$, the index of $N$ in $G$. If $G$ is finite, the index is also equal to the order of $G$ divided by the order of $N$. Note that $G/N$ may be finite, although both $G$ and $N$ are infinite (e.g. $\mathbf{Z}/2\mathbf{Z}$).

There is a "natural" surjective group homomorphism $\pi : G \to G/N$, sending each element $g$ of $G$ to the coset of $N$ to which $g$ belongs, that is: $\pi(g) = gN$. The mapping $\pi$ is sometimes called the *canonical projection of G onto G/N*. Its kernel is $N$.

There is a bijective correspondence between the subgroups of $G$ that contain $N$ and the subgroups of $G/N$; if $H$ is a subgroup of $G$ containing $N$, then the corresponding subgroup of $G/N$ is $\pi(H)$. This correspondence holds for normal subgroups of $G$ and $G/N$ as well, and is formalized in the lattice theorem.

Several important properties of quotient groups are recorded in the fundamental theorem on homomorphisms and the isomorphism theorems.

If $G$ is abelian, nilpotent, solvable, cyclic or finitely generated, then so is $G/N$.

If $H$ is a subgroup in a finite group $G$, and the order of $H$ is one half of the order of $G$, then $H$ is guaranteed to be a normal subgroup, so $G/H$ exists and is isomorphic to $C_2$. This result can also be stated as "any subgroup of index 2 is normal", and in this form it applies also to infinite groups. Furthermore, if $p$ is the smallest prime number dividing the order of a finite group, $G$, then if $G/H$ has order $p$, $H$ must be a normal subgroup of $G$.[1]

Given $G$ and a normal subgroup $N$, then $G$ is a group extension of $G/N$ by $N$. One could ask whether this extension is trivial or split; in other words, one could ask whether $G$ is a direct product or semidirect product of $N$ and $G/N$. This is a special case of the extension problem. An example where the extension is not split is as follows: Let $G = \mathbf{Z}_4 = \{0, 1, 2, 3\}$, and $N = \{0, 2\}$, which is isomorphic to $\mathbf{Z}_2$. Then $G/N$ is also isomorphic to $\mathbf{Z}_2$. But $\mathbf{Z}_2$ has only the trivial automorphism, so the only semi-direct product of $N$ and $G/N$ is the direct product. Since $\mathbf{Z}_4$ is different from $\mathbf{Z}_2 \times \mathbf{Z}_2$, we conclude that $G$ is not a semi-direct product of $N$ and $G/N$.

# Quotients of Lie groups

If $G$ is a Lie group and $N$ is a normal Lie subgroup of $G$, the quotient $G / N$ is also a Lie group. In this case, the original group $G$ has the structure of a fiber bundle (specifically, a principal $N$-bundle), with base space $G / N$ and fiber $N$.

For a non-normal Lie subgroup $N$, the space $G / N$ of left cosets is not a group, but simply a differentiable manifold on which $G$ acts. The result is known as a homogeneous space.

# See also

- Group extension
- Lattice theorem
- Quotient category

- Short exact sequence

## Notes

1. Dummit & Foote (2003, p. 120)

## References

- Dummit, David S.; Foote, Richard M. (2003), *Abstract Algebra* (3rd ed.), New York: Wiley, ISBN 978-0-471-43334-7
- Herstein, I. N. (1975), *Topics in Algebra* (2nd ed.), New York: Wiley, ISBN 0-471-02371-X