Monoid

For the object in category theory, see Monoid (category theory).
Not to be confused with monad.

In abstract algebra, a branch of mathematics, a **monoid** is an algebraic structure with a single associative binary operation and an identity element. Monoids are studied in semigroup theory as they are semigroups with identity. Monoids occur in several branches of mathematics; for instance, they can be regarded as categories with a single object. Thus, they capture the idea of function composition within a set. Monoids are also commonly used in computer science, both in its foundational aspects and in practical programming. The set of strings built from a given set of characters is a free monoid. The transition monoid and syntactic monoid are used in describing finite state machines, whereas trace monoids and history monoids provide a foundation for process calculi and concurrent computing. Some of the more important results in the study of monoids are the Krohn–Rhodes theorem and the star height problem. The history of monoids, as well as a discussion of additional general properties, are found in the article on semigroups.

1 Definition

Suppose that S is a set and • is some binary operation $S \times S \to S$, then S with • is a **monoid** if it satisfies the following two axioms:

Associativity For all a, b and c in S, the equation $(a \bullet b) \bullet c = a \bullet (b \bullet c)$ holds.

Identity element There exists an element e in S such that for every element a in S, the equations $e \bullet a = a \bullet e = a$ hold.

In other words, a monoid is a semigroup with an identity element. It can also be thought of as a magma with associativity and identity. The identity element of a monoid is unique.[1] A monoid in which each element has an inverse is a group.

Depending on the context, the symbol for the binary operation may be omitted, so that the operation is denoted by juxtaposition; for example, the monoid axioms may be written $(ab)c = a(bc)$ and $ea = ae = a$. This notation does not imply that it is numbers being multiplied.

2 Monoid structures

2.1 Submonoids

A **submonoid** of a monoid $(M, \bullet)$ is a subset N of M that is closed under the monoid operation and contains the identity element e of M.[2][3] Symbolically, N is a submonoid of M if $N \subseteq M$, $x \bullet y \in N$ whenever x, $y \in N$, and $e \in N$. N is thus a monoid under the binary operation inherited from M.

2.2 Generators

A subset S of M is said to be a **generator** of M if M is the smallest set containing S that is closed under the monoid operation, or equivalently M is the result of applying the finitary closure operator to S. If there is a generator of M that has finite cardinality, then M is said to be **finitely generated**. Not every set S will generate a monoid, as the generated structure may lack an identity element.

2.3 Commutative monoid

A monoid whose operation is commutative is called a **commutative monoid** (or, less commonly, an **abelian monoid**). Commutative monoids are often written additively. Any commutative monoid is endowed with its **algebraic** preordering $\leq$, defined by $x \leq y$ if there exists z such that $x + z = y$.[4] An **order-unit** of a commutative monoid M is an element u of M such that for any element x of M, there exists a positive integer n such that $x \leq nu$. This is often used in case M is the positive cone of a partially ordered abelian group G, in which case we say that u is an order-unit of G.

2.4 Partially commutative monoid

A monoid for which the operation is commutative for some, but not all elements is a trace monoid; trace monoids commonly occur in the theory of concurrent computation.

3 Examples

- Out of the 16 possible binary Boolean operators, each of the four that has a two sided identity is

also commutative and associative and thus makes the set {False, True} a commutative monoid. Under the standard definitions, AND and XNOR have the identity True while XOR and OR have the identity False. The monoids from AND and OR are also idempotent while those from XOR and XNOR are not.

- The natural numbers, **N**, form a commutative monoid under addition (identity element zero), or multiplication (identity element one). A submonoid of **N** under addition is called a numerical monoid.

- The positive integers, **N** \ {0}, form a commutative monoid under multiplication (identity element one).

- Given a set A, all subsets of A form a commutative monoid under intersection operation (identity element is A itself).

- Given a set A, all subsets of A form a commutative monoid under union operation (identity element is the empty set).

- Generalizing the previous example, every bounded semilattice is an idempotent commutative monoid.

  - In particular, any bounded lattice can be endowed with both a meet- and a join- monoid structure. The identity elements are the lattice's top and its bottom, respectively. Being lattices, Heyting algebras and Boolean algebras are endowed with these monoid structures.

- Every singleton set {x} closed under a binary operation • forms the trivial (one-element) monoid, which is also the trivial group.

- Every group is a monoid and every abelian group a commutative monoid.

