Module (mathematics)

In abstract algebra, the concept of a **module** over a ring is a generalization of the notion of vector space, wherein the corresponding scalars are allowed to lie in an arbitrary ring. Modules also generalize the notion of abelian groups, which are modules over the ring of integers.

Thus, a module, like a vector space, is an additive abelian group; a product is defined between elements of the ring and elements of the module, and this multiplication is associative (when used with the multiplication in the ring) and distributive.

Modules are very closely related to the representation theory of groups. They are also one of the central notions of commutative algebra and homological algebra, and are used widely in algebraic geometry and algebraic topology.

Motivation

In a vector space, the set of scalars forms a field and acts on the vectors by scalar multiplication, subject to certain axioms such as the distributive law. In a module, the scalars need only be a ring, so the module concept represents a significant generalization. In commutative algebra, it is important that both ideals and quotient rings are modules, so that many arguments about ideals or quotient rings can be combined into a single argument about modules. In non-commutative algebra the distinction between left ideals, ideals, and modules becomes more pronounced, though some important ring theoretic conditions can be expressed either about left ideals or left modules.

Much of the theory of modules consists of extending as many as possible of the desirable properties of vector spaces to the realm of modules over a "well-behaved" ring, such as a principal ideal domain. However, modules can be quite a bit more complicated than vector spaces; for instance, not all modules have a basis, and even those that do, free modules, need not have a unique rank if the underlying ring does not satisfy the invariant basis number condition, unlike vector spaces which always have a basis whose cardinality is then unique (assuming the axiom of choice).

Formal definition

A **left *R*-module** *M* over the ring *R* consists of an abelian group (*M*, +) and an operation $R \times M \to M$ (called *scalar multiplication*, usually just written by juxtaposition, i.e. as *rx* for *r* in *R* and *x* in *M*) such that

For all *r*,*s* in *R*, *x*,*y* in *M*, we have

1. $r(x+y) = rx + ry$
2. $(r+s)x = rx + sx$
3. $(rs)x = r(sx)$
4. $1_R x = x$ if *R* has multiplicative identity 1_R.

If one writes the scalar action as f_r so that $f_r(x) = rx$, and *f* for the map which takes each *r* to its corresponding map f_r, then the first axiom states that every f_r is a group homomorphism of *M*, and the other three axioms assert that *f* is a ring homomorphism from *R* to the endomorphism ring End(*M*). Thus a module is a ring action on an abelian group (cf. group action). In this sense, module theory generalizes representation theory, which deals with group actions on vector spaces, or equivalently group ring actions.

Usually, we simply write "a left *R*-module *M*" or $_RM$. A **right *R*-module** *M* or M_R is defined similarly, only the ring acts on the right, i.e. we have a scalar multiplication of the form $M \times R \to M$, and the above axioms are written with scalars *r* and *s* on the right of *x* and *y*.

(Authors who do not require rings to be unital omit condition 4 above in the definition of an *R*-module, and so would call the structures defined above "unital left *R*-modules". In this article, consistent with the glossary of ring theory, all rings and modules are assumed to be unital.)

A bimodule is a module which is a left module and a right module such that the two multiplications are compatible.

If R is commutative, then left R-modules are the same as right R-modules and are simply called R-modules.

Examples

- If K is a field, then the concepts "K-vector space" (a vector space over K) and K-module are identical.
- The concept of a **Z**-module agrees with the notion of an abelian group. That is, every abelian group is a module over the ring of integers **Z** in a unique way. For $n > 0$, let $nx = x + x + ... + x$ (n summands), $0x = 0$, and $(-n)x = -(nx)$. Such a module need not have a basis—groups containing torsion elements do not. (For example, in the group of integers modulo 3, one cannot find even one element which satisfies the definition of a linearly independent set since when an integer such as 3 or 6 multiplies an element the result is 0. However if a finite field is considered as a module over the same finite field taken as a ring, it is a vector space and does have a basis.)
- If R is any ring and n a natural number, then the cartesian product R^n is both a left and a right module over R if we use the component-wise operations. Hence when $n = 1$, R is an R-module, where the scalar multiplication is just ring multiplication. The case $n = 0$ yields the trivial R-module $\{0\}$ consisting only of its identity element. Modules of this type are called free and if R has invariant basis number (e.g. any commutative ring or field) the number n is then the rank of the free module.
- If S is a nonempty set, M is a left R-module, and M^S is the collection of all functions $f : S \to M$, then with addition and scalar multiplication in M^S defined by $(f + g)(s) = f(s) + g(s)$ and $(rf)(s) = rf(s)$, M^S is a left R-module. The right R-module case is analogous. In particular, if R is commutative then the collection of *R-module homomorphisms* $h : M \to N$ (see below) is an R-module (and in fact a *submodule* of N^M).
- If X is a smooth manifold, then the smooth functions from X to the real numbers form a ring $C^\infty(X)$. The set of all smooth vector fields defined on X form a module over $C^\infty(X)$, and so do the tensor fields and the differential forms on X. More generally, the sections of any vector bundle form a projective module over $C^\infty(X)$, and by Swan's theorem, every projective module is isomorphic to the module of sections of some bundle; the category of $C^\infty(X)$-modules and the category of vector bundles over X are equivalent.
- The square n-by-n matrices with real entries form a ring R, and the Euclidean space $\mathbf{R}^n$ is a left module over this ring if we define the module operation via matrix multiplication.
- If R is any ring and I is any left ideal in R, then I is a left module over R. Analogously of course, right ideals are right modules.
- If R is a ring, we can define the ring R^{op} which has the same underlying set and the same addition operation, but the opposite multiplication: if $ab = c$ in R, then $ba = c$ in R^{op}. Any *left* R-module M can then be seen to be a *right* module over R^{op}, and any right module over R can be considered a left module over R^{op}.

Submodules and homomorphisms

Suppose M is a left R-module and N is a subgroup of M. Then N is a **submodule** (or R-submodule, to be more explicit) if, for any n in N and any r in R, the product $r\,n$ is in N (or nr for a right module).

The set of submodules of a given module M, together with the two binary operations + and $\cap$, forms a lattice which satisfies the **modular law**: Given submodules U, N_1, N_2 of M such that $N_1 \subset N_2$, then the following two submodules are equal: $(N_1 + U) \cap N_2 = N_1 + (U \cap N_2)$.

If M and N are left R-modules, then a map $f : M \to N$ is a **homomorphism of *R*-modules** if, for any m, n in M and r, s in R,

$$f(rm + sn) = rf(m) + sf(n)$$

This, like any homomorphism of mathematical objects, is just a mapping which preserves the structure of the objects. Another name for a homomorphism of modules over R is an R-linear map.

A bijective module homomorphism is an isomorphism of modules, and the two modules are called *isomorphic*. Two isomorphic modules are identical for all practical purposes, differing solely in the notation for their elements.

The kernel of a module homomorphism $f : M \to N$ is the submodule of M consisting of all elements that are sent to zero by f. The isomorphism theorems familiar from groups and vector spaces are also valid for R-modules.

The left R-modules, together with their module homomorphisms, form a category, written as R-**Mod**. This is an abelian category.

Types of modules

Finitely generated. A module M is finitely generated if there exist finitely many elements $x_1,...,x_n$ in M such that every element of M is a linear combination of those elements with coefficients from the scalar ring R.

Cyclic module. