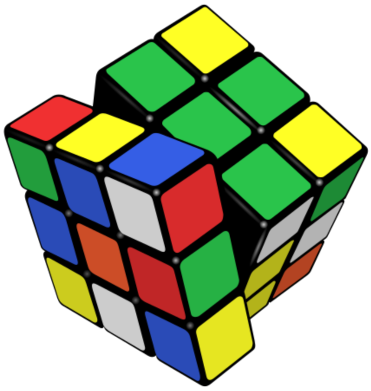
Permutation group

From Wikipedia, the free encyclopedia

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 group of *all* permutations of a set *M* is the symmetric group of *M*, often written as Sym(*M*).[1] The term *permutation group* thus means a subgroup of the symmetric group. If *M* = {1,2,...,*n*} then, Sym(*M*), the *symmetric group on n letters* is usually denoted by S_n.

The way in which the elements of a permutation group permute the elements of the set is called its group action. Group actions have applications in the study of symmetries, combinatorics and many other branches of mathematics, physics and chemistry.

Contents



The popular puzzle Rubik's cube invented in 1974 by Ernő Rubik has been used as an illustration of permutation groups. Each rotation of a layer of the cube results in a permutation of the surface colors and is a member of the group. The permutation group of the cube is called the Rubik's cube group.

Basic properties and terminology

Being a subgroup of a symmetric group, all that is necessary for a set of permutations to satisfy the group axioms and be a permutation group is that it contain the identity permutation, the inverse permutation of each permutation it contains, and be closed under composition of its permutations.[2] 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.[3]

The **degree** of a group of permutations of a finite set is the number of elements in the set. The **order** of a group (of any type) is the number of elements (cardinality) in the group. By Lagrange's theorem, the order of any finite permutation group of degree *n* must divide *n*! (*n*-factorial, the order of the symmetric group S_n).

Notation

Since permutations are bijections of a set, they can be represented by Cauchy's *two-line notation*.[4] This notation lists each of the elements of *M* in the first row, and for each element, its image under the permutation below it in the second row. If σ is a permutation of the set $M = \{x_1, x_2, \ldots, x_n\}$ then,

$$\sigma = \begin{pmatrix} x_1 & x_2 & x_3 & \cdots & x_n \\ \sigma(x_1) & \sigma(x_2) & \sigma(x_3) & \cdots & \sigma(x_n) \end{pmatrix}.$$

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 *σ*(1)=2, *σ*(2)=5, *σ*(3)=4, *σ*(4)=3, and *σ*(5)=1. The elements of *M* need not appear in any special order in the first row. This permutation could also be written as:

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

Permutations are also often written in cyclic notation (*cyclic form*)[5] 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 single letters or digits, commas and spaces can also be dispensed with, and we have a notation such as (124). The permutation written above in 2-line notation would be written in cyclic notation as $\sigma = (125)(34).$

Composition of permutations–the group product

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, [6] [7] because of the way function application is written. Some authors prefer the leftmost factor acting first, [8] [9] [10] but to that end permutations must be written to the *right* of their argument, often as an exponent, so the permutation σ acting on the element x results in the image x^{σ}. With this convention, the product is given by $x^{\sigma\cdot\pi} = (x^{\sigma})^{\pi}$. However, this gives a *different* rule for multiplying permutations. This convention is commonly used in the permutation group literature, but this article uses the convention 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. In two-line notation, the product of two permutations is obtained by rearranging the columns of the second (leftmost) permutation so that its first row is identical with the second row of the first (rightmost) permutation. The product can then be written as the first row of the first permutation over the second row of the modified second permutation. For example, given the permutations,

$$P = \begin{pmatrix} 1 & 2 & 3 & 4 & 5 \\ 2 & 4 & 1 & 3 & 5 \end{pmatrix} \quad \text{and} \quad Q = \begin{pmatrix} 1 & 2 & 3 & 4 & 5 \\ 5 & 4 & 3 & 2 & 1 \end{pmatrix},$$

the product QP is:

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

The composition of permutations, when they are written in cyclic form, is obtained by juxtaposing the two permutations (with the second one written on the left) and then simplifying to a disjoint cycle form if desired. Thus, in cyclic notation the above product would be given by:

$$Q \cdot P = (15)(24) \cdot (1243) = (1435).$$

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 two or more 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 dots of the previous example were added for emphasis).