- Any semigroup S may be turned into a monoid simply by adjoining an element e not in S and defining $e • s = s = s • e$ for all $s \in S$. This conversion of any semigroup to the monoid is done by the free functor between the category of semigroups and the category of monoids.[5]

  - Thus, an idempotent monoid (sometimes known as *find-first*) may be formed by adjoining an identity element e to the left zero semigroup over a set S. The opposite monoid (sometimes called *find-last*) is formed from the right zero semigroup over S.

    - Adjoin an identity e to the left-zero semigroup with two elements {lt; gt}. Then the resulting idempotent monoid {lt; e; gt} models the lexicographical order of a sequence given the orders of its elements, with e representing equality.

- The elements of any unital ring, with addition or multiplication as the operation.

  - The integers, rational numbers, real numbers or complex numbers, with addition or multiplication as operation.[6]

  - The set of all n by n matrices over a given ring, with matrix addition or matrix multiplication as the operation.

- The set of all finite strings over some fixed alphabet Σ forms a monoid with string concatenation as the operation. The empty string serves as the identity element. This monoid is denoted Σ^* and is called the **free monoid** over Σ.

- Given any monoid M, the *opposite monoid* M^{op} has the same carrier set and identity element as M, and its operation is defined by $x •^{op} y = y • x$. Any commutative monoid is the opposite monoid of itself.

- Given two sets M and N endowed with monoid structure (or, in general, any finite number of monoids, M_1, ..., Mk), their cartesian product $M \times N$ is also a monoid (respectively, $M_1 \times ... \times Mk$). The associative operation and the identity element are defined pairwise.[7]

- Fix a monoid M. The set of all functions from a given set to M is also a monoid. The identity element is a constant function mapping any value to the identity of M; the associative operation is defined pointwise.

- Fix a monoid M with the operation • and identity element e, and consider its power set $P(M)$ consisting of all subsets of M. A binary operation for such subsets can be defined by $S • T = \{ s • t : s \in S, t \in T \}$. This turns $P(M)$ into a monoid with identity element {e}. In the same way the power set of a group G is a monoid under the product of group subsets.

- Let S be a set. The set of all functions $S \to S$ forms a monoid under function composition. The identity is just the identity function. It is also called the **full transformation monoid** of S. If S is finite with n elements, the monoid of functions on S is finite with n^n elements.

- Generalizing the previous example, let C be a category and X an object in C. The set of all endomorphisms of X, denoted End$C(X)$, forms a monoid under composition of morphisms. For more on the relationship between category theory and monoids see below.

- The set of homeomorphism classes of compact surfaces with the connected sum. Its unit element is the class of the ordinary 2-sphere. Furthermore, if a denotes the class of the torus, and b denotes the class of the projective plane, then every element c of the

monoid has a unique expression the form $c = na + mb$ where n is the integer ≥ 0 and $m = 0, 1,$ or 2. We have $3b = a + b$.

- Let $\langle f \rangle$ be a cyclic monoid of order n, that is, $\langle f \rangle = \{f^0, f^1, \ldots, f^{n-1}\}$. Then $f^n = f^k$ for some $0 \leq k < n$. In fact, each such k gives a distinct monoid of order n, and every cyclic monoid is isomorphic to one of these.

Moreover, f can be considered as a function on the points $\{0, 1, 2, \ldots, n - 1\}$ given by

$$\begin{bmatrix} 0 & 1 & 2 & \ldots & n-2 & n-1 \\ 1 & 2 & 3 & \ldots & n-1 & k \end{bmatrix}$$

or, equivalently

$$f(i) := \begin{cases} i + 1, & \text{if } 0 \leq i < n - 1 \\ k, & \text{if } i = n - 1. \end{cases}$$

Multiplication of elements in $\langle f \rangle$ is then given by function composition.

Note also that when $k = 0$ then the function f is a permutation of $\{0, 1, 2, \ldots, n - 1\}$ and gives the unique cyclic group of order n.

4 Properties

In a monoid, one can define positive integer powers of an element x : $x^1 = x$, and $x^n = x \bullet \ldots \bullet x$ (n times) for $n > 1$. The rule of powers $x^{n + p} = x^n \bullet x^p$ is obvious.

From the definition of a monoid, one can show that the identity element e is unique. Then, for any x, one can set $x^0 = e$ and the rule of powers is still true with nonnegative exponents.

