ENTRY GROUP THEORY

[ENTRY GROUP THEORY] Authors: started Mark Lezama: October 2003 Literature: ”Algebra” by Michael Artin, Mathworld

Group theory

[Group theory] is studies algebraic objects called groups. The German mathematician Karl Friedrich Gauss (1777-1855) developed but did not publish some of the mathematics of group theory. The French mathematician Evariste Galois (1811-1832) is generally credited with being the first to develop the theory, which he did by developing new techniques to study the solubility of equations. Group theory is a powerful method for analyzing abstract and physical systems in which symmetry –the intrinsic property of an object to remain invariant under certain classes of transformations– is present because the mathematical study of symmetry is systematized and formalized in group theory. Consequently, group theory is an important tool in physics particularly in quantum mechanics.

group

A [group] is an object consisting of a set G and a law of composition (or binary operation) L on G satisfying:

- L is associative.
- L has an identity in G.
- Every element of G has an inverse.

The study of groups is known as group theory. If a group G has n elements where n is a positive integer, then G is a finite group with order n. If a group is not finite it is infinite. Examples:

- Z^+, the integers under addition;
- $R^+ = (R, +)$, the real numbers under addition;
- $R^\times = (R - \{0\}, \cdot)$, the real numbers without zero under multiplication;
- $GL_n(C)$, the $n \times n$ general linear group under matrix multiplication;
- S_n, the symmetric group on n objects under composition.

law of composition

A [law of composition] or, binary operation, on a set S is a function from $S \times S$ into S. That is, a law of composition on S prescribes a rule for combining pairs of elements in S to get an element in S. For convenience, functional notation is not used; that is, if a law of composition f sends (a, b) to c, one does not usually write $f(a, b) = c$. It is customary to instead use notation that resembles that used for multiplication or addition of real numbers, such as $ab = c$, $a \cdot b = c$, $a \circ b = c$, $a + b = c$, and so on.

An example of a law of composition is multiplication on the real numbers, R. If $m\colon R \times R \to R$ defines multiplication on R then $m(x, y) = x \cdot y$. For example $m(2, 5) = 2 \cdot 5 = 10$.

binary operation

A [binary operation], or law of composition, on a set S is a function from $S \times S$ into S. That is, a binary operation on S prescribes a rule for combining pairs of elements in S to get an element in S. For convenience, functional notation is not used; that is, if a binary operation f sends (a, b) to c, one does not usually write $f(a, b) = c$. It is customary to instead use notation that resembles that used for multiplication or addition of real numbers, such as $ab = c$, $a \cdot b = c$, $a \circ b = c$, $a + b = c$, and so on.
An example of a binary operation is multiplication on the real numbers, R. If $m\colon R \times R \to R$ defines multiplication on R then $m(x, y) = x \cdot y$. For example $m(2, 5) = 2 \cdot 5 = 10$.

associative

A law of composition on a set S is [associative] if for all $a, b, c \in S$, $(ab)c = a(bc)$. The informal intuition behind associativity (the property of being associative) is that if one has an expression in which there are many parentheses and the only operation performed in this expression is that defined by an associative law of composition, then one may ignore the parentheses. For example, if $\cdot$ is an associative law of composition on S and $a, b, c, d \in S$, then $((a \cdot (b \cdot c)) \cdot d = ((a \cdot b) \cdot c) \cdot d = (a \cdot b) \cdot (c \cdot d)$ and so on; thus one may write $a \cdot b \cdot c \cdot d$ without being ambiguous.
An example of an associative law of composition is addition on the integers, Z. That is, for all $a, b, c \in Z$, $(a + b) + c = a + (b + c)$.

identity

An [identity] for a law of composition on a set S is an element e such that, for all $a \in S$, $ea = a$ and $ae = a$. Note that a law of composition has at most one identity. The symbols e, 0 and 1 are commonly used to denote the identity element of a group. The number 0 is an identity for addition on the real numbers.

identity

Suppose a set S has a law of composition with identity 1. For every element $a \in S$, if there exists an element $b \in S$ such that $ab = 1$ and $ba = 1$ then b is the [inverse] of a. When using multiplicative notation for the law of composition, the inverse of a can be written as a^{-1}. As an example, the inverse of any integer n is $-n$ where the law of composition is addition and the identity is 0. As another example, the inverse of any nonzero real number x is $\frac{1}{x}$, where the law of composition is multiplication and the identity is 1.