Neutral element and inverses

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

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

In cyclic notation, $e = (1)(2)(3)...(n)$ which by convention is also denoted by just (1) or even ().[11]

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

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

To obtain the inverse of a single cycle, we reverse the order of its elements. Thus,

$$(125)^{-1} = (521) = (152).$$

To obtain the inverse of a product of cycles, we first reverse the order of the cycles, and then we take the inverse of each as above. Thus,

$$[(125)(34)]^{-1} = (34)^{-1}(125)^{-1} = (43)(521) = (34)(152).$$

Having an associative product, an identity element, and inverses for all its elements, makes the set of all permutations of *M* into a group, Sym(*M*); a permutation group.

Examples

Consider the following set G_1 of permutations of the set *M* = {1,2,3,4}:

- *e* = (1)(2)(3)(4)= (1)
  - 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_1 forms a group, since *aa* = *bb* = *e*, *ba* = *ab*, and *abab* = *e*. This permutation group is isomorphic, as an abstract group, to the Klein group V_4.

As another example consider the group of symmetries of a square. Let the vertices of a square be labeled 1, 2, 3 and 4 (counterclockwise around the square starting with 1 in the top left corner). The symmetries are determined by the images of the vertices, that can, in turn, be described by permutations. The rotation by 90° (counterclockwise) about the center of the square is described by the permutation (1234). The 180° and 270° rotations are given by (13)(24) and (1432), respectively. The reflection about the horizontal line through the center is given by (12)(34) and the corresponding vertical line reflection is (14)(23). The reflection about the 1,3−diagonal line is (24) and reflection about the 2,4−diagonal is (13). The only remaining symmetry is the identity (1)(2)(3)(4). This permutation group is abstractly known as the dihedral group of order 8.

Group actions

In the above example of the symmetry group of a square, the permutations "describe" the movement of the vertices of the square induced by the group of symmetries. It is common to say that these group elements are "acting" on the set of vertices of the square. This idea can be made precise by formally defining a **group action**.[12]

Let *G* be a group and *M* a nonempty set. An **action** of *G* on *M* is a function *f*: *G* × *M* → *M* such that

- $f(1, x) = x$, for all *x* in *M* (1 is the identity (neutral) element of the group *G*), and
- $f(g, f(h, x)) = f(gh, x)$, for all *g*,*h* in *G* and all *x* in *M*.

This last condition can also be expressed as saying that the action induces a group homomorphism from *G* into *Sym*(*M*).[12] Any such homomorphism is called a *(permutation) representation* of *G* on *M*.

For any permutation group, the action that sends $(g, x) \to g(x)$ is called the **natural action** of *G* on *M*. This is the action that is assumed unless otherwise indicated.[12] In the example of the symmetry group of the square, the group's action on the set of vertices is the natural action. However, this group also induces an action on the set of four triangles in the square, which are: t_1 = 234, t_2 = 134, t_3 = 124 and t_4 = 123. It also acts on the two diagonals: d_1 = 13 and d_2 = 24.

Group element	Action on triangles	Action on diagonals
(1)	(1)	(1)
(1234)	$(t_1\ t_2\ t_3\ t_4)$	$(d_1\ d_2)$
(13)(24)	$(t_1\ t_3)(t_2\ t_4)$	(1)
(1432)	$(t_1\ t_4\ t_3\ t_2)$	$(d_1\ d_2)$
(12)(34)	$(t_1\ t_2)(t_3\ t_4)$	$(d_1\ d_2)$
(14)(23)	$(t_1\ t_4)(t_2\ t_3)$	$(d_1\ d_2)$
(13)	$(t_1\ t_3)$	(1)
(24)	$(t_2\ t_4)$	(1)

Cayley's theorem

Any group G can act on itself (the elements of the group being thought of as the set M) in many ways. In particular, there is a regular action given by (left) multiplication in the group. That is, $f(g, x) = gx$ for all g and x in G. For each fixed g, the function $f_g(x) = gx$ is a bijection on G and therefore a permutation of the "set" G. Each element of G can be thought of as a permutation in this way and so, G is isomorphic to a permutation group; this is the content of Cayley's theorem.

Consider the group G_1 acting on the set {1,2,3,4} given above. Let the elements of this group be denoted by e, a, b and $c = ab = ba$. The action of G_1 on itself described in Cayley's theorem gives the following permutation representation:

$$f_e \mapsto (e)(a)(b)(c)$$
$$f_a \mapsto (ea)(bc)$$
$$f_b \mapsto (eb)(ac)$$
$$f_c \mapsto (ec)(ab).$$

Permutation isomorphic groups

If G and H are two permutation groups on sets X and Y with actions f_1 and f_2 respectively, then we say that G and H are *permutation isomorphic* (*isomorphic as permutation groups*) if there exists a bijective map $\lambda : X \to Y$ and a group isomorphism $\psi : G \to H$ such that:[13]

$$\lambda(f_1(g, x)) = f_2(\psi(g), \lambda(x)) \text{ for all } g \text{ in } G \text{ and } x \text{ in } X.$$

If $X = Y$ this is equivalent to G and H being conjugate as subgroups of Sym(X).[14] The special case where $G = H$ and ψ is the identity map gives rise to the concept of *equivalent actions* of a group.[15]

In the example of the symmetries of a square given above, the natural action on the set {1,2,3,4} is equivalent to the action on the triangles. The bijection λ between the sets is given by $i \mapsto t_i$. The natural action of group G_1 above and its action on itself (via left multiplication) are not equivalent as the natural action has fixed points and the second action does not.

