



planetmath.org

Math for the people, by the people.

examples of groups

Canonical name	ExamplesOfGroups
Date of creation	2013-03-22 12:49:19
Last modified on	2013-03-22 12:49:19
Owner	AxelBoldt (56)
Last modified by	AxelBoldt (56)
Numerical id	34
Author	AxelBoldt (56)
Entry type	Example
Classification	msc 20-00
Classification	msc 20A05
Related topic	ExamplesOfFiniteSimpleGroups
Related topic	SpinGroup
Related topic	ExamplesOfAlgebraicKTheoryGroups
Related topic	QuantumGroups
Related topic	GroupsOfSmallOrder
Related topic	TriangleGroups

<http://planetmath.org/Group> Groups are ubiquitous throughout mathematics. Many “naturally occurring” groups are either groups of numbers (typically Abelian) or groups of symmetries (typically non-Abelian).

Groups of numbers

- The most important group is the group of integers \mathbb{Z} with addition as operation and zero as identity element.
- The integers modulo n , often denoted by \mathbb{Z}_n , form a group under addition. Like \mathbb{Z} itself, this is a cyclic group; any cyclic group is isomorphic to one of these.
- The rational (or real, or complex) numbers form a group under addition.
- The positive rationals form a group under multiplication with identity element 1, and so do the non-zero rationals. The same is true for the reals and real algebraic numbers.
- The non-zero complex numbers form a group under multiplication. So do the non-zero quaternions. The latter is our first example of a non-Abelian group.
- More generally, any (skew) field gives rise to two groups: the additive group of all field elements with 0 as identity element, and the multiplicative group of all non-zero field elements with 1 as identity element.
- The complex numbers of absolute value 1 form a group under multiplication, best thought of as the unit circle. The quaternions of absolute value 1 form a group under multiplication, best thought of as the three-dimensional unit sphere S^3 . The two-dimensional sphere S^2 however is not a group in any natural way.
- The positive integers less than n which are coprime to n form a group if the operation is defined as multiplication modulo n . This is an Abelian group whose order is given by the Euler phi-function $\phi(n)$.
- The units of the number ring $\mathbb{Z}[\sqrt{3}]$ form the multiplicative group consisting of all integer powers of $2 + \sqrt{3}$ and their negatives (see units of quadratic fields).

- Generalizing the last two examples, if R is a ring with multiplicative identity 1, then the <http://planetmath.org/GroupOfUnits> units of R (the elements invertible with respect to multiplication) form a group with respect to ring multiplication and with identity element 1. See examples of rings.

Most groups of numbers carry natural topologies turning them into topological groups.

Symmetry groups

- The symmetric group of degree n , denoted by S_n , consists of all permutations of n items and has $n!$ elements. Every finite group is isomorphic to a subgroup of some S_n (Cayley's theorem).
- An important subgroup of the symmetric group of degree n is the alternating group, denoted A_n . This consists of all *even* permutations on n items. A permutation is said to be even if it can be written as the product of an even number of transpositions. The alternating group is normal in S_n , of index 2, and it is an interesting fact that A_n is simple for $n \geq 5$. See the proof on the simplicity of the alternating groups. See also examples of finite simple groups.
- If any geometrical object is given, one can consider its symmetry group consisting of all rotations and reflections which leave the object unchanged. For example, the symmetry group of a cone is isomorphic to S^1 ; the symmetry group of a square has eight elements and is isomorphic to the dihedral group D_4 .
- The set of all automorphisms of a given group (or field, or graph, or topological space, or object in any category) forms a group with operation given by the composition of homomorphisms. This is the automorphism group of the given object and captures its “internal symmetries”.
- In Galois theory, the symmetry groups of field extensions (or equivalently: the symmetry groups of solutions to polynomial equations) are the central object of study; they are called Galois groups. One version of the inverse Galois problem asks whether every finite group can arise as the symmetry group of some algebraic extension of the rational numbers. The answer is unknown.

- Several matrix groups describe various aspects of the symmetry of n -space:
 - The general linear group $GL(n, \mathbb{R})$ of all real invertible $n \times n$ matrices (with matrix multiplication as operation) contains rotations, reflections, dilations, shear transformations, and their combinations.
 - The orthogonal group $O(n, \mathbb{R})$ of all real orthogonal $n \times n$ matrices contains the rotations and reflections of n -space.
 - The special orthogonal group $SO(n, \mathbb{R})$ of all real orthogonal $n \times n$ matrices with determinant 1 contains the rotations of n -space.

All these matrix groups are Lie groups: groups which are differentiable manifolds such that the group operations are smooth maps.

Other groups

- The trivial group consists only of its identity element.
- The Klein 4-group is a non-cyclic abelian group with four elements. For other small groups, see groups of small order.
- If X is a topological space and x is a point of X , we can define the fundamental group of X at x . It consists of (homotopy classes of) continuous paths starting and ending at x and describes the structure of the “holes” in X accessible from x . The fundamental group is generalized by the higher homotopy groups.
- Other groups studied in algebraic topology are the homology groups of a topological space. In a different way, they also provide information about the “holes” of the space.
- The free groups are important in algebraic topology. In a sense, they are the most general groups, having only those relations among their elements that are absolutely required by the group axioms. The free group on the set S has as members all the finite strings that can be formed from elements of S and their inverses; the operation comes from string concatenation.

- If A and B are two Abelian groups (or modules over the same ring), then the set $\text{Hom}(A, B)$ of all homomorphisms from A to B is an Abelian group. Note that the commutativity of B is crucial here: without it, one couldn't prove that the sum of two homomorphisms is again a homomorphism.
- Given any set X , the powerset $\mathcal{P}(X)$ of X becomes an abelian group if we use the symmetric difference as operation. In this group, any element is its own inverse, which makes it into a vector space over \mathbb{Z}_2 .
- If R is a ring with multiplicative identity, then the set of all invertible $n \times n$ matrices over R forms a group under matrix multiplication with the identity matrix as identity element; this group is denoted by $\text{GL}(n, R)$. It is the group of units of the ring of all $n \times n$ matrices over R . For a given n , the groups $\text{GL}(n, R)$ with commutative ring R can be viewed as the points on the general linear group scheme GL_n .
- If K is a number field, then multiplication of (equivalence classes of) non-zero ideals in the ring of algebraic integers \mathcal{O}_K gives rise to the ideal class group of K .
- The set of the equivalence classes of commensurability of the positive real numbers is an Abelian group with respect to the defined operation.
- The set of arithmetic functions that take a value other than 0 at 1 form an Abelian group under Dirichlet convolution. They include as a subgroup the set of multiplicative functions.
- Consider the curve $C = \{(x, y) \in K^2 \mid y^2 = x^3 - x\}$, where K is any field. Every straight line intersects this set in three points (counting a point twice if the line is tangent, and allowing for a point at infinity). If we require that those three points add up to zero for any straight line, then we have defined an abelian group structure on C . Groups like these are called abelian varieties.
- Let E be an elliptic curve defined over any field F . Then the set of F -rational points in the curve E , denoted by $E(F)$, can be given the structure of abelian group. If F is a number field, then $E(F)$ is a finitely generated abelian group. The curve C in the example above

is an elliptic curve defined over \mathbb{Q} , thus $C(\mathbb{Q})$ is a finitely generated abelian group.

- In the classification of all finite simple groups, several “sporadic” groups occur which don’t follow any discernable pattern. The largest of these is the monster group with about $8 \cdot 10^{53}$ elements.