general linear group

The $n \times n$ [general linear group] $GL_n(F)$ is the set of $n \times n$ matrices with entries in the field F and nonzero determinant, under the law of composition of matrix multiplication. Thus $GL_n(F)$ is the group of $n \times n$ invertible matrices with entries in F. If F is a finite field of field order q then sometimes the general linear group $GL_n(F)$ is denoted by $GL_n(q)$. The general linear group often appears with respect to the real numbers, R, or the complex numbers, C; that is, the general linear group often appears as $GL_n(R)$ or $GL_n(C)$.
The special linear group $SL_n(F)$ is the subgroup of $GL_n(F)$ whose elements have determinant equal to 1.

special linear group

The $n \times n$ [special linear group] $SL_n(F)$ is the set of $n \times n$ matrices with entries in the field F and determinant equal to 1, under the law of composition of matrix multiplication.
If F is a finite field of field order q then sometimes the special linear group $SL_n(F)$ is denoted by $SL_n(q)$.
$SL_n(F)$ is a subgroup of the general linear group $GL_n(F)$.

trivial

A group is [trivial] if it contains exactly one element. The one element in the group is the identity element. As all trivial groups are isomorphic, one usually refers to a trivial group as *the* trivial group. A group that is not trivial is nontrivial.

trivial

The group containing exactly one element (the identity) is unique up to isomorphism and is therefore called the [trivial group]. The trivial group is a normal subgroup of every group.

nontrivial

A group is [nontrivial] if it is not trivial.

abelian

A group is [abelian] if its law of composition is commutative. Examples of abelian groups include the following:

- $R^+ = (R, +)$, the real numbers under addition;
- $R^\times = (R - \{0\}, \cdot)$, the real numbers without zero under multiplication;
- any cyclic group.

Examples of nonabelian groups, i.e. groups that are not abelian:

- $GL_n(C)$, the general linear group;
- The symmetric group on n objects, where n is a positive integer greater than 2.

commutative

A law of composition on a set S is [commutative] if for all $a, b \in S$ $ab = ba$. An example of a commutative law of composition is addition on the real numbers: for example, $3.2 + 4 = 7.2 = 4 + 3.2$.

cancellation Law

The [cancellation Law] states that if a, b, and c are elements of a group and if $ab = ac$ then $b = c$. Similarly, if $ba = ca$ then $b = c$. The Cancellation Law follows from the fact that every element of a group has an inverse.

permutation

If S is a set, then a [permutation] of S is a bijective map from S into S. The intuition underlying the definition of a permutation is that a permutation determines a reordering of the elements in a list or the rearrangement of objects. For example, the permutation $\sigma : \{1, 2, 3\} \rightarrow \{1, 2, 3\}$ defined by $\sigma(1) = 2$, $\sigma(2) = 1$, and $\sigma(3) = 3$ can be thought to represent the reordering of the list 1,2,3 that results in the list 2,1,3. There is an important kind of permutation called a transposition. A transposition of a set S is a permutation $\sigma\colon S \rightarrow S$ satisfying the following: there exist $s_1, s_2 \in S$ such that

- $\sigma(s_1) = s_2$
- $\sigma(s_2) = s_1$
- and for all $s \in S$, if $s \neq s_1$ and $s \neq s_2$, then $\sigma(s) = s$.

Every permutation of a finite set can be written as the composition of a finite number of transpositions of that set. For example, the permutation $\sigma : \{1, 2, 3\} \rightarrow \{1, 2, 3\}$ defined by $\sigma(1) = 2$, $\sigma(2) = 3$, and $\sigma(3) = 1$ is equivalent to the composition of two transpositions. Define $\sigma_1 : \{1, 2, 3\} \rightarrow \{1, 2, 3\}$ by $\sigma_1(1) = 2$, $\sigma_1(2) = 1$, and $\sigma(3) = 3$, and define $\sigma_2 : \{1, 2, 3\} \rightarrow \{1, 2, 3\}$ by $\sigma_2(1) = 3$, $\sigma_1(2) = 2$, and $\sigma(3) = 1$. Then σ_1 and σ_2 are transpositions and $\sigma = \sigma_2 \circ \sigma_1$.

