Permutations Applied To Construction Company Management

PDF generated using the open source mwlib toolkit. See http://code.pediapress.com/ for more information.
PDF generated at: Sat, 21 Sep 2013 01:41:34 UTC

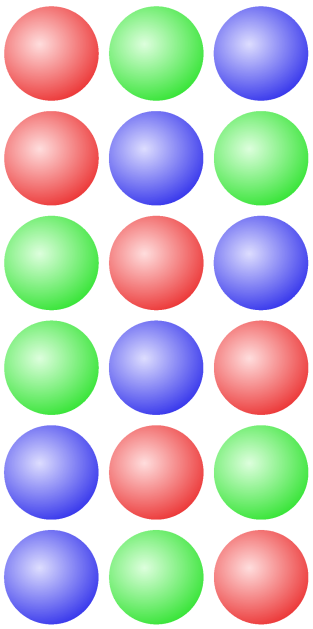
Contents

Articles

References

Article Licenses

Permutation



The 6 permutations of 3 balls

In mathematics, the notion of **permutation** is used with several slightly different meanings, all related to the act of **permuting** (rearranging) objects or values. Informally, a permutation of a set of objects is an arrangement of those objects into a particular order. For example, there are six permutations of the set {1,2,3}, namely (1,2,3), (1,3,2), (2,1,3), (2,3,1), (3,1,2), and (3,2,1). For example, an anagram of a word is a permutation of its letters. The study of permutations in this sense generally belongs to the field of combinatorics.

The number of permutations of n distinct objects is $n\times(n-1)\times(n-2)\times\cdots\times1$, which is commonly denoted as "n factorial" and written "$n!$".

Permutations occur, in more or less prominent ways, in almost every domain of mathematics. They often arise when different orderings on certain finite sets are considered, possibly only because one wants to ignore such orderings and needs to know how many configurations are thus identified. For similar reasons permutations arise in the study of sorting algorithms in computer science.

In algebra and particularly in group theory, a permutation of a set S is defined as a bijection from S to itself (i.e., a map $S \to S$ for which every element of S occurs exactly once as image value). This is related to the rearrangement of S in which each element s takes the place of the corresponding $f(s)$. The collection of such permutations form a symmetric group. The key to its structure is the possibility to compose permutations: performing two given rearrangements in succession defines a third rearrangement, the composition. Permutations may *act* on composite objects by rearranging their components, or by certain replacements (substitutions) of symbols.

In elementary combinatorics, the k-permutations, or partial permutations, are the sequences of k distinct elements selected from a set. When k is equal to the size of the set, these are the permutations of the set.

History

The rule to determine the number of permutations of n objects was known in Indian culture at least as early as around 1150: the Lilavati by the Indian mathematician Bhaskara II contains a passage that translates to

> The product of multiplication of the arithmetical series beginning and increasing by unity and continued to the number of places, will be the variations of number with specific figures.[1]

A first case in which seemingly unrelated mathematical questions were studied with the help of permutations occurred around 1770, when Joseph Louis Lagrange, in the study of polynomial equations, observed that properties of the permutations of the roots of an equation are related to the possibilities to solve it. This line of work ultimately resulted, through the work of Évariste Galois, in Galois theory, which gives a complete description of what is possible and impossible with respect to solving polynomial equations (in one unknown) by radicals. In modern mathematics there are many similar situations in which understanding a problem requires studying certain permutations related to it.

Generalities

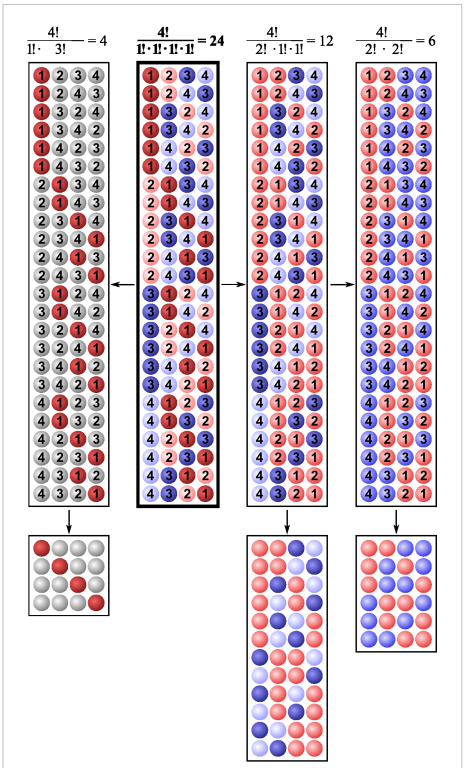
The notion of permutation is used in the following contexts.

In group theory

In group theory and related areas, one considers permutations of arbitrary sets, even infinite ones. A permutation of a set S is a bijection from S to itself. This allows for permutations to be composed, which allows the definition of groups of permutations. If S is a finite set of n elements, then there are $n!$ permutations of S.

In combinatorics

In combinatorics, a permutation is usually understood to be a sequence containing each element from a finite set once, and only once. The concept of *sequence* is distinct from that of a *set*, in that the elements of a sequence appear in some order: the sequence has a first element (unless it is empty), a second element (unless its length is less than 2), and so on. In contrast, the elements in a set have no order; {1, 2, 3} and {3, 2, 1} are different ways to denote the same set. In this sense a permutation of a finite set S of n elements is equivalent to a bijection from {1, 2, ..., n} to S (in which any i is mapped to the i-th element of the sequence), or to a choice of a total ordering on S (for which $x < y$ if x comes before y in the sequence). There are $n!$ permutations of S.



Permutations of multisets

There is also a weaker meaning of the term "permutation" that is sometimes used in elementary combinatorics texts, designating those sequences in which no element occurs more than once, but without the requirement to use all elements from a given set. Indeed this use often involves considering sequences of a fixed length k of elements taken from a given set of size n. These objects are also known as **partial permutations** or as **sequences without repetition**, terms that avoids confusion with the other, more common, meanings of "permutation". The number of such ***k*-permutations of *n*** is denoted variously by such symbols as ${}_nP_k$, ${}^nP_k$, $P_{n,k}$, or $P(n,k)$, and its value is given by the product

$$n \cdot (n-1) \cdot (n-2) \cdots (n-k+1)$$

which is 0 when $k > n$, and otherwise is equal to

$$\frac{n!}{(n-k)!}.$$

The product is well defined without the assumption that n is a non-negative integer and is of importance outside combinatorics as well; it is known as the Pochhammer symbol $(n)_k$ or as the k-th falling factorial power $n^{\underline{k}}$ of n.

If M is a finite multiset, then a **multiset permutation** is a sequence of elements of M in which each element appears exactly as often as is its multiplicity in M. If the multiplicities of the elements of M (taken in some order) are m_1, m_2, ..., m_l and their sum (i.e., the size of M) is n, then the number of multiset permutations of M is given by the multinomial coefficient

$$\binom{n}{m_1, m_2, \ldots, m_l} = \frac{n!}{m_1!\, m_2! \cdots m_l!}.$$

Permutations in group theory

In group theory, the term *permutation* of a set means a bijective map, or bijection, from that set onto itself. The set of all permutations of any given set *S* forms a group, with composition of maps as product and the identity as neutral element. This is the **symmetric group** of *S*. Up to isomorphism, this symmetric group only depends on the cardinality of the set, so the nature of elements of *S* is irrelevant for the structure of the group. Symmetric groups have been studied most in the case of a finite sets, in which case one can assume without loss of generality that $S=\{1,2,...,n\}$ for some natural number *n*, which defines the symmetric group of degree *n*, written $\mathbf{S}_n$.

Any subgroup of a symmetric group is called a **permutation group**. In fact by Cayley's theorem any group is isomorphic to some permutation group, and every finite group to a subgroup of some finite symmetric group. However, permutation groups have more structure than abstract groups, allowing for instance to define the cycle type of an element of a permutation group; different realizations of a group as a permutation group need not be equivalent for this additional structure. For instance $\mathbf{S}_3$ is naturally a permutation group, in which any transposition has cycle type (2,1), but the proof of Cayley's theorem realizes $\mathbf{S}_3$ as a subgroup of $\mathbf{S}_6$ (namely the permutations of the 6 elements of $\mathbf{S}_3$ itself), in which permutation group transpositions get cycle type (2,2,2). So in spite of Cayley's theorem, the study of permutation groups differs from the study of abstract groups.

Notation

There are three main notations for permutations of a finite set *S*. In Cauchy's *two-line notation*, one lists the elements of *S* in the first row, and for each one its image under the permutation below it in the second row. For instance, a particular permutation of the set {1,2,3,4,5} can be written as:

$$\sigma = \begin{pmatrix} 1 & 2 & 3 & 4 & 5 \\ 2 & 5 & 4 & 3 & 1 \end{pmatrix};$$

this means that σ satisfies $\sigma(1)=2$, $\sigma(2)=5$, $\sigma(3)=4$, $\sigma(4)=3$, and $\sigma(5)=1$.

In *one-line notation*, one gives only the second row of this array, so the one-line notation for the permutation above is 25431. (It is typical to use commas to separate these entries only if some have two or more digits.)