It is possible to define invertible elements: an element x is called invertible if there exists an element y such that $x \bullet y = e$ and $y \bullet x = e$. The element y is called the inverse of x. If y and z are inverses of x, then by associativity $y = (zx)y = z(xy) = z$. Thus inverses, if they exist, are unique.[8]

If y is the inverse of x, one can define negative powers of x by setting $x^{-1} = y$ and $x^{-n} = y \bullet \ldots \bullet y$ (n times) for $n > 1$. And the rule of exponents is still verified for all n, p rational integers. This is why the inverse of x is usually written x^{-1}. The set of all invertible elements in a monoid M, together with the operation $\bullet$, forms a group. In that sense, every monoid contains a group (possibly only the trivial group consisting of only the identity).

However, not every monoid sits inside a group. For instance, it is perfectly possible to have a monoid in which two elements a and b exist such that $a \bullet b = a$ holds even though b is not the identity element. Such a monoid cannot be embedded in a group, because in the group we

could multiply both sides with the inverse of a and would get that $b = e$, which isn't true. A monoid $(M, \bullet)$ has the cancellation property (or is cancellative) if for all a, b and c in M, $a \bullet b = a \bullet c$ always implies $b = c$ and $b \bullet a = c \bullet a$ always implies $b = c$. A commutative monoid with the cancellation property can always be embedded in a group via the Grothendieck construction. That is how the additive group of the integers (a group with operation +) is constructed from the additive monoid of natural numbers (a commutative monoid with operation + and cancellation property). However, a non-commutative cancellative monoid need not be embeddable in a group.

If a monoid has the cancellation property and is *finite*, then it is in fact a group. Proof: Fix an element x in the monoid. Since the monoid is finite, $x^n = x^m$ for some $m > n > 0$. But then, by cancellation we have that $x^{m-n} = e$ where e is the identity. Therefore, $x \bullet x^{m-n-1} = e$, so x has an inverse.

The right- and left-cancellative elements of a monoid each in turn form a submonoid (i.e. obviously include the identity and not so obviously are closed under the operation). This means that the cancellative elements of any commutative monoid can be extended to a group.

It turns out that requiring the cancellative property in a monoid is not required to perform the Grothendieck construction – commutativity is sufficient. However, if the original monoid has an absorbing element then its Grothendieck group is the trivial group. Hence the homomorphism is, in general, not injective.

An **inverse monoid** is a monoid where for every a in M, there exists a unique a^{-1} in M such that $a = a \bullet a^{-1} \bullet a$ and $a^{-1} = a^{-1} \bullet a \bullet a^{-1}$. If an inverse monoid is cancellative, then it is a group.

In the opposite direction, a **zerosumfree monoid** is an additively written monoid in which $a + b = 0$ implies that $a = 0$ and $b = 0$:[9] equivalently, that no element other than zero has an additive inverse.
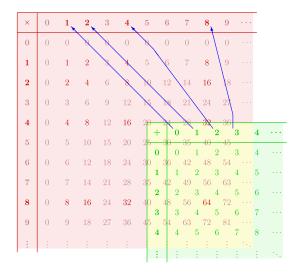
5 Acts and operator monoids

Main article: monoid act

Let M be a monoid, with the binary operation denoted by $\bullet$ and the identity element denoted by e. Then a (left) **M-act** (or left act over M) is a set X together with an operation $\cdot : M \times X \to X$ which is compatible with the monoid structure as follows:

- for all x in X: $e \cdot x = x$;

- for all a, b in M and x in X: $a \cdot (b \cdot x) = (a \bullet b) \cdot x$.

This is the analogue in monoid theory of a (left) group action. Right M-acts are defined in a similar way.

A monoid with an act is also known as an **operator monoid**. Important examples include transition systems of semiautomata. A transformation semigroup can be made into an operator monoid by adjoining the identity transformation.

6 Monoid homomorphisms

Example monoid homomorphism x ↦ 2ˣ from (N, +, 0) to (N, ×, 1). It is injective, but not surjective.

A homomorphism between two monoids $(M, *)$ and $(N, \bullet)$ is a function $f : M \to N$ such that

- $f(x * y) = f(x) \bullet f(y)$ for all x, y in M

- $f(eM) = eN$,

where eM and eN are the identities on M and N respectively. Monoid homomorphisms are sometimes simply called **monoid morphisms**.