The sign of a permutation σ is $(-1)^n$ where n is a finite positive integer such that there exist n transpositions whose composition equals σ. If a permutation has sign 1, then it is called an even permutation. If a permutation has sign -1 then it is called an odd permutation. Thus the identity permutation is an even permutation (since it is equal to the composition of any transposition with itself), and any transposition is an odd permutation (since it is equal to one transposition). The sign map encapsulates the notion of the sign of a permutation of a finite set.

The set of permutations on a set forms a group where the law of composition is composition of functions. One example of a group of permutations that appears frequently in group theory is the symmetric group on n objects, i.e. the group of permutations of the set $\{1, 2, \ldots, n\}$.

transposition

A [transposition] of a set S is a permutation $\sigma\colon S \rightarrow S$ satisfying the following: there exist $s_1, s_2 \in S$ such that

- $\sigma(s_1) = s_2$
- $\sigma(s_2) = s_1$
- and for all $s \in S$, if $s \neq s_1$ and $s \neq s_2$, then $\sigma(s) = s$.

Every permutation of a finite set can be written as the composition of a finite number of transpositions of that set. For example, the permutation $\sigma : \{1, 2, 3\} \rightarrow \{1, 2, 3\}$ defined by $\sigma(1) = 2$, $\sigma(2) = 3$, and $\sigma(3) = 1$ is equivalent to the composition of two transpositions. Define $\sigma_1 : \{1, 2, 3\} \rightarrow \{1, 2, 3\}$ by $\sigma_1(1) = 2$, $\sigma_1(2) = 1$, and $\sigma(3) = 3$, and define $\sigma_2 : \{1, 2, 3\} \rightarrow \{1, 2, 3\}$ by $\sigma_2(1) = 3$, $\sigma_1(2) = 2$, and $\sigma(3) = 1$. Then σ_1 and σ_2 are transpositions and $\sigma = \sigma_2 \circ \sigma_1$. Every transposition is an odd permutation.

sign

The [sign] of a permutation σ is $(-1)^n$ where n is a finite positive integer such that there exist n transpositions whose composition equals σ. If a permutation has sign 1, then it is called an even permutation. If a permutation has sign -1 then it is called an odd permutation. Thus the identity permutation is an even permutation (since it is equal to the composition of any transposition with itself), and any transposition is an odd permutation (since it is equal to one transposition).

even permutation

An [even permutation] is a permutation that has sign 1. That is, an even permutation is the composition of an even number of transpositions. Thus the identity permutation is an even permutation.

odd permutation

An [odd permutation] is a permutation that has sign -1. That is, an odd permutation is the composition of an odd number of transpositions. Thus every tranposition is an odd permutation.

symmetric group

The [symmetric group] on n objects, denoted S_n, is the group of permutations of the set $\{1, 2, \ldots, n\}$; the law of composition is composition of functions. The order of S_n is $n!$ for all positive integers n. For example, $S_2 = \{e, \sigma\}$, where e is the identity permutation, and σ is a transposition. That is, e is the identity element of S_2 and is defined by $e(1) = 1$ and $e(2) = 2$; σ is defined by $\sigma(1) = 2$ and $\sigma(2) = 1$.

sign map

The [sign map], denoted sign, is a group homomorphism from the symmetric group, S_n, into the group $\{1, -1\}$ (under multiplication). The sign map is defined by $\mathrm{sign}(\sigma) = (-1)^k$ where σ is equal to the composition of k transpositions. The sign map is well-defined because it is a standard result that if σ is any permutation (of any set), and if σ is equal to the composition of k transpositions and is also equal to the composition of m transpositions, then $(-1)^k = (-1)^m$. The kernel of the sign map is the alternating group, A_n; that is, A_n is the group of even permutations on n objects.

alternating group

The [alternating group] is the kernel of the sign map. In other words, the alternating group on n objects, usually denoted A_n, is a normal subgroup of the symmetric group on n objects: $A_n = \{\sigma \in S_n \mid \mathrm{sign}(\sigma) = 1\}$. Thus A_n is the group of even permutations in S_n. For $n \geq 5$, A_n is a simple group, i.e. a group that has no proper normal subgroup.

simple group

A group G is a [simple group] if every normal subgroup N of G is not a proper subgroup. That is, G is simple if its only normal subgroups are G and the trivial group. The alternating group A_n is simple for $n \geq 5$. Any cyclic group of prime order is simple. Any cyclic group of prime order is simple. In fact, any simple abelian group is a cyclic group of prime order.

subgroup

A subset H of a group G is a [subgroup] of G if it satisfies the following properties:

- If $a \in H$ and $b \in H$, then $ab \in H$.
- $1 \in H$, where 1 is the identity element of G.
- If $a \in H$ then the inverse of a, a^{-1}, is also in H.