Cycle notation, the third method of notation, focuses on the effect of successively applying the permutation. It expresses the permutation as a product of cycles corresponding to the orbits (with at least two elements) of the permutation; since distinct orbits are disjoint, this is loosely referred to as "the decomposition into disjoint cycles" of the permutation. It works as follows: starting from some element *x* of *S* with $\sigma(x) \neq x$, one writes the sequence $(x\ \sigma(x)\ \sigma(\sigma(x))\ ...)$ of successive images under σ, until the image would be *x*, at which point one instead closes the parenthesis. The set of values written down forms the orbit (under σ) of *x*, and the parenthesized expression gives the corresponding cycle of σ. One then continues choosing an element *y* of *S* that is not in the orbit already written down, and such that $\sigma(y) \neq y$, and writes down the corresponding cycle, and so on until all elements of *S* either belong to a cycle written down or are fixed points of σ. Since for every new cycle the starting point can be chosen in different ways, there are in general many different cycle notations for the same permutation; for the example above one has for instance

$$\begin{pmatrix} 1 & 2 & 3 & 4 & 5 \\ 2 & 5 & 4 & 3 & 1 \end{pmatrix} = (1\ \ 2\ \ 5)(3\ \ 4) = (3\ \ 4)(1\ \ 2\ \ 5) = (3\ \ 4)(5\ \ 1\ \ 2).$$

Each cycle $(x_1\ x_2\ ...\ x_l)$ of σ denotes a permutation in its own right, namely the one that takes the same values as σ on this orbit (so it maps x_i to x_{i+1} for $i < l$, and x_l to x_1), while mapping all other elements of *S* to themselves. The size *l* of the orbit is called the length of the cycle. Distinct orbits of σ are by definition disjoint, so the corresponding cycles commute, and σ is the product of its cycles (taken in any order). Therefore the concatenation of cycles in the cycle notation can be interpreted as denoting composition of permutations, whence the name "decomposition" of the permutation. This decomposition is essentially unique: apart from the reordering the cycles in the product, there are no other ways to write σ as a product of cycles (possibly unrelated to the cycles of σ) that have disjoint orbits. The

cycle notation is less unique, since each individual cycle can be written in different ways, as in the example above where (5 1 2) denotes the same cycle as (1 2 5) (but (5 2 1) would denote a different permutation).

An orbit of size 1 (a fixed point x in S) has no corresponding cycle, since that permutation would fix x as well as every other element of S, in other words it would be the identity, independently of x. It is possible to include (x) in the cycle notation for σ to stress that σ fixes x (and this is even standard in combinatorics, as described in cycles and fixed points), but this does not correspond to a factor in the (group theoretic) decomposition of σ. If the notion of "cycle" were taken to include the identity permutation, then this would spoil the uniqueness (up to order) of the decomposition of a permutation into disjoint cycles. The decomposition into disjoint cycles of the identity permutation is an empty product; its cycle notation would be empty, so some other notation like e is usually used instead.

Cycles of length two are called transpositions; such permutations merely exchange the place of two elements.

Group structure

Product and inverse

The product of two permutations is defined as their composition as functions, in other words $\sigma\cdot\pi$ is the function that maps any element x of the set to $\sigma(\pi(x))$. Note that the rightmost permutation is applied to the argument first, because of the way function application is written. Some authors prefer the leftmost factor acting first, but to that end permutations must be written to the *right* of their argument, for instance as an exponent, where σ acting on x is written x^{σ}; then the product is defined by $x^{\sigma\cdot\pi}=(x^{\sigma})^{\pi}$. However this gives a *different* rule for multiplying permutations; this article uses the definition where the rightmost permutation is applied first.

Since the composition of two bijections always gives another bijection, the product of two permutations is again a permutation. Since function composition is associative, so is the product operation on permutations: $(\sigma\cdot\pi)\cdot\varrho=\sigma\cdot(\pi\cdot\varrho)$. Therefore, products of more than two permutations are usually written without adding parentheses to express grouping; they are also usually written without a dot or other sign to indicate multiplication.

The identity permutation, which maps every element of the set to itself, is the neutral element for this product. In two-line notation, the identity is

$$\begin{pmatrix}1 & 2 & 3 & \cdots & n\\ 1 & 2 & 3 & \cdots & n\end{pmatrix}.$$

Since bijections have inverses, so do permutations, and the inverse σ^{-1} of σ is again a permutation. Explicitly, whenever $\sigma(x)=y$ one also has $\sigma^{-1}(y)=x$. In two-line notation the inverse can be obtained by interchanging the two lines (and sorting the columns if one wishes the first line to be in a given order). For instance

$$\begin{pmatrix}1 & 2 & 3 & 4 & 5\\ 2 & 5 & 4 & 3 & 1\end{pmatrix}^{-1}=\begin{pmatrix}2 & 5 & 4 & 3 & 1\\ 1 & 2 & 3 & 4 & 5\end{pmatrix}=\begin{pmatrix}1 & 2 & 3 & 4 & 5\\ 5 & 1 & 4 & 3 & 2\end{pmatrix}.$$

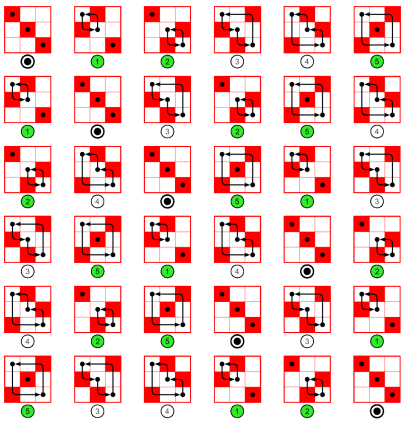
In cycle notation one can reverse the order of the elements in each cycle to obtain a cycle notation for its inverse.

Having an associative product, a neutral element, and inverses for all its elements, makes the set of all permutations of S into a group, called the symmetric group of S.

Properties

Every permutation of a finite set can be expressed as the product of transpositions. Moreover, although many such expressions for a given permutation may exist, there can never be among them both expressions with an even number and expressions with an odd number of transpositions. All permutations are then classified as even or odd, according to the parity of the transpositions in any such expression.

Multiplying permutations written in cycle notation follows no easily described pattern, and the cycles of the product can be entirely different from those of the permutations being composed. However the cycle structure is preserved in the special case of conjugating a permutation σ by another permutation π, which means forming the product $\pi\cdot\sigma\cdot\pi^{-1}$. Here the cycle notation of the result can be obtained by taking the cycle notation for σ and applying π to all the entries in it.



Composition of permutations corresponds to multiplication of permutation matrices.

Matrix representation

One can represent a permutation of {1, 2, ..., n} as an $n\times n$ matrix. There are two natural ways to do so, but only one for which multiplications of matrices corresponds to multiplication of permutations in the same order: this is the one that associates to σ the matrix M whose entry $M_{i,j}$ is 1 if $i = \sigma(j)$, and 0 otherwise. The resulting matrix has exactly one entry 1 in each column and in each row, and is called a *permutation matrix*. Here [2] (file) is a list of these matrices for permutations of 4 elements. The Cayley table on the right shows these matrices for permutations of 3 elements.

Permutation of components of a sequence

As with any group, one can consider actions of a symmetric group on a set, and there are many ways in which such an action can be defined. For the symmetric group of {1, 2, ..., n} there is one particularly natural action, namely the action by permutation on the set X^n of sequences of n symbols taken from some set X. Like for the matrix representation, there are two natural ways in which the result of permuting a sequence $(x_1,x_2,...,x_n)$ by σ can be defined, but only one is compatible with the multiplication of permutations (so as to give a left action of the symmetric group on X^n); with the multiplication rule used in this article this is the one given by

$$\sigma\cdot(x_1,\ldots,x_n) = (x_{\sigma^{-1}(1)},\ldots,x_{\sigma^{-1}(n)}).$$

This means that each component x_i ends up at position $\sigma(i)$ in the sequence permutate by σ.

Permutations in combinatorics

In combinatorics a permutation of a set S with n elements is a listing of the elements of S in some order (each element occurring exactly once). This can be defined formally as a bijection from the set { 1, 2, ..., n } to S. Note that if S equals { 1, 2, ..., n }, then this definition coincides with the definition in group theory. More generally one could use instead of { 1, 2, ..., n } any set equipped with a total ordering of its elements.

One combinatorial property that is related to the group theoretic interpretation of permutations, and can be defined without using a total ordering of S, is the cycle structure of a permutation σ. It is the partition of n describing the lengths of the cycles of σ. Here there is a part "1" in the partition for every fixed point of σ. A permutation that has no fixed point is called a derangement.

Other combinatorial properties however are directly related to the ordering of S, and to the way the permutation relates to it. Here are a number of such properties.

Ascents, descents and runs

An *ascent* of a permutation σ of n is any position $i < n$ where the following value is bigger than the current one. That is, if $\sigma = \sigma_1\sigma_2...\sigma_n$, then i is an ascent if $\sigma_i < \sigma_{i+1}$.

For example, the permutation 3452167 has ascents (at positions) 1,2,5,6.

Similarly, a *descent* is a position $i < n$ with $\sigma_i > \sigma_{i+1}$, so every i with $1 \leq i < n$ either is an ascent or is a descent of σ.

The number of permutations of n with k ascents is the Eulerian number $\left\langle {n \atop k} \right\rangle$; this is also the number of permutations of n with k descents.[3]

An *ascending run* of a permutation is a nonempty increasing contiguous subsequence of the permutation that cannot be extended at either end; it corresponds to a maximal sequence of successive ascents (the latter may be empty: between two successive descents there is still an ascending run of length 1). By contrast an *increasing subsequence* of a permutation is not necessarily contiguous: it is an increasing sequence of elements obtained from the permutation by omitting the values at some positions. For example, the permutation 2453167 has the ascending runs 245, 3, and 167, while it has an increasing subsequence 2367.

If a permutation has $k - 1$ descents, then it must be the union of k ascending runs. Hence, the number of permutations of n with k ascending runs is the same as the number $\left\langle {n \atop k-1} \right\rangle$ of permutations with $k - 1$ descents.[4]

Inversions

An *inversion* of a permutation σ is a pair (i,j) of positions where the entries of a permutation are in the opposite order: $i < j$ and $\sigma_i > \sigma_j$.[5] So a descent is just an inversion at two adjacent positions. For example, the permutation σ = 23154 has three inversions: (1,3), (2,3), (4,5), for the pairs of entries (2,1), (3,1), (5,4).