History

The study of groups originally grew out of an understanding of permutation groups.[16] Permutations had themselves been intensively studied by Lagrange in 1770 in his work on the algebraic solutions of polynomial equations. This subject flourished and by the mid 19th century a well-developed theory of permutation groups existed, codified by Camille Jordan in his book *Traité des Substitutions et des Équations Algébriques* of 1870. Jordan's book was, in turn, based on the papers that were left by Évariste Galois in 1832.

When Cayley introduced the concept of an abstract group, it was not immediately clear whether or not this was a larger collection of objects than the known permutation groups (which had a definition different from the modern one). Cayley went on to prove that the two concepts were equivalent in Cayley's theorem.[17]

Another classical text containing several chapters on permutation groups is Burnside's *Theory of Groups of Finite Order* of 1911.[18] The first half of the twentieth century was a fallow period in the study of group theory in general, but interest in permutation groups was revived in the 1950s by H. Wielandt whose German lecture notes were reprinted as *Finite Permutation Groups* in 1964.[19]

See also

- Rank 3 permutation group
- Primitive group
- Oligomorphic group

Notes

1. The notations $\mathbf{S}_M$ and $\mathbf{S}^M$ are also used.
2. Rotman 2006, p. 148, Definition of subgroup
3. Rotman 2006, p. 149, Proposition 2.69
4. Wussing, Hans (2007), *The Genesis of the Abstract Group Concept: A Contribution to the History of the Origin of Abstract Group Theory* (https://books.google.com/books?id=Xp3JymnfAq4C&pg=PA94), Courier Dover Publications, p. 94, ISBN 9780486458687, "Cauchy used his permutation notation—in which the arrangements are written one below the other and both are enclosed in parentheses—for the first time in 1815."
5. especially when the algebraic properties of the permutation are of interest.

6. Biggs, Norman L.; White, A. T. (1979). *Permutation groups and combinatorial structures*. Cambridge University Press. ISBN 0-521-22287-7.
7. Rotman 2006, p. 107 – note especially the footnote on this page.
8. Dixon & Mortimer 1996, p. 3 – see the comment following Example 1.2.2
9. Cameron, Peter J. (1999). *Permutation groups*. Cambridge University Press. ISBN 0-521-65302-9.
10. Jerrum, M. (1986). "A compact representation of permutation groups". *J. Algor*. **7** (1): 60–78. doi:10.1016/0196-6774(86)90038-6 (https://doi.org/10.1016%2F0196-6774%2886%2990038-6).
11. Rotman 2006, p. 108
12. Dixon & Mortimer 1996, p. 5
13. Dixon & Mortimer 1996, p. 17
14. Dixon & Mortimer 1996, p. 18
15. Cameron 1994, p. 228
16. Dixon & Mortimer 1996, p. 28
17. Cameron 1994, p. 226
18. Burnside, William (1955) [1911], *Theory of Groups of Finite Order* (2nd ed.), Dover
19. Wielandt, H. (1964), *Finite Permutation Groups*, Academic Press

References

- Cameron, Peter J. (1994), *Combinatorics: Topics, Techniques, Algorithms*, Cambridge University Press, ISBN 0-521-45761-0
- Dixon, John D.; Mortimer, Brian (1996), *Permutation Groups*, Graduate Texts in Mathematics 163), Springer-Verlag, ISBN 0-387-94599-7
- Rotman, Joseph J. (2006), *A First Course in Abstract Algebra with Applications* (3rd ed.), Pearson Prentice-Hall, ISBN 0-13-186267-7

Further reading

- 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.
- 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.

External links

- Hazewinkel, Michiel, ed. (2001) [1994], "Permutation group" (https://www.encyclopediaofmath.org/index.php?title=p/p072280), *Encyclopedia of Mathematics*, Springer Science+Business Media B.V. / Kluwer Academic Publishers, ISBN 978-1-55608-010-4
- Alexander Hulpke. GAP Data Library "Transitive Permutation Groups" (http://www.gap-system.org/Datalib/trans.html).

Retrieved from "https://en.wikipedia.org/w/index.php?title=Permutation_group&oldid=768281016"