When it is clear that G is a group, sometimes $H \subseteq G$ is used to denote that H is a subgroup of G (as opposed to merely being a subset of G).
Every nontrivial group G has at least two subgroups: the whole group G and the subgroup $\{1\}$ consisting exactly of the identity element of G. If G is trivial then these two subgroups are the same and G has exactly one subgroup. A subgroup is a proper subgroup if it is neither the whole group nor the trivial group.
As an example, the integers under addition are a subgroup of the real numbers under addition.
By Lagrange's Group Theorem, if H is a subgroup of a finite group G, the order of H divides the order of G.

proper subgroup

A [proper subgroup] of a group G is a nontrivial subgroup of G that is not equal to G.

order

A finite group G is said to have [order] n if G has n elements. More generally, the order of a group G is the cardinality of the set G, both of which are often denoted $|G|$.
For any given element x of a given group, if there exists a positive integer k such that $x^k = 1$, then x is said to have order m, where m is the least positive integer satisfying $x^m = 1$. If $x^k \neq 1$ for all positive integers k, then x is said to have infinite order.

cyclic group

If G is a group and if x is an element of G, the [cyclic group] $\langle x \rangle$ generated by x is the set of all powers of x: $\langle x \rangle = \{\ldots, x^{-2}, x^{-1}, 1, x, x^2, \ldots\}$.
Note that $\langle x \rangle$ is the smallest subgroup of G which contains x. Further note that any cyclic group is abelian. If x has infinite order then $\langle x \rangle$ is said to be infinite cyclic. Note that if $\langle x \rangle$ is infinite cyclic then $\langle x \rangle$ is isomorphic to Z^+, the integers under addition. As a result, one sometimes refers to any infinite cyclic group as *the* infinite cyclic group, denoted Z^+.
If x has order n, then $\langle x \rangle$ has order n and is called a cyclic group of order n: $\langle x \rangle = \{1, x, x^2, \ldots, x^n\}$.
If $\langle x \rangle$ is a cyclic group of order n, then $\langle x \rangle$ is isomorphic to Z/n, where Z/n is the group satisfying the following properties (we use additive notation as opposed to multiplicative notation for the law of composition of Z/n): 1. $Z/n = \{0, 1, 2, \ldots, n-1\}$. 2. for any $x, y \in Z/n$, $x +_1 y$ is the unique element in Z/n which is congruent modulo n to $x + y$, where $+_1$ denotes the law of composition on Z/n and $+$ denotes conventional integer addition. Normally $+$ is used to denote the law of composition on Z/n, but $+_1$ is used here to distinguish it from conventional addition. Two integers a and b are congruent modulo n, written $a \equiv b(\text{modulo } n)$, if n divides $b - a$.
As a result, one sometimes refers to any cyclic group of order n as *the* cyclic group of order n, often denoted Z/n.

cyclic group

Let G_1 and G_2 be groups. A map $\varphi\colon G_1 \to G_2$ is a group [homomorphism] if $\varphi(ab) = \varphi(a)\varphi(b)$ for all $a, b \in G_1$. Here we use the same multiplicative notation for the laws of composition of G_1 and G_2, even though there is no requirement that their laws of composition be the same.
Note that $\varphi(1_{G_1}) = 1_{G_2}$ and $\varphi(a^{-1}) = \varphi(a)^{-1}$ for all $a \in G$, where 1_{G_i} is the identity of G_i.
The kernel of φ, sometimes denoted ker φ, is the set $\{x \in G_1 \mid \varphi(x) = 1_{G_2}\}$. Note that ker φ is a normal subgroup of G_2.
Another subgroup of G_2 determined by φ is the image of φ, sometimes denoted im φ. The image of φ is im $\varphi = \{x \in G_2 \mid x = \varphi(a)$ for some $a \in G_1\}$. Sometimes the image of φ is denoted $\varphi(G_1)$. The following are examples of homomorphisms:

- The inclusion map $i\colon H \to G$ defined by $i(a) = a$, where H is a subgroup of G. ker $i = \{1_G\}$ and im $i = H$.
- For a fixed $a \in G$, the map $\varphi\colon Z^+ \to G$ defined by $\varphi(n) = a^n$, where Z^+ denotes the integers with addition. ker $\varphi = \{n \mid a^n = 1_G\}$ and im $\varphi = \langle a \rangle$ (the cyclic subgroup generated by a).
- The determinant map det: $GL_n(R) \to R^\times$, where $GL_n(R)$ denotes the general linear group and $R^\times$ denotes the real numbers without zero under multiplication. $kerdet = SL_n(R)$, the special linear group, and $imdet = R^\times$.
- The sign map on permutations sign: $S_n \to \{1, -1\}$, where S_n denotes the symmetric group on n objects. ker sign $= A_n$, the alternating group, and im sign $= \{1, -1\}$.

Let R_1 and R_2 be rings. A map $\varphi\colon R_1 \to R_2$ is a ring homomorphism if

- $\varphi(a + b) = \varphi(a) + \varphi(b)$,
- $\varphi(ab) = \varphi(a)\varphi(b)$, and
- $\varphi(1_{R_1}) = 1_{R_2}$, for all $a, b \in R_1$.

Here we use the same additive and multiplicative notation for the laws of composition of R_1 and R_2, even though there is no requirement that their laws of composition be the same.

kernel

The [kernel] of a group homomorphism $\varphi\colon G_1 \to G_2$ is the set $\ker\varphi = \{x \in G_1 \mid \varphi(x) = 1_{G_2}\}$, where 1_{G_2} denotes the identity of G_2. The kernel of a homomorphism is an important example of a normal subgroup. There are many results involving the kernel of a homomorphism.

image

The [image] of a map $\varphi\colon G_1 \to G_2$ is the set $\{x \in G_2 \mid x = \varphi(a) \text{ for some } a \in G_1\}$. In general, the image of φ is often denoted $\varphi(G_1)$. If φ is a group homomorphism, then the image of φ is a subgroup of G_2 and is sometimes denoted $\operatorname{im}\varphi$.

isomorphism

A group [isomorphism] is a bijective group homomorphism.
A ring isomorphism is a bijective ring homomorphism.

isomorphic

Two groups G_1 and G_2 are [isomorphic] if there exists a group isomorphism from G_1 into G_2. Sometimes $G_1 \cong G_2$ is used to denote 'G_1 and G_2 are isomorphic.' Note that $\cong$ is an equivalence relation on the set of all groups. When one speaks of classifying groups, hat is usually referred to is the classification of isomorphism classes. Thus one might say that there are two groups of order 6 *up to isomorphism*, meaning that there are two isomorphism classes of groups of order 6.
One sometimes says that 'G_1 is isomorphic to G_2' instead of saying 'G_1 and G_2 are isomorphic.'

automorphism

An [automorphism] of a group G is an isomorphism from G into G. The identity map is a simple example of an automorphism. Conjugation by an element of the group is an important example of an automorphism. That is, for a fixed element $b \in G$, conjugation by b is the map $\varphi\colon G \to G$ defined by $\varphi(a) = bab^{-1}$. Here we use multiplicative notation for the group law of composition. Note that if G is abelian, then conjugation by any element is the identity map. However, if G is not abelian, then there exists a nontrivial conjugation (i.e. a conjugation not equal to the identity map) of G.

automorphism

Let G be a group and let $b \in G$. The map $\varphi\colon G \to G$ defined by $\varphi(a) = bab^{-1}$ is [conjugation] by b. Note that conjugation is an automorphism of G. Further note that if G is abelian, then conjugation by any element is the identity map. However, if G is not abelian, then there exists a nontrivial conjugation (i.e. a conjugation not equal to the identity map) of G.

conjugation

Let G be a group and let H be a subgroup of G. H is a [normal subgroup] of G (sometimes written $H \lhd G$) if for all $a \in H$ and for all $x \in G$, $xax^{-1} \in H$. Note that it follows that any subgroup of an abelian group is normal.