Sometimes an inversion is defined as the pair of values (σ_i,σ_j) itself whose order is reversed; this makes no difference for the *number* of inversions, and this pair (reversed) is also an inversion in the above sense for the inverse permutation σ^{-1}. The number of inversions is an important measure for the degree to which the entries of a permutation are out of order; it is the same for σ and for σ^{-1}. To bring a permutation with k inversions into order (i.e., transform it into the identity permutation), by successively applying (right-multiplication by) adjacent transpositions, is always possible and requires a sequence of k such operations. Moreover any reasonable choice for the adjacent transpositions will work: it suffices to choose at each step a transposition of i and $i + 1$ where i is a descent of the permutation as modified so far (so that the transposition will remove this particular descent, although it might create other descents). This is so because applying such a transposition reduces the number of inversions by 1; also note that as long as this number is not zero, the permutation is not the identity, so it has at least one descent. Bubble sort and insertion sort can be interpreted as particular instances of this procedure to put a sequence into order. Incidentally this procedure proves that any permutation σ can be written as a product of adjacent transpositions; for this one may simply reverse any sequence of such transpositions that transforms σ into the identity. In fact, by enumerating all sequences of adjacent transpositions that would transform σ into the identity, one obtains (after reversal) a *complete* list of all expressions of minimal length writing σ as a product of adjacent transpositions.

The number of permutations of n with k inversions is expressed by a Mahonian number,[6] it is the coefficient of X^k in the expansion of the product

$$\prod_{m=1}^{n} \sum_{i=0}^{m-1} X^i = 1(1+X)(1+X+X^2)\cdots(1+X+X^2+\cdots+X^{n-1}),$$

which is also known (with q substituted for X) as the q-factorial $[n]_q!$. The expansion of the product appears in Necklace (combinatorics).

Counting sequences without repetition

In this section, a *k*-permutation of a set *S* is an ordered sequence of *k* distinct elements of *S*. For example, given the set of letters {C, E, G, I, N, R}, the sequence ICE is a 3-permutation, RING and RICE are 4-permutations, NICER and REIGN are 5-permutations, and CRINGE is a 6-permutation; since the latter uses all letters, it is a permutation of the given set in the ordinary combinatorial sense. ENGINE on the other hand is not a permutation, because of the repetitions: it uses the elements E and N twice.

Let *n* be the size of *S*, the number of elements available for selection. In constructing a *k*-permutation, there are *n* possible choices for the first element of the sequence, and this is then number of 1-permutations. Once it has been chosen, there are $n - 1$ elements of *S* left to choose from, so a second element can be chosen in $n - 1$ ways, giving a total $n \times (n - 1)$ possible 2-permutations. For each successive element of the sequence, the number of possibilities decreases by 1 which leads to the number of

$n \times (n - 1) \times (n - 2) \ldots \times (n - k + 1)$ possible *k*-permutations.

This gives in particular the number of *n*-permutations (which contain all elements of *S* once, and are therefore simply permutations of *S*):

$n \times (n - 1) \times (n - 2) \times \ldots \times 2 \times 1,$

a number that occurs so frequently in mathematics that it is given a compact notation "*n*!", and is called "*n* factorial". These *n*-permutations are the longest sequences without repetition of elements of *S*, which is reflected by the fact that the above formula for the number of *k*-permutations gives zero whenever $k > n$.

The number of *k*-permutations of a set of *n* elements is sometimes denoted by $P(n,k)$ or a similar notation (usually accompanied by a notation for the number of *k*-combinations of a set of *n* elements in which the "*P*" is replaced by "*C*"). That notation is rarely used in other contexts than that of counting *k*-permutations, but the expression for the number does arise in many other situations. Being a product of *k* factors starting at *n* and decreasing by unit steps, it is called the *k*-th falling factorial power of *n*:

$$n^{\underline{k}} = n \times (n-1) \times (n-2) \times \cdots \times (n-k+1),$$

though many other names and notations are in use, as detailed at Pochhammer symbol. When $k \leq n$ the factorial power can be completed by additional factors: $n^{\underline{k}} \times (n - k)! = n!$, which allows writing

$$n^{\underline{k}} = \frac{n!}{(n-k)!}.$$

The right hand side is often given as expression for the number of *k*-permutations, but its main merit is using the compact factorial notation. Expressing a product of *k* factors as a quotient of potentially much larger products, where all factors in the denominator are also explicitly present in the numerator, is not particularly efficient; as a method of computation there is the additional danger of overflow or rounding errors. It should also be noted that the expression is undefined when $k > n$, whereas in those cases the number $n^{\underline{k}}$ of *k*-permutations is just 0.

Permutations in computing

Numbering permutations

One way to represent permutations of *n* is by an integer *N* with $0 \leq N < n!$, provided convenient methods are given to convert between the number and the usual representation of a permutation as a sequence. This gives the most compact representation of arbitrary permutations, and in computing is particularly attractive when *n* is small enough that *N* can be held in a machine word; for 32-bit words this means $n \leq 12$, and for 64-bit words this means $n \leq 20$. The conversion can be done via the intermediate form of a sequence of numbers d_n, d_{n-1}, ..., d_2, d_1, where d_i is a non-negative integer less than *i* (one may omit d_1, as it is always 0, but its presence makes the subsequent conversion to a permutation easier to describe). The first step then is simply expression of *N* in the **factorial number system**, which is just a particular mixed radix representation, where for numbers up to *n*! the bases for successive digits are *n*,

$n - 1$, ..., 2, 1. The second step interprets this sequence as a Lehmer code or (almost equivalently) as an inversion table.

Rothe diagram for

i \ σ_i	**1**	**2**	**3**	**4**	**5**	**6**	**7**	**8**	**9**	**Lehmer code**
1	×	×	×	×	×	•				$d_9 = 5$
2	×	×	•							$d_8 = 2$
3	×	×		×	×		×	•		$d_7 = 5$
4	•									$d_6 = 0$
5		×		•						$d_5 = 1$
6		×			×		×		•	$d_4 = 3$
7		×			×		•			$d_3 = 2$
8		•								$d_2 = 0$
9					•					$d_1 = 0$
inversion table	3	6	1	2	4	0	2	0	0	

In the **Lehmer code** for a permutation σ, the number d_n represents the choice made for the first term σ_1, the number d_{n-1} represents the choice made for the second term σ_2 among the remaining $n - 1$ elements of the set, and so forth. More precisely, each d_{n+1-i} gives the number of *remaining* elements strictly less than the term σ_i. Since those remaining elements are bound to turn up as some later term σ_j, the digit d_{n+1-i} counts the *inversions* (i,j) involving i as smaller index (the number of values j for which $i < j$ and $\sigma_i > \sigma_j$). The **inversion table** for σ is quite similar, but here d_{n+1-k} counts the number of inversions (i,j) where $k = \sigma_j$ occurs as the smaller of the two values appearing in inverted order.[7] Both encodings can be visualized by an n by n **Rothe diagram**[8] (named after Heinrich August Rothe) in which dots at (i,σ_i) mark the entries of the permutation, and a cross at (i,σ_j) marks the inversion (i,j); by the definition of inversions a cross appears in any square that comes both before the dot (j,σ_j) in its column, and before the dot (i,σ_i) in its row. The Lehmer code lists the numbers of crosses in successive rows, while the inversion table lists the numbers of crosses in successive columns; it is just the Lehmer code for the inverse permutation, and vice versa.

To effectively convert a Lehmer code d_n, d_{n-1}, ..., d_2, d_1 into a permutation of an ordered set S, one can start with a list of the elements of S in increasing order, and for i increasing from 1 to n set σ_i to the element in the list that is preceded by d_{n+1-i} other ones, and remove that element from the list. To convert an inversion table d_n, d_{n-1}, ..., d_2, d_1 into the corresponding permutation, one can traverse the numbers from d_1 to d_n while inserting the elements of S from largest to smallest into an initially empty sequence; at the step using the number d from the inversion table, the element from S inserted into the sequence at the point where it is preceded by d elements already present. Alternatively one could process the numbers from the inversion table and the elements of S both in the opposite order, starting with a row of n empty slots, and at each step place the element from S into the empty slot that is preceded by d other empty slots.

Converting successive natural numbers to the factorial number system produces those sequences in lexicographic order (as is the case with any mixed radix number system), and further converting them to permutations preserves the lexicographic ordering, provided the Lehmer code interpretation is used (using inversion tables, one gets a different ordering, where one starts by comparing permutations by the *place* of their entries 1 rather than by the value of their first entries). The sum of the numbers in the factorial number system representation gives the number of inversions of the permutation, and the parity of that sum gives the signature of the permutation. Moreover the positions of the zeroes in the inversion table give the values of left-to-right maxima of the permutation (in the

example 6, 8, 9) while the positions of the zeroes in the Lehmer code are the positions of the right-to-left minima (in the example positions the 4, 8, 9 of the values 1, 2, 5); this allows computing the distribution of such extrema among all permutations. A permutation with Lehmer code d_n, d_{n-1}, ..., d_2, d_1 has an ascent $n - i$ if and only if $d_i \geq d_{i+1}$.

Algorithms to generate permutations

In computing it may be required to generate permutations of a given sequence of values. The methods best adapted to do this depend on whether one wants some randomly chosen permutations, or all permutations, and in the latter case if a specific ordering is required. Another question is whether possible equality among entries in the given sequence is to be taken into account; if so, one should only generate distinct multiset permutations of the sequence.