Not every semigroup homomorphism is a monoid homomorphism, since it may not map the identity to the identity of the target monoid, even though the element it maps the identity to will be an identity of the image of the mapping. In contrast, a semigroup homomorphisms between groups is always a group homomorphism, as it necessarily preserves the identity. Since for monoids this isn't always true, it is necessary to state this as a separate requirement.

A bijective monoid homomorphism is called a monoid isomorphism. Two monoids are said to be isomorphic if there is a monoid isomorphism between them.

7 Equational presentation

Main article: Presentation of a monoid

Monoids may be given a **presentation**, much in the same way that groups can be specified by means of a group presentation. One does this by specifying a set of generators Σ, and a set of relations on the free monoid Σ^*. One does this by extending (finite) binary relations on Σ^* to monoid congruences, and then constructing the quotient monoid, as above.

Given a binary relation $R \subset \Sigma^* \times \Sigma^*$, one defines its symmetric closure as $R \cup R^{-1}$. This can be extended to a symmetric relation $E \subset \Sigma^* \times \Sigma^*$ by defining $x \sim_E y$ if and only if $x = sut$ and $y = svt$ for some strings u, v, s, $t \in \Sigma^*$ with $(u,v) \in R \cup R^{-1}$. Finally, one takes the reflexive and transitive closure of E, which is then a monoid congruence.

In the typical situation, the relation R is simply given as a set of equations, so that $R = \{u_1 = v_1, \cdots, u_n = v_n\}$. Thus, for example,

$$\langle p, q \mid pq = 1 \rangle$$

is the equational presentation for the bicyclic monoid, and

$$\langle a, b \mid aba = baa, bba = bab \rangle$$

is the plactic monoid of degree 2 (it has infinite order). Elements of this plactic monoid may be written as $a^i b^j (ba)^k$ for integers i, j, k, as the relations show that ba commutes with both a and b.

8 Relation to category theory

Monoids can be viewed as a special class of categories. Indeed, the axioms required of a monoid operation are exactly those required of morphism composition when restricted to the set of all morphisms whose source and target is a given object.[10] That is,

> *A monoid is, essentially, the same thing as a category with a single object.*

More precisely, given a monoid $(M, \bullet)$, one can construct a small category with only one object and whose morphisms are the elements of M. The composition of morphisms is given by the monoid operation $\bullet$.

Likewise, monoid homomorphisms are just functors between single object categories.[10] So this construction gives an equivalence between the category of (small) monoids **Mon** and a full subcategory of the category of (small) categories **Cat**. Similarly, the category of groups is equivalent to another full subcategory of **Cat**.

In this sense, category theory can be thought of as an extension of the concept of a monoid. Many definitions and

theorems about monoids can be generalised to small categories with more than one object. For example, a quotient of a category with one object is just a quotient monoid.

Monoids, just like other algebraic structures, also form their own category, **Mon**, whose objects are monoids and whose morphisms are monoid homomorphisms.[10]

There is also a notion of monoid object which is an abstract definition of what is a monoid in a category. A monoid object in **Set** is just a monoid.

9 Monoids in computer science

In computer science, many abstract data types can be endowed with a monoid structure. In a common pattern, a sequence of elements of a monoid is "folded" or "accumulated" to produce a final value. For instance, many iterative algorithms need to update some kind of "running total" at each iteration; this pattern may be elegantly expressed by a monoid operation. Alternatively, the associativity of monoid operations ensures that the operation can be parallelized by employing a prefix sum or similar algorithm, in order to utilize multiple cores or processors efficiently.

Given a sequence of values of type M with identity element ε and associative operation $*$, the *fold* operation is defined as follows:

$$\text{fold} : M^* \to M = l \mapsto \begin{cases} \varepsilon & \text{if } l = \text{nil} \\ m * \text{fold}\, l' & \text{if } l = \text{cons}\, m\, l' \end{cases}$$

In addition, any data structure can be 'folded' in a similar way, given a serialization of its elements. For instance, the result of "folding" a binary tree might differ depending on pre-order vs. post-order tree traversal.