Normal subgroups appear often in group theory. Every group G has at least one normal subgroup, called the center of G, denoted by Z or $Z(G)$. The center of G is the set of elements that commute with every element of G: $Z(G) = \{z \in G \mid zx = xz \text{ for all } x \in G\}$. Another important example of a normal subgroup is the kernel of a group homomorphism.

center

The [center] of a group G, denoted by Z or $Z(G)$ is the set of elements that commute with every element of G: $Z(G) = \{z \in G \mid zx = xz \text{ for all } x \in G\}$. Note that if G is abelian then $Z(G) = G$.

coset

Given a subgroup H of a group G, a [coset] of H is a subset H' of G such that there exists an $a \in G$ such that (1) $H' = aH = \{ah \mid h \in H\}$, in which case H' is said to be a left coset; or (2) $H' = Ha = \{ha \mid h \in H\}$, in which case H' is said to be a right coset.

Given $a \in G$, aH is not necessarily equal to Ha. However, one can show that the subgroup H of G is a normal subgroup if and only if $aH = Ha$ for every $a \in G$.

In what follows, only left cosets will be discussed, though similar statements may be made about right cosets.

The left cosets of H are the equivalence classes of the equivalence relation $\sim$ defined by $a \sim b$ if there exists $h \in H$ such that $a = bh$. Since equivalence classes form a partition, the left cosets of H partition G.

The cardinality of the set of left cosets of H is called the index of H in G and is denoted by $[G : H]$. Given $a \in G$, $h \mapsto ah$ defines a bijective map from H into aH. If G is finite, it follows that $|G| = |H|[G : H]$, where $|G|$ denotes the order of G. A very important result follows: if G is finite, then the order of H divides the order of G. Moreover, since the order of any element of G is the order of the cyclic subgroup it generates, if G is finite then the order of an element of G divides the order of G. These results follow from a special case of what is known as Lagrange's Group Theorem: if G is a group, H is a subgroup of G and K is a sugroup of H, then $[G : K] = [G : H][H : K]$, where the products are taken as products of cardinals.

An important result that follows from Lagrange's Theorem is that if the order of G is a prime number then $G = \langle a \rangle$ for any $a \in G$ such that a is not the identity, where $\langle a \rangle$ denotes the cyclic group generated by a.

Note that if $\varphi\colon G \to G'$ is a group [homomorphism], then $[G : ker\varphi] = |im\varphi|$. Thus another result of Langrange's Theorem is that $|G| = |ker\varphi| \cdot |im\varphi|$.

left coset

Given a subgroup H of a group G, a [left coset] of H is a subset H' of G such that there exists an $a \in G$ such that $H' = aH = \{ah \mid h \in H\}$.

Given $a \in G$, aH is not necessarily equal to Ha. However, one can show that the subgroup H of G is a normal subgroup if and only if $aH = Ha$ for every $a \in G$.

In what follows, only left cosets will be discussed, though similar statements may be made about right cosets.

The left cosets of H are the equivalence classes of the equivalence relation $\sim$ defined by $a \sim b$ if there exists $h \in H$ such that $a = bh$. Since equivalence classes form a partition, the left cosets of H partition G.

The cardinality of the set of left cosets of H is called the index of H in G and is denoted by $[G : H]$. Given $a \in G$, $h \mapsto ah$ defines a bijective map from H into aH. If G is finite, it follows that $|G| = |H|[G : H]$, where $|G|$ denotes the order of G. A very important result follows: if G is finite, then the order of H divides the order of G. Moreover, since the order of any element of G is the order of the cyclic subgroup it generates, if G is finite then the order of an element of G divides the order of G. These results follow from a special case of what is known as Lagrange's Group Theorem: if G is a group, H is a subgroup of G and K is a sugroup of H, then $[G : K] = [G : H][H : K]$, where the products are taken as products of cardinals.

An important result that follows from Lagrange's Theorem is that if the order of G is a prime number then $G = \langle a \rangle$ for any $a \in G$ such that a is not the identity, where $\langle a \rangle$ denotes the cyclic group generated by a.

Note that if $\varphi\colon G \to G'$ is a group [homomorphism], then $[G : ker(\varphi)] = |im(\varphi)|$. Thus another result of Langrange's Theorem is that $|G| = |ker(\varphi)| \cdot |im(\varphi)|$.

right coset

Given a subgroup H of a group G, a [right coset] of H is a subset H' of G such that there exists an $a \in G$ such that $H' = Ha = \{ha \mid h \in H\}$.