An obvious way to generate permutations of n is to generate values for the Lehmer code (possibly using the factorial number system representation of integers up to $n!$), and convert those into the corresponding permutations. However, the latter step, while straightforward, is hard to implement efficiently, because it requires n operations each of selection from a sequence and deletion from it, at an arbitrary position; of the obvious representations of the sequence as an array or a linked list, both require (for different reasons) about $n^2/4$ operations to perform the conversion. With n likely to be rather small (especially if generation of all permutations is needed) that is not too much of a problem, but it turns out that both for random and for systematic generation there are simple alternatives that do considerably better. For this reason it does not seem useful, although certainly possible, to employ a special data structure that would allow performing the conversion from Lehmer code to permutation in $O(n \log n)$ time.

Random generation of permutations

For generating random permutations of a given sequence of n values, it makes no difference whether one means apply a randomly selected permutation of n to the sequence, or choose a random element from the set of distinct (multiset) permutations of the sequence. This is because, even though in case of repeated values there can be many distinct permutations of n that result in the same permuted sequence, the number of such permutations is the same for each possible result. Unlike for systematic generation, which becomes unfeasible for large n due to the growth of the number $n!$, there is no reason to assume that n will be small for random generation.

The basic idea to generate a random permutation is to generate at random one of the $n!$ sequences of integers $d_1,d_2,...,d_n$ satisfying $0 \leq d_i < i$ (since d_1 is always zero it may be omitted) and to convert it to a permutation through a bijective correspondence. For the latter correspondence one could interpret the (reverse) sequence as a Lehmer code, and this gives a generation method first published in 1938 by Ronald A. Fisher and Frank Yates. While at the time computer implementation was not an issue, this method suffers from the difficulty sketched above to convert from Lehmer code to permutation efficiently. This can be remedied by using a different bijective correspondence: after using d_i to select an element among i remaining elements of the sequence (for decreasing values of i), rather than removing the element and compacting the sequence by shifting down further elements one place, one swaps the element with the final remaining element. Thus the elements remaining for selection form a consecutive range at each point in time, even though they may not occur in the same order as they did in the original sequence. The mapping from sequence of integers to permutations is somewhat complicated, but it can be seen to produce each permutation in exactly one way, by an immediate induction. When the selected element happens to be the final remaining element, the swap operation can be omitted. This does not occur sufficiently often to warrant testing for the condition, but the final element must be included among the candidates of the selection, to guarantee that all permutations can be generated.

The resulting algorithm for generating a random permutation of $a[0]$, $a[1]$, ..., $a[n - 1]$ can be described as follows in pseudocode:

for i **from** n **downto** 2
do $d_i \leftarrow$ random element of { 0, ..., $i - 1$ }
swap $a[d_i]$ and $a[i - 1]$

This can be combined with the initialization of the array $a[i] = i$ as follows:

for i **from** 0 **to** $n-1$
do $d_{i+1} \leftarrow$ random element of { 0, ..., i }
$a[i] \leftarrow a[d_{i+1}]$
$a[d_{i+1}] \leftarrow i$

If $d_{i+1} = i$, the first assignment will copy an uninitialized value, but the second will overwrite it with the correct value i.

Generation in lexicographic order

There are many ways to systematically generate all permutations of a given sequence. One classical algorithm, which is both simple and flexible, is based on finding the next permutation in lexicographic ordering, if it exists. It can handle repeated values, for which case it generates the distinct multiset permutations each once. Even for ordinary permutations it is significantly more efficient than generating values for the Lehmer code in lexicographic order (possibly using the factorial number system) and converting those to permutations. To use it, one starts by sorting the sequence in (weakly) increasing order (which gives its lexicographically minimal permutation), and then repeats advancing to the next permutation as long as one is found. The method goes back to Narayana Pandita in 14th century India, and has been frequently rediscovered ever since.

The following algorithm generates the next permutation lexicographically after a given permutation. It changes the given permutation in-place.

1. Find the largest index k such that $a[k] < a[k + 1]$. If no such index exists, the permutation is the last permutation.
2. Find the largest index l such that $a[k] < a[l]$.
3. Swap the value of $a[k]$ with that of $a[l]$.
4. Reverse the sequence from $a[k + 1]$ up to and including the final element $a[n]$.

For example, given the sequence [1, 2, 3, 4] which starts in a weakly increasing order, and given that the index is zero-based, the steps are as follows:

1. Index $k = 2$, because 3 is placed at an index that satisfies condition of being the largest index that is still less than *a[k + 1]* which is 4.
2. Index $l = 3$, because 4 is the only value in the sequence that is greater than 3 in order to satisfy the condition *a[k] < a[l]*.
3. The values of *a[2]* and *a[3]* are swapped to form the new sequence [1,2,4,3].
4. The sequence after *k-index a[2]* to the final element is reversed. Because only one value lies after this index (the 3), the sequence remains unchanged in this instance. Thus the lexicographic successor of the initial state is permuted: [1,2,4,3].

Following this algorithm, the next lexicographic permutation will be [1,3,2,4], and the 24th permutation will be [4,3,2,1] at which point *a[k] < a[k + 1]* does not exist, indicating that this is the last permutation.

Generation with minimal changes

An alternative to the above algorithm, the Steinhaus–Johnson–Trotter algorithm, generates an ordering on all the permutations of a given sequence with the property that any two consecutive permutations in its output differ by swapping two adjacent values. This ordering on the permutations was known to 17th-century English bell ringers, among whom it was known as "plain changes". One advantage of this method is that the small amount of change from one permutation to the next allows the method to be implemented in constant time per permutation. The same can also easily generate the subset of even permutations, again in constant time per permutation, by skipping every other output permutation.

Software implementations

Calculator functions

Many scientific calculators and computing software have a built-in function for calculating the number of k-permutations of n.

- Casio and TI calculators: **nPr**
- HP calculators: **PERM**[9]
- Mathematica: **FallingFactorial**

Spreadsheet functions

Most spreadsheet software also provides a built-in function for calculating the number of k-permutations of n, called PERMUT in many popular spreadsheets.

Applications

Permutations are used in the interleaver component of the error detection and correction algorithms, such as turbo codes, for example 3GPP Long Term Evolution mobile telecommunication standard uses these ideas (see 3GPP technical specification 36.212 [10]). Such applications raise the question of fast generation of permutations satisfying certain desirable properties. One of the methods is based on the permutation polynomials.

Notes

[1] N. L. Biggs, *The roots of combinatorics*, Historia Math. 6 (1979) 109–136

[2] http://upload.wikimedia.org/wikipedia/commons/thumb/6/6d/Symmetric_group_4%3B_permutation_list_with_matrices.svg/1000px-Symmetric_group_4%3B_permutation_list_with_matrices.svg.png

[3] Combinatorics of Permutations, ISBN 1-58488-434-7, M. Bóna, 2004, p. 3

[4] Combinatorics of Permutations, ISBN 1-58488-434-7, M. Bóna, 2004, p. 4f

[5] Combinatorics of Permutations, ISBN 1-58488-434-7, M. Bóna, 2004, p. 43

[6] Combinatorics of Permutations, ISBN 1-58488-434-7, M. Bóna, 2004, p. 43ff

[7] D. E. Knuth, *The Art of Computer Programming*, Vol 3, Sorting and Searching, Addison-Wesley (1973), p. 12. This book mentions the Lehmer code (without using that name) as a variant $C_1,...,C_n$ of inversion tables in exercise 5.1.1–7 (p. 19), together with two other variants.

[8] H. A. Rothe, *Sammlung combinatorisch-analytischer Abhandlungen* **2** (Leipzig, 1800), 263–305. Cited in,N. L. Biggs, *The roots of combinatorics*, Historia Math. 6 (1979) 109–136 p. 14.

[9] http://h20331.www2.hp.com/Hpsub/downloads/50gProbability-Rearranging_items.pdf

[10] 3GPP TS 36.212 (http://www.3gpp.org/ftp/Specs/html-info/36212.htm)

References

- Miklós Bóna. "Combinatorics of Permutations", Chapman Hall-CRC, 2004. ISBN 1-58488-434-7.
- Donald Knuth. *The Art of Computer Programming*, Volume 4: *Generating All Tuples and Permutations*, Fascicle 2, first printing. Addison-Wesley, 2005. ISBN 0-201-85393-0.
- Donald Knuth. *The Art of Computer Programming*, Volume 3: *Sorting and Searching*, Second Edition. Addison-Wesley, 1998. ISBN 0-201-89685-0. Section 5.1: Combinatorial Properties of Permutations, pp. 11–72.
- Humphreys, J. F.. *A course in group theory*. Oxford University Press, 1996. ISBN 978-0-19-853459-4

External links

- Hazewinkel, Michiel, ed. (2001), "Permutation" (http://www.encyclopediaofmath.org/index.php?title=p/p072270), *Encyclopedia of Mathematics*, Springer, ISBN 978-1-55608-010-4

Group theory

Algebraic structure → **Group theory**

Group theory

In mathematics and abstract algebra, **group theory** studies the algebraic structures known as groups. The concept of a group is central to abstract algebra: other well-known algebraic structures, such as rings, fields, and vector spaces can all be seen as groups endowed with additional operations and axioms. Groups recur throughout mathematics, and the methods of group theory have strongly influenced many parts of algebra. Linear algebraic groups and Lie groups are two branches of group theory that have experienced tremendous advances and have become subject areas in their own right.

Various physical systems, such as crystals and the hydrogen atom, can be modelled by symmetry groups. Thus group theory and the closely related representation theory have many important applications in physics and chemistry.

One of the most important mathematical achievements of the 20th century[1] was the collaborative effort, taking up more than 10,000 journal pages and mostly published between 1960 and 1980, that culminated in a complete classification of finite simple groups.