10 Complete monoids

A **complete monoid** is a commutative monoid equipped with an infinitary sum operation Σ_I for any index set I such that:[11][12][13][14]

$$\sum_{i \in \emptyset} m_i = 0; \quad \sum_{i \in \{j\}} m_i = m_j; \quad \sum_{i \in \{j,k\}} m_i = m_j + m_k \quad \text{for } j \neq k$$

and

$$\sum_{j \in J} \sum_{i \in I_j} m_i = \sum_{i \in I}(m_i) \text{ if } \bigcup_{j \in J} I_j = I \text{ and } I_j \cap I_{j'} = \emptyset \text{ for } j \neq j'$$

A **continuous monoid** is an ordered commutative monoid in which every directed set has a least upper bound compatible with the monoid operation:

$$a + \sup S = \sup(a + S).$$

These two concepts are closely related: a continuous

monoid is a complete monoid in which the infinitary sum may be defined as

$$\sum_I a_i = \sup \sum_E a_i$$

where the supremum on the right runs over all finite subsets E of I and each sum on the right is a finite sum in the monoid.[14]

11 See also

- Green's relations
- Monad (functional programming)
- Semiring and Kleene algebra
- Star height problem
- Vedic square

12 Notes

[1] If both e_1 and e_2 satisfy the above equations, then $e_1 = e_1 \bullet e_2 = e_2$.

[2] Jacobson (2009)

[3] Some authors omit the requirement that a submonoid must contain the identity element from its definition, requiring only that it have *an* identity element, which can be distinct from that of *M*.

[4] Gondran, Michel; Minoux, Michel (2008). *Graphs, Dioids and Semirings: New Models and Algorithms*. Operations Research/Computer Science Interfaces Series **41**. Dordrecht: Springer-Verlag. p. 13. ISBN 978-0-387-75450-5. Zbl 1201.16038.

[5] Rhodes, John; Steinberg, Benjamin (2009), *The q-theory of Finite Semigroups: A New Approach*, Springer Monographs in Mathematics **71**, Springer, p. 22, ISBN 9780387097817.

[6] Jacobson (2009), p. 29, examples 1, 2, 4 & 5.

[7] Jacobson (2009), p. 35

[8] Jacobson, I.5. p. 22

[9] Wehrung, Friedrich (1996). "Tensor products of structures with interpolation". *Pacific Journal of Mathematics* **176** (1): 267–285. Zbl 0865.06010.

[10] Awodey, Steve (2006). *Category Theory*. Oxford Logic Guides **49**. Oxford University Press. p. 10. ISBN 0-19-856861-4. Zbl 1100.18001.

[11] Droste, M., & Kuich, W. (2009). Semirings and Formal Power Series. *Handbook of Weighted Automata*, 3–28. doi:10.1007/978-3-642-01492-5_1, pp. 7-10

[12] Hebisch, Udo (1992). "Eine algebraische Theorie un-
     endlicher Summen mit Anwendungen auf Halbgruppen
     und Halbringe". *Bayreuther Mathematische Schriften* (in
     German) **40**: 21–152. Zbl 0747.08005.

[13] Kuich, Werner (1990). "ω-continuous semirings, alge-
     braic systems and pushdown automata". In Paterson,
     Michael S. *Automata, Languages and Programming: 17th
     International Colloquium, Warwick University, England,
     July 16-20, 1990, Proceedings*. Lecture Notes in Com-
     puter Science **443**. Springer-Verlag. pp. 103–110. ISBN
     3-540-52826-1.

[14] Kuich, Werner (2011). "Algebraic systems and pushdown
     automata". In Kuich, Werner. *Algebraic foundations in
     computer science. Essays dedicated to Symeon Bozapalidis
     on the occasion of his retirement*. Lecture Notes in Com-
     puter Science **7020**. Berlin: Springer-Verlag. pp. 228–
     256. ISBN 978-3-642-24896-2. Zbl 1251.68135.