Given $a \in G$, aH is not necessarily equal to Ha. However, one can show that the subgroup H of G is a normal subgroup if and only if $aH = Ha$ for every $a \in G$.

In what follows, only left cosets will be discussed, though similar statements may be made about right cosets.

The left cosets of H are the equivalence classes of the equivalence relation $\sim$ defined by $a \sim b$ if there exists $h \in H$ such that $a = bh$. Since equivalence classes form a partition, the left cosets of H partition G.

The cardinality of the set of left cosets of H is called the index of H in G and is denoted by $[G : H]$. Given $a \in G$, $h \mapsto ah$ defines a bijective map from H into aH. If G is finite, it follows that $|G| = |H|[G : H]$, where $|G|$ denotes the order of G. A very important result follows: if G is finite, then the order of H divides the order of G. Moreover, since the order of any element of G is the order of the cyclic subgroup it generates, if G is finite then the order of an element of G divides the order of G. These results follow from a special case of what is known as Lagrange's Group Theorem: if G is a group, H is a subgroup of G and K is a sugroup of H, then $[G : K] = [G : H][H : K]$, where the products are taken as products of cardinals.

An important result that follows from Lagrange's Theorem is that if the order of G is a prime number then $G = \langle a \rangle$ for any $a \in G$ such that a is not the identity, where $\langle a \rangle$ denotes the cyclic group generated by a.

Note that if $\varphi\colon G \to G'$ is a group homomorphism, then $[G : ke(\varphi)] = |im(\varphi)|$. Thus another result of Langrange's Theorem is that $|G| = |ker(\varphi)| \cdot |im(\varphi)|$.

index

The [index] of subgroup H of a group G is the cardinality of the set of left cosets of H in G. The index of H in G is denoted $[G : H]$.

quotient group

Given a group G and a normal subgroup N of G, the [quotient group] of N in G, written G/N and read "G mod(ulo) N", is the set of cosets of N in G, under the law of composition that is defined as follows: $(aN)(bN) = abN$, where $xN = \{xn \mid n \in N\}$. Note that since N is normal, $aN = Na$ for all $a \in G$, so it is not necessary to define this law of composition in terms of left cosets instead of right cosets.
The order of G/N is the index $[G : N]$ of N in G.
Quotient groups can be identified by the First Isomorphism Theorem: if $\varphi\colon G \to G'$ is a surjective group homomorphism and if $N = ke(\varphi)$ then $\psi\colon G/N \to G'$ is an isomorphism, where ψ is defined by $\psi(aN) = \varphi(a)$.

First Isomorphism Theorem

The [First Isomorphism Theorem]. Suppose $\varphi\colon G \to G'$ is a surjective group homomorphism, and let N denote the kernel of φ. Then the quotient group G/N is isomorphic to G' by the map ψ defined by $\psi(aN) = \varphi(a)$.
The First Isomorphism Theorem is the principle method of identifying quotient groups. As an example, consider the group homomorphism φ from $C^\times$, the nonzero complex numbers under multiplication, into $R^\times$, the nonzero real numbers under multiplication, defined by $\varphi(z) = |z|$, where $|z|$ denotes the absolute value of z. The kernel of φ is the unit circle, U, and the image of φ is the group of positive real numbers. So $C^\times/U$ is isomorphic to the multiplicative group of positive real numbers.

operation

Given a group G and a set S, an [operation] of a G on S is a map from $G \times S$ into S - often written using multiplicative notation: $(g, s) \mapsto gs$ - satisfying:

- $1s = s$ for all $s \in S$, where 1 is the identity of G; and
- $(gg')s = g(g's)$, for all $g, g' \in G$ and for all $s \in S$.

There are some terms that are sometimes associated with a group operation: S is often called a G-set; G is sometimes called a transformation group; and the group operation is often also called a group action.
Mathworld: "Historically, the first group action studied was the action of the Galois group on the roots of a polynomial. However, there are numerous examples and applications of group actions in many branches of mathematics, including algebra, topology, geometry, number theory, and analysis, as well as the sciences, including chemistry and physics."

This file is part of the Sofia project sponsored by the Provost's fund for teaching and learning at Harvard university. There are 44 entries in this file.

Index