History

Group theory has three main historical sources: number theory, the theory of algebraic equations, and geometry. The number-theoretic strand was begun by Leonhard Euler, and developed by Gauss's work on modular arithmetic and additive and multiplicative groups related to quadratic fields. Early results about permutation groups were obtained by Lagrange, Ruffini, and Abel in their quest for general solutions of polynomial equations of high degree. Évariste Galois coined the term "group" and established a connection, now known as Galois theory, between the nascent theory of groups and field theory. In geometry, groups first became important in projective geometry and, later, non-Euclidean geometry. Felix Klein's Erlangen program proclaimed group theory to be the organizing principle of geometry.

Galois, in the 1830s, was the first to employ groups to determine the solvability of polynomial equations. Arthur Cayley and Augustin Louis Cauchy pushed these investigations further by creating the theory of permutation groups. The second historical source for groups stems from geometrical situations. In an attempt to come to grips with possible geometries (such as euclidean, hyperbolic or projective geometry) using group theory, Felix Klein initiated the Erlangen programme. Sophus Lie, in 1884, started using groups (now called Lie groups) attached to analytic problems. Thirdly, groups were (first implicitly and later explicitly) used in algebraic number theory.

The different scope of these early sources resulted in different notions of groups. The theory of groups was unified starting around 1880. Since then, the impact of group theory has been ever growing, giving rise to the birth of abstract algebra in the early 20th century, representation theory, and many more influential spin-off domains. The classification of finite simple groups is a vast body of work from the mid 20th century, classifying all the finite simple groups.

Main classes of groups

The range of groups being considered has gradually expanded from finite permutation groups and special examples of matrix groups to abstract groups that may be specified through a presentation by generators and relations.

Permutation groups

The first class of groups to undergo a systematic study was permutation groups. Given any set X and a collection G of bijections of X into itself (known as *permutations*) that is closed under compositions and inverses, G is a group acting on X. If X consists of n elements and G consists of *all* permutations, G is the symmetric group S_n; in general, any permutation group G is a subgroup of the symmetric group of X. An early construction due to Cayley exhibited any group as a permutation group, acting on itself ($X = G$) by means of the left regular representation.

In many cases, the structure of a permutation group can be studied using the properties of its action on the corresponding set. For example, in this way one proves that for $n \geq 5$, the alternating group A_n is simple, i.e. does not admit any proper normal subgroups. This fact plays a key role in the impossibility of solving a general algebraic equation of degree $n \geq 5$ in radicals.

Matrix groups

The next important class of groups is given by *matrix groups*, or linear groups. Here G is a set consisting of invertible matrices of given order n over a field K that is closed under the products and inverses. Such a group acts on the n-dimensional vector space K^n by linear transformations. This action makes matrix groups conceptually similar to permutation groups, and the geometry of the action may be usefully exploited to establish properties of the group G.

Transformation groups

Permutation groups and matrix groups are special cases of transformation groups: groups that act on a certain space X preserving its inherent structure. In the case of permutation groups, X is a set; for matrix groups, X is a vector space. The concept of a transformation group is closely related with the concept of a symmetry group: transformation groups frequently consist of *all* transformations that preserve a certain structure.

The theory of transformation groups forms a bridge connecting group theory with differential geometry. A long line of research, originating with Lie and Klein, considers group actions on manifolds by homeomorphisms or diffeomorphisms. The groups themselves may be discrete or continuous.

Abstract groups

Most groups considered in the first stage of the development of group theory were "concrete", having been realized through numbers, permutations, or matrices. It was not until the late nineteenth century that the idea of an abstract group as a set with operations satisfying a certain system of axioms began to take hold. A typical way of specifying an abstract group is through a presentation by *generators and relations*,

$$G = \langle S | R \rangle.$$

A significant source of abstract groups is given by the construction of a *factor group*, or quotient group, G/H, of a group G by a normal subgroup H. Class groups of algebraic number fields were among the earliest examples of factor groups, of much interest in number theory. If a group G is a permutation group on a set X, the factor group G/H is no longer acting on X; but the idea of an abstract group permits one not to worry about this discrepancy.

The change of perspective from concrete to abstract groups makes it natural to consider properties of groups that are independent of a particular realization, or in modern language, invariant under isomorphism, as well as the classes of group with a given such property: finite groups, periodic groups, simple groups, solvable groups, and so on. Rather than exploring properties of an individual group, one seeks to establish results that apply to a whole class of groups.

The new paradigm was of paramount importance for the development of mathematics: it foreshadowed the creation of abstract algebra in the works of Hilbert, Emil Artin, Emmy Noether, and mathematicians of their school.[*citation needed*]

Topological and algebraic groups

An important elaboration of the concept of a group occurs if G is endowed with additional structure, notably, of a topological space, differentiable manifold, or algebraic variety. If the group operations m (multiplication) and i (inversion),

$$m : G \times G \to G, (g, h) \mapsto gh, \quad i : G \to G, g \mapsto g^{-1},$$

are compatible with this structure, i.e. are continuous, smooth or regular (in the sense of algebraic geometry) maps then G becomes a topological group, a Lie group, or an algebraic group.[2]

The presence of extra structure relates these types of groups with other mathematical disciplines and means that more tools are available in their study. Topological groups form a natural domain for abstract harmonic analysis, whereas Lie groups (frequently realized as transformation groups) are the mainstays of differential geometry and unitary representation theory. Certain classification questions that cannot be solved in general can be approached and resolved for special subclasses of groups. Thus, compact connected Lie groups have been completely classified. There is a fruitful relation between infinite abstract groups and topological groups: whenever a group Γ can be realized as a lattice in a topological group G, the geometry and analysis pertaining to G yield important results about Γ. A comparatively recent trend in the theory of finite groups exploits their connections with compact topological groups (profinite groups): for example, a single p-adic analytic group G has a family of quotients which are finite p-groups of various orders, and properties of G translate into the properties of its finite quotients.

Combinatorial and geometric group theory

Groups can be described in different ways. Finite groups can be described by writing down the group table consisting of all possible multiplications $g \cdot h$. A more compact way of defining a group is by *generators and relations*, also called the *presentation* of a group. Given any set F of generators $\{g_i\}_{i \in I}$, the free group generated by F surjects onto the group G. The kernel of this map is called subgroup of relations, generated by some subset D. The presentation is usually denoted by $\langle F \mid D \rangle$. For example, the group $\mathbf{Z} = \langle a \mid \rangle$ can be generated by one element a (equal to +1 or −1) and no relations, because $n \cdot 1$ never equals 0 unless n is zero. A string consisting of generator symbols and their inverses is called a *word*.

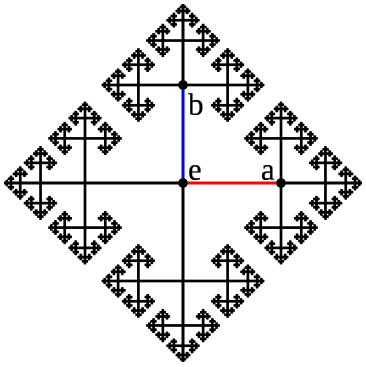
Combinatorial group theory studies groups from the perspective of generators and relations. It is particularly useful where finiteness assumptions are satisfied, for example finitely generated groups, or finitely presented groups (i.e. in addition the relations are finite). The area makes use of the connection of graphs via their fundamental groups. For example, one can show that every subgroup of a free group is free.

There are several natural questions arising from giving a group by its presentation. The *word problem* asks whether two words are effectively the same group element. By relating the problem to Turing machines, one can show that there is in general no algorithm solving this task. Another, generally harder, algorithmically insoluble problem is the group isomorphism problem, which asks whether two groups given by different presentations are actually isomorphic. For example the additive group $\mathbf{Z}$ of integers can also be presented by

$$\langle x, y \mid xyxyx = e \rangle ;$$

it may not be obvious that these groups are isomorphic.[3]

Geometric group theory attacks these problems from a geometric viewpoint, either by viewing groups as geometric objects, or by finding suitable geometric objects a group acts on. The first idea is made precise by means of the Cayley graph, whose vertices correspond to group elements and edges correspond to right multiplication in the group. Given two elements, one constructs the word metric given by the length of the minimal path between the elements. A theorem of Milnor and Svarc then says that given a group G acting in a reasonable manner on a metric space X, for example a compact manifold, then G is quasi-isometric (i.e. looks similar from the far) to the space X.



The Cayley graph of ⟨ x, y | ⟩, the free group of rank 2.

Representation of groups

Saying that a group G *acts* on a set X means that every element defines a bijective map on a set in a way compatible with the group structure. When X has more structure, it is useful to restrict this notion further: a representation of G on a vector space V is a group homomorphism:

$$\varrho : G \to GL(V),$$

where $GL(V)$ consists of the invertible linear transformations of V. In other words, to every group element g is assigned an automorphism $\varrho(g)$ such that $\varrho(g) \circ \varrho(h) = \varrho(gh)$ for any h in G.

This definition can be understood in two directions, both of which give rise to whole new domains of mathematics.[4] On the one hand, it may yield new information about the group G: often, the group operation in G is abstractly given, but via ϱ, it corresponds to the multiplication of matrices, which is very explicit.[5] On the other hand, given a well-understood group acting on a complicated object, this simplifies the study of the object in question. For example, if G is finite, it is known that V above decomposes into irreducible parts. These parts in turn are much more easily manageable than the whole V (via Schur's lemma).

Given a group G, representation theory then asks what representations of G exist. There are several settings, and the employed methods and obtained results are rather different in every case: representation theory of finite groups and representations of Lie groups are two main subdomains of the theory. The totality of representations is governed by the group's characters. For example, Fourier polynomials can be interpreted as the characters of $U(1)$, the group of complex numbers of absolute value *1*, acting on the L^2-space of periodic functions.