13   References

- Howie, John M. (1995), *Fundamentals of Semi-
  group Theory*, London Mathematical Society Mono-
  graphs. New Series **12**, Oxford: Clarendon Press,
  ISBN 0-19-851194-9, Zbl 0835.20077

- Jacobson, Nathan (1951), *Lectures in Abstract Al-
  gebra* **I**, D. Van Nostrand Company, ISBN 0-387-
  90122-1

- Jacobson, Nathan (2009), *Basic algebra* **1** (2nd ed.),
  Dover, ISBN 978-0-486-47189-1

- Kilp, Mati; Knauer, Ulrich; Mikhalev, Alexander V.
  (2000), *Monoids, acts and categories. With applica-
  tions to wreath products and graphs. A handbook for
  students and researchers*, de Gruyter Expositions in
  Mathematics **29**, Berlin: Walter de Gruyter, ISBN
  3-11-015248-7, Zbl 0945.20036

- Lothaire, M. (1997), *Combinatorics on words*, En-
  cyclopedia of Mathematics and Its Applications
  17, Perrin, D.; Reutenauer, C.; Berstel, J.; Pin,
  J. E.; Pirillo, G.; Foata, D.; Sakarovitch, J.; Si-
  mon, I.; Schützenberger, M. P.; Choffrut, C.; Cori,
  R.; Lyndon, Roger; Rota, Gian-Carlo. Foreword
  by Roger Lyndon (2nd ed.), Cambridge University
  Press, doi:10.1017/CBO9780511566097, ISBN 0-
  521-59924-5, MR 1475463, Zbl 0874.20040

14   External links

- Hazewinkel, Michiel, ed.   (2001), "Monoid",
  Encyclopedia of Mathematics, Springer, ISBN 978-
  1-55608-010-4

- Weisstein, Eric W., "Monoid", *MathWorld*.

- Monoid at PlanetMath.org.

15 Text and image sources, contributors, and licenses

15.1 Text

- **Monoid** *Source:* https://en.wikipedia.org/wiki/Monoid?oldid=697159443 *Contributors:* Damian Yerrick, AxelBoldt, Brion VIBBER, Bryan Derksen, Zundark, XJaM, Ben-Zin~enwiki, Mjb, Youandme, Michael Hardy, Andres, Ideyal, Revolver, Charles Matthews, Dysprosia, GPHemsley, Robbot, Fredrik, Mattblack82, Fuelbottle, Anthony, Tobias Bergemann, SimonMayer, Giftlite, Fropuff, Cambyses, Li-Daobing, MarkSweep, Kusunose, Gauss, Smimram, El C, Robotje, Obradovic Goran, Msh210, Phi beta, Oleg Alexandrov, Linas, Dionyziz, Graham87, SixWingedSeraph, Chenxlee, Salix alba, Vlad Patryshev, VKokielov, YurikBot, Hairy Dude, Michael Slone, Grubber, Gaius Cornelius, Trovatore, Mikeblas, Bota47, Reyk, Netrapt, Jsnx, BiT, Cybercobra, DRLB, Jack Daw, Djinnit, Antonielly, TooMuchMath, Rschwieb, LDH, StephenBuxton, CRGreathouse, Simian1k, Rawling, Cydebot, Gogo Dodo, Pascal.Tesson, Thijs!bot, Oerjan, Hannes Eder, Salgueiro~enwiki, Magioladitis, Dosboot, Jakob.scholbach, David Eppstein, JaGa, Gentlestone, Kimse, Fruits Monster, Daniel5Ko, GaborLajos, Policron, Potatoswatter, Deadspirit90, VolkovBot, TXiKiBoT, Geometry guy, Fwehrung, AlleborgoBot, SieBot, Thehotelambush, Jorgen W, Classicalecon, Mr. Granger, Paulsavala, Daveagp, Alexbot, He7d3r, Beroal, Pichpich, Addbot, Tjlaxs, Download, AndersBot, Luckas-bot, Yobot, Ptbotgourou, Pcap, Nallimbot, AnomieBOT, Ciphers, Datandrews, FrescoBot, DrilBot, Pinethicket, Ebony Jackson, Chaecker, Asharsultan, Jesse V., Chharvey, Quondum, Jcubic, ChuispastonBot, ClueBot NG, Niehren, HazelAB, Helpful Pixie Bot, Beaumont877, Wikihelperhelper, Brad7777, Nadapez~enwiki, Deltahedron, Mansour.cs, Jochen Burghardt, Mark viking, CsDix, Oh Goes the Waterholes, Soujak, JMP EAX, JJMC89 and Anonymous: 70

15.2 Images

- **File:Exponentiation_as_monoid_homomorphism_svg.svg** *Source:* https://upload.wikimedia.org/wikipedia/commons/a/a3/Exponentiation_as_monoid_homomorphism_svg.svg *License:* CC BY-SA 3.0 *Contributors:* Own work *Original artist:* Jochen Burghardt

15.3 Content license