Connection of groups and symmetry

Given a structured object X of any sort, a symmetry is a mapping of the object onto itself which preserves the structure. This occurs in many cases, for example

1. If X is a set with no additional structure, a symmetry is a bijective map from the set to itself, giving rise to permutation groups.
2. If the object X is a set of points in the plane with its metric structure or any other metric space, a symmetry is a bijection of the set to itself which preserves the distance between each pair of points (an isometry). The corresponding group is called isometry group of X.
3. If instead angles are preserved, one speaks of conformal maps. Conformal maps give rise to Kleinian groups, for example.
4. Symmetries are not restricted to geometrical objects, but include algebraic objects as well. For instance, the equation

$$x^2 - 3 = 0$$

has the two solutions $+\sqrt{3}$, and $-\sqrt{3}$. In this case, the group that exchanges the two roots is the Galois group belonging to the equation. Every polynomial equation in one variable has a Galois group, that is a certain permutation group on its roots.

The axioms of a group formalize the essential aspects of symmetry. Symmetries form a group: they are closed because if you take a symmetry of an object, and then apply another symmetry, the result will still be a symmetry. The identity keeping the object fixed is always a symmetry of an object. Existence of inverses is guaranteed by undoing the symmetry and the associativity comes from the fact that symmetries are functions on a space, and composition of functions are associative.

Frucht's theorem says that every group is the symmetry group of some graph. So every abstract group is actually the symmetries of some explicit object.

The saying of "preserving the structure" of an object can be made precise by working in a category. Maps preserving the structure are then the morphisms, and the symmetry group is the automorphism group of the object in question.

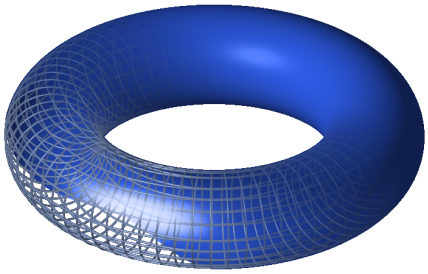
Applications of group theory

Applications of group theory abound. Almost all structures in abstract algebra are special cases of groups. Rings, for example, can be viewed as abelian groups (corresponding to addition) together with a second operation (corresponding to multiplication). Therefore group theoretic arguments underlie large parts of the theory of those entities.

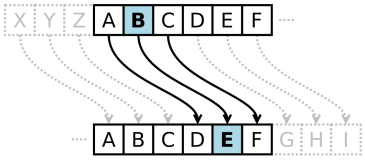
Galois theory uses groups to describe the symmetries of the roots of a polynomial (or more precisely the automorphisms of the algebras generated by these roots). The fundamental theorem of Galois theory provides a link between algebraic field extensions and group theory. It gives an effective criterion for the solvability of polynomial equations in terms of the solvability of the corresponding Galois group. For example, S_5, the symmetric group in 5 elements, is not solvable which implies that the general quintic equation cannot be solved by radicals in the way equations of lower degree can. The theory, being one of the historical roots of group theory, is still fruitfully applied to yield new results in areas such as class field theory.

Algebraic topology is another domain which prominently associates groups to the objects the theory is interested in. There, groups are used to describe certain invariants of topological spaces. They are called "invariants" because they are defined in such a way that they do not change if the space is subjected to some deformation. For example, the fundamental group "counts" how many paths in the space are essentially different. The Poincaré conjecture, proved in 2002/2003 by Grigori Perelman is a prominent application of this idea. The influence is not unidirectional, though. For example, algebraic topology makes use of Eilenberg–MacLane spaces which are spaces with prescribed homotopy groups. Similarly algebraic K-theory stakes in a crucial way on classifying spaces of groups. Finally, the name of the torsion subgroup of an infinite group shows the legacy of topology in group theory.

Algebraic geometry and cryptography likewise uses group theory in many ways. Abelian varieties have been introduced above. The presence of the group operation yields additional information which makes these varieties particularly accessible. They also often serve as a test for new conjectures.[6] The one-dimensional case, namely elliptic curves is studied in particular detail. They are both theoretically and practically intriguing.[7] Very large groups of prime order constructed in Elliptic-Curve Cryptography serve for public key cryptography. Cryptographical methods of this kind benefit from the flexibility of the geometric objects, hence their group structures, together with the complicated structure of these groups, which make the discrete logarithm very hard to calculate. One of the earliest encryption protocols, Caesar's cipher, may also be interpreted as a (very easy) group operation. In another direction, toric varieties are algebraic varieties acted on by a torus. Toroidal embeddings have recently led to advances in algebraic geometry, in particular resolution of singularities.



A torus. Its abelian group structure is induced from the map $\mathbf{C} \to \mathbf{C}/\mathbf{Z}+\tau\mathbf{Z}$, where τ is a parameter living in the upper half plane.



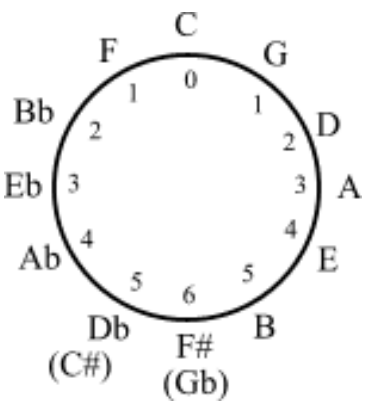
The cyclic group $\mathbf{Z}_{26}$ underlies Caesar's cipher.

Algebraic number theory is a special case of group theory, thereby following the rules of the latter. For example, Euler's product formula

$$\sum_{n\geq 1} \frac{1}{n^s} = \prod_{p \text{ prime}} \frac{1}{1-p^{-s}}$$

captures the fact that any integer decomposes in a unique way into primes. The failure of this statement for more general rings gives rise to class groups and regular primes, which feature in Kummer's treatment of Fermat's Last Theorem.

- The concept of the Lie group (named after mathematician Sophus Lie) is important in the study of differential equations and manifolds; they describe the symmetries of continuous geometric and analytical structures. Analysis on these and other groups is called harmonic analysis. Haar measures, that is integrals invariant under the translation in a Lie group, are used for pattern recognition and other image processing techniques.
- In combinatorics, the notion of permutation group and the concept of group action are often used to simplify the counting of a set of objects; see in particular Burnside's lemma.
- The presence of the 12-periodicity in the circle of fifths yields applications of elementary group theory in musical set theory.
- In physics, groups are important because they describe the symmetries which the laws of physics seem to obey. According to Noether's theorem, every continuous symmetry of a physical system corresponds to a conservation law of the system. Physicists are very interested in group representations, especially of Lie groups, since these representations often point the way to the "possible" physical theories. Examples of the use of groups in physics include the Standard Model, gauge theory, the Lorentz group, and the Poincaré group.



The circle of fifths may be endowed with a cyclic group structure

- In chemistry and materials science, groups are used to classify crystal structures, regular polyhedra, and the symmetries of molecules. The assigned point groups can then be used to determine physical properties (such as polarity and chirality), spectroscopic properties (particularly useful for Raman spectroscopy and infrared spectroscopy), and to construct molecular orbitals.

Notes

[1] * Elwes, Richard, " An enormous theorem: the classification of finite simple groups, (http://plus.maths.org/issue41/features/elwes/index.html)" *Plus Magazine*, Issue 41, December 2006.

[2] This process of imposing extra structure has been formalized through the notion of a group object in a suitable category. Thus Lie groups are group objects in the category of differentiable manifolds and affine algebraic groups are group objects in the category of affine algebraic varieties.

[3] Writing , one has

[4] Such as group cohomology or equivariant K-theory.

[5] In particular, if the representation is faithful.

[6] For example the Hodge conjecture (in certain cases).

[7] See the Birch-Swinnerton-Dyer conjecture, one of the millennium problems

References

- Borel, Armand (1991), *Linear algebraic groups*, Graduate Texts in Mathematics **126** (2nd ed.), Berlin, New York: Springer-Verlag, ISBN 978-0-387-97370-8, MR 1102012 (http://www.ams.org/mathscinet-getitem?mr=1102012)
- Carter, Nathan C. (2009), *Visual group theory* (http://web.bentley.edu/empl/c/ncarter/vgt/), Classroom Resource Materials Series, Mathematical Association of America, ISBN 978-0-88385-757-1, MR 2504193 (http://www.ams.org/mathscinet-getitem?mr=2504193)
- Cannon, John J. (1969), "Computers in group theory: A survey", *Communications of the Association for Computing Machinery* **12**: 3–12, doi: 10.1145/362835.362837 (http://dx.doi.org/10.1145/362835.362837), MR 0290613 (http://www.ams.org/mathscinet-getitem?mr=0290613)
- Frucht, R. (1939), "Herstellung von Graphen mit vorgegebener abstrakter Gruppe" (http://www.numdam.org/numdam-bin/fitem?id=CM_1939__6__239_0), *Compositio Mathematica* **6**: 239–50, ISSN 0010-437X (http://www.worldcat.org/issn/0010-437X)
- Golubitsky, Martin; Stewart, Ian (2006), "Nonlinear dynamics of networks: the groupoid formalism", *Bull. Amer. Math. Soc. (N.S.)* **43** (03): 305–364, doi: 10.1090/S0273-0979-06-01108-6 (http://dx.doi.org/10.1090/S0273-0979-06-01108-6), MR 2223010 (http://www.ams.org/mathscinet-getitem?mr=2223010) Shows the advantage of generalising from group to groupoid.
- Judson, Thomas W. (1997), *Abstract Algebra: Theory and Applications* (http://abstract.ups.edu) An introductory undergraduate text in the spirit of texts by Gallian or Herstein, covering groups, rings, integral domains, fields and Galois theory. Free downloadable PDF with open-source GFDL license.
- Kleiner, Israel (1986), "The evolution of group theory: a brief survey", *Mathematics Magazine* **59** (4): 195–215, doi: 10.2307/2690312 (http://dx.doi.org/10.2307/2690312), ISSN 0025-570X (http://www.worldcat.org/issn/0025-570X), JSTOR 2690312 (http://www.jstor.org/stable/2690312), MR 863090 (http://www.ams.org/mathscinet-getitem?mr=863090)
- La Harpe, Pierre de (2000), *Topics in geometric group theory*, University of Chicago Press, ISBN 978-0-226-31721-2
- Livio, M. (2005), *The Equation That Couldn't Be Solved: How Mathematical Genius Discovered the Language of Symmetry*, Simon & Schuster, ISBN 0-7432-5820-7 Conveys the practical value of group theory by explaining how it points to symmetries in physics and other sciences.
- Mumford, David (1970), *Abelian varieties*, Oxford University Press, ISBN 978-0-19-560528-0, OCLC 138290 (http://www.worldcat.org/oclc/138290)

- Ronan M., 2006. *Symmetry and the Monster*. Oxford University Press. ISBN 0-19-280722-6. For lay readers. Describes the quest to find the basic building blocks for finite groups.
- Rotman, Joseph (1994), *An introduction to the theory of groups*, New York: Springer-Verlag, ISBN 0-387-94285-8 A standard contemporary reference.
- Schupp, Paul E.; Lyndon, Roger C. (2001), *Combinatorial group theory*, Berlin, New York: Springer-Verlag, ISBN 978-3-540-41158-1
- Scott, W. R. (1987) [1964], *Group Theory*, New York: Dover, ISBN 0-486-65377-3 Inexpensive and fairly readable, but somewhat dated in emphasis, style, and notation.
- Shatz, Stephen S. (1972), *Profinite groups, arithmetic, and geometry*, Princeton University Press, ISBN 978-0-691-08017-8, MR 0347778 (http://www.ams.org/mathscinet-getitem?mr=0347778)
- Weibel, Charles A. (1994), *An introduction to homological algebra*, Cambridge Studies in Advanced Mathematics **38**, Cambridge University Press, ISBN 978-0-521-55987-4, OCLC 36131259 (http://www.worldcat.org/oclc/36131259), MR 1269324 (http://www.ams.org/mathscinet-getitem?mr=1269324)

External links

- History of the abstract group concept (http://www-history.mcs.st-andrews.ac.uk/history/HistTopics/Abstract_groups.html)
- Higher dimensional group theory (http://www.bangor.ac.uk/r.brown/hdaweb2.htm) This presents a view of group theory as level one of a theory which extends in all dimensions, and has applications in homotopy theory and to higher dimensional nonabelian methods for local-to-global problems.
- Plus teacher and student package: Group Theory (http://plus.maths.org/issue48/package/index.html) This package brings together all the articles on group theory from *Plus*, the online mathematics magazine produced by the Millennium Mathematics Project at the University of Cambridge, exploring applications and recent breakthroughs, and giving explicit definitions and examples of groups.
- US Naval Academy group theory guide (http://www.usna.edu/Users/math/wdj/tonybook/gpthry/node1.html) A general introduction to group theory with exercises written by Tony Gaglione.

Permutation group

Algebraic structure → **Group theory**

Group theory

In mathematics, a **permutation group** is a group G whose elements are permutations of a given set M, and whose group operation is the composition of permutations in G (which are thought of as bijective functions from the set M to itself); the relationship is often written as (G,M). Note that the group of *all* permutations of a set is the symmetric group; the term *permutation group* is usually restricted to mean a subgroup of the symmetric group. The symmetric group of n elements is denoted by S_n; if M is any finite or infinite set, then the group of all permutations of M is often written as Sym(M).

The application of a permutation group to the elements being permuted is called its group action; it has applications in both the study of symmetries, combinatorics and many other branches of mathematics, physics and chemistry.

Closure properties

As a subgroup of a symmetric group, all that is necessary for a permutation group to satisfy the group axioms is that it contain the identity permutation, the inverse permutation of each permutation it contains, and be closed under composition of its permutations. A general property of finite groups implies that a finite nonempty subset of a symmetric group is again a group if and only if it is closed under the group operation.

Examples

Permutations are often written in *cyclic form*[1] so that given the set $M = \{1,2,3,4\}$, a permutation g of M with $g(1) = 2$, $g(2) = 4$, $g(4) = 1$ and $g(3) = 3$ will be written as (1,2,4)(3), or more commonly, (1,2,4) since 3 is left unchanged; if the objects are denoted by a single letter or digit, commas are also dispensed with, and we have a notation such as (1 2 4).

Consider the following set G of permutations of the set $M = \{1,2,3,4\}$:

- e = (1)(2)(3)(4)= (1)[2][3]
  - This is the identity, the trivial permutation which fixes each element.
- a = (1 2)(3)(4) = (1 2)
  - This permutation interchanges 1 and 2, and fixes 3 and 4.
- b = (1)(2)(3 4) = (3 4)
  - Like the previous one, but exchanging 3 and 4, and fixing the others.
- ab = (1 2)(3 4)
  - This permutation, which is the composition of the previous two, exchanges simultaneously 1 with 2, and 3 with 4.

G forms a group, since $aa = bb = e$, $ba = ab$, and $baba = e$. So (G,M) forms a permutation group.

The Rubik's Cube puzzle is another example of a permutation group. The underlying set being permuted is the coloured subcubes of the whole cube. Each of the rotations of the faces of the cube is a permutation of the positions and orientations of the subcubes. Taken together, the rotations form a generating set, which in turn generates a group by composition of these rotations. The axioms of a group are easily seen to be satisfied; to invert any sequence of rotations, simply perform their opposites, in reverse order.

The group of permutations on the Rubik's Cube does not form a complete symmetric group of the 20 corner and face cubelets; there are some final cube positions which cannot be achieved through the legal manipulations of the cube.

More generally, *every* group G is isomorphic to a subgroup of a permutation group by virtue of its regular action on G as a set; this is the content of Cayley's theorem.

Isomorphisms

If G and H are two permutation groups on the same set X, then we say that G and H are *isomorphic as permutation groups* if there exists a bijective map $f : X \to X$ such that $r \mapsto f^{-1}$ o r o f defines a bijective map between G and H; in other words, if for each element g in G, there is a unique h_g in H such that for all x in X, $(g \text{ o } f)(x) = (f \text{ o } h_g)(x)$. This is equivalent to G and H being conjugate as subgroups of *Sym(X)*. In this case, G and H are also isomorphic as groups.

Notice that different permutation groups may well be isomorphic as abstract groups, but not as permutation groups. For instance, the permutation group on {1,2,3,4} described above is isomorphic as a group (but not as a permutation group) to {(1)(2)(3)(4), (12)(34), (13)(24), (14)(23)}. Both are isomorphic as groups to the Klein group V_4.

Transpositions, simple transpositions, inversions and sorting

A 2-cycle is known as a transposition. A *simple transposition* in S_n is a 2-cycle of the form $(i \;\; i+1)$.

For a permutation p in S_n, a pair $(i\ , j) \in I_n$ is a *permutation inversion*, if when $i<j$, we have $p(i) > p(j)$.[4]

Every permutation can be written as a product of simple transpositions; furthermore, the number of simple transpositions one can write a permutation p in S_n can be the number of inversions of p and if the number of inversions in p is odd or even the number of transpositions in p will also be odd or even corresponding to the oddness of p.

Notes

[1] e.g. during cycle index computations

[2] This is just a notation that is often used

[3] Math Circle- Berkeley: Application of Groups to Solve Rubik's Cube (http://mathcircle.berkeley.edu/BMC3/perm/node3.html)

[4] Weisstein, Eric W. "Permutation Inversion." From MathWorld--A Wolfram Web Resource. http://mathworld.wolfram.com/PermutationInversion.html

References

- John D. Dixon and Brian Mortimer. *Permutation Groups*. Number 163 in Graduate Texts in Mathematics. Springer-Verlag, 1996.
- Akos Seress. *Permutation group algorithms*. Cambridge Tracts in Mathematics, 152. Cambridge University Press, Cambridge, 2003.
- Meenaxi Bhattacharjee, Dugald Macpherson, Rögnvaldur G. Möller and Peter M. Neumann. *Notes on Infinite Permutation Groups*. Number 1698 in Lecture Notes in Mathematics. Springer-Verlag, 1998.
- Hazewinkel, Michiel, ed. (2001), "Permutation group" (http://www.encyclopediaofmath.org/index.php?title=p/p072280), *Encyclopedia of Mathematics*, Springer, ISBN 978-1-55608-010-4
- Alexander Hulpke. GAP Data Library "Transitive Permutation Groups" (http://www.gap-system.org/Datalib/trans.html).
- Peter J. Cameron. *Permutation Groups*. LMS Student Text 45. Cambridge University Press, Cambridge, 1999.
- Peter J. Cameron. *Oligomorphic Permutation Groups*. Cambridge University Press, Cambridge, 1990.

Article Sources and Contributors

Permutation *Source*: http://en.wikipedia.org/w/index.php?oldid=573696348 *Contributors*: .:Ajvol:., A. B., A. Pichler, Aaronchall, Abhishekbh, Aboctok, Alansohn, Albert0168, Alexander Chervov, AlphaPyro, Altenmann, Andre Engels, Angela, Anita5192, Anna1609, Anonymous Dissident, Archelon, Armend, Arved, AxelBoldt, AzaToth, B-Con, BRG, Beland, BenRG, Bender235, Bender2k14, Bhatele, Bhound89, Bigblackdad, Bkumartvm, Blokhead, Bongwarrior, Boothy443, Borgx, Burn, Bus stop, CBM, CRGreathouse, Callanecc, Captpossum, Charles Matthews, ChevyC, Chris the speller, Citizen Premier, Ck lostsword, Classicalecon, CoderHoop, Constructive editor, Conversion script, CountingPine, Courcelles, Cullinane, Curmi, Damian Yerrick, Daonguyen95, David Eppstein, Dcoetzee, Delldot, DerHexer, Desertsky85451, Dickguertin, Dicklyon, Dkasak, Dmcq, Dominus, DoubleAW, DoubleBlue, Dratman, Dreadstar, Dreftymac, Dubhe.sk, Dysprosia, Eco2009, Ed g2s, Edaelon, Elwikipedista, Emperorbma, Eric119, Eusebio42, Evercat, Exercisephys, Extransit, FF2010, Fabiform, Faisal.akeel, Fresheneesz, Galoisprotege, Garde, Geekygator, Gerbrant, GianlucaCiccarelli, Giftlite, Goochelaar, Graeme Bartlett, Graham87, Guy Harris, Haham hanuka, Haipa Doragon, Happy-melon, Hariva, Hedgehog83, Helder.wiki, Hfastedge, Ht686rg90, Hyacinth, Hydrogen Iodide, I dream of horses, Iainscott, Ideyal, Ih8evilstuff, ImperatorExercitus, Insanity Incarnate, InverseHypercube, Ionescuac, J.delanoy, JEzratty, JackSchmidt, Jason Quinn, Jeff G., Jesse V., Jlaire, Jlau521, Joel B. Lewis, JoergenB, John Chamberlain, John wesley, Johnteslade, JonathLee, Jonpro, Jonverve, Joshk, K0rq, KSmrq, Kruusamägi, LOL, Lambiam, Lantonov, Leen Droogendijk, Lemmon Juice, LilHelpa, Linas, LingLingJ, Lunkwill, MFH, MSGJ, Mabuhelwa, Macrakis, Manik762007, Manscher, Marc van Leeuwen, Masterflex, Mate2code, Materialscientist, MaxEnt, Memming, Memodude, Mesoderm, Michael Hardy, Michael Slone, Michael.Pohoreski, Migvnk, Mikez302, Mindmatrix, Minimac, Mmccoo, Mojo Hand, Moondyne, Mxn, NOrbeck, NYKevin, Nbarth, Newportm, Nightkey, Nikai, Nishantsah, Nissanskyline923, Nk, Nolaiz, Nonette, NuclearWarfare, Obradovic Goran, Octahedron80, Oleg Alexandrov, Omnipaedista, Oobopshark, Patrick, Paul August, Pecunia, Pfortuny, Pgoyal13, Phil.a, Philip Trueman, Pikiwyn, Policron, Poor Yorick, Preslethe, Profvk, R. J. Mathar, Ravibodake, ResearchRave, Revolver, Romanm, Saippuakauppias, Samikc, Sdornan, Sggsayan93, Shadowjams, Simetrical, Slady, Solarapex, Stevenj, Stone Pastor, Sun Creator, Super-real dance, Svick, Technochocolate, Tenth Plague, Terrek, The Anome, TheBendster, Tide rolls, Timwi, Tjclutten, Tlroche, Tocharianne, Tom harrison, Tom jgg, Tonymaric, Tosha, Trusilver, Tsujigiri, Upendedappender, Vanished user psdfiwnef3niurunfiuh234ruhfwdb7, Victor M. Vicente Selvas, Vince Vatter, Wavelength, Wikidrone, Wikimachine, Wshun, Wzwz, Zero0000, 391 anonymous edits

Group theory *Source*: http://en.wikipedia.org/w/index.php?oldid=569899631 *Contributors*: Adan, Adgjdghjdety, Alberto da Calvairate, Ale jrb, Alksentrs, Alpha Beta Epsilon, Andreas Carter, Arcfrk, Archie Paulson, ArnoldReinhold, ArzelaAscoli, Auclairde, Avouac, AxelBoldt, Baccyak4H, Bevo, Bhuna71, BiT, Bogdangiusca, Bongwarrior, Boulaur, Brad7777, CRGreathouse, Calcio33, Cate, Cessator, Charles Matthews, Chris Pressey, Christopherodonovan, Chun-hian, Ciro.santilli, Cmbankester, ComplexZeta, CountingPine, Crasshopper, CsDix, Cwitty, CàlculIntegral, D stankov, D15724C710N, DYLAN LENNON, David Callan, David Eppstein, Davipo, Dcljr, Debator of mathematics, Dennis Estenson II, Doshell, Dratman, Drschawrz, Dysprosia, Eakirkman, Eamonster, EchoBravo, Edward, Edwinconnell, Eubulides, FT2, Favonian, Fibonacci, Finlay McWalter, Fluffernutter, Fly by Night, Friviere, GBL, Gabriel Kielland, Gandalf61, Giftlite, Gombang, Googl, Graeme Bartlett, Gregbard, Gromlakh, Grubber, H00kwurm, HMSSolent, Hairy Dude, Hamtechperson, Hans Adler, Hard Sin, Headbomb, HenryLi, Hillman, Hyacinth, Ijgt, Indeed123, Ivan Štambuk, J.delanoy, JWSchmidt, JackSchmidt, Jaimedv, Jakob.scholbach, Jauhienij, JinJian, Jitse Niesen, JohnBlackburne, Jordi Burguet Castell, Josh Parris, Julia W, Justin W Smith, KF, Karl-Henner, Kmg90, Kranix, Kristine8, Kwantus, Lambiam, Laxfan1977, Lemonaftertaste, Lfh, LiDaobing, Lightmouse, Ligulem, Lord Roem, Luqui, M cuffa, MTC, MaEr, Magmi, Manuel Trujillo Berges, Masv, Mate2code, MathMartin, Mayooranathan, Meclee, Melchoir, Merlincooper, Messagetolove, Michael Hardy, Michael Slone, Mike Fikes, Mspraveen, NERIUM, Nadav1, Natebarney, Ngyikp, NobillyT, Obradovic Goran, OdedSchramm, Orhanghazi, Padicgroup, Palapa, Papadopc, Paul August, Peter Stalin, PeterPearson, Petter Strandmark, Philip Trueman, Phys, Pieter Kuiper, Pilotguy, Poor Yorick, R.e.b., Ranveig, Recentchanges, Reedy, Rich Farmbrough, Richard L. Peterson, Rifleman 82, Rjwilmsi, RobHar, Romanm, RonnieBrown, Rossami, Rune.welsh, Rursus, Salix alba, Scullin, Seaphoto, Shishir332, SomeRandomPerson23, Sławomir Biały, Tbsmith, The Anome, Tide rolls, Tigershrike, TimothyRias, Tommy2010, Tompw, Treisijs, Tyskis, Useight, Utopianheaven, V8rik, Vegetator, VictorAnyakin, Viskonsas, WVhybrid, Willtron, WinoWeritas, Wshun, Xylthixlm, Yger, Zundark, Μυρμηγκάκι, 171 anonymous edits

Permutation group *Source*: http://en.wikipedia.org/w/index.php?oldid=540212596 *Contributors*: 01001, Albmont, Andreask, AxelBoldt, CBM, CRGreathouse, Calle, Ceradon, Charles Matthews, Chas zzz brown, Conversion script, CsDix, Cullinane, Deltabeignet, Derek Ross, Dj3500, Dominus, Ducnm, Dysprosia, Giftlite, Goochelaar, Graham87, Grestrepo, Hadal, Inkling, JackSchmidt, Jason Quinn, Jonas Kölker, Kostmo, Krasnoludek, Linas, Michael Hardy, Michael Slone, Nickhann, Pako, Patrick, Policron, Pratik.mallya, R.e.b., RA0808, Radicalt, Salix alba, SlamDiego, Sniffnoy, Stefan Kohl, Sławomir Biały, Tong, Unco, Wik, Zahlentheorie, 26 anonymous edits

Image Sources, Licenses and Contributors

File:Permutations RGB.svg *Source*: http://en.wikipedia.org/w/index.php?title=File:Permutations_RGB.svg *License*: Public Domain *Contributors*: Lipedia

File:Permutations with repetition.svg *Source*: http://en.wikipedia.org/w/index.php?title=File:Permutations_with_repetition.svg *License*: Public Domain *Contributors*: Mate2code

File:Symmetric group 3; Cayley table; matrices.svg *Source*: http://en.wikipedia.org/w/index.php?title=File:Symmetric_group_3;_Cayley_table;_matrices.svg *License*: Public Domain *Contributors*: User:Mate2code

Image:Cayley graph of F2.svg *Source*: http://en.wikipedia.org/w/index.php?title=File:Cayley_graph_of_F2.svg *License*: Public Domain *Contributors*: User:Dbenbenn

Image:Torus.png *Source*: http://en.wikipedia.org/w/index.php?title=File:Torus.png *License*: Public Domain *Contributors*: LucasVB, Rimshot, SharkD

Image:Caesar3.svg *Source*: http://en.wikipedia.org/w/index.php?title=File:Caesar3.svg *License*: Public Domain *Contributors*: Cepheus

Image:Fifths.png *Source*: http://en.wikipedia.org/w/index.php?title=File:Fifths.png *License*: GNU Free Documentation License *Contributors*: Hyacinth, Jtir, Tó campos1, Wst, 1 anonymous edits

License

Creative Commons Attribution-Share Alike 3.0 Unported
//creativecommons.org/licenses/by-sa/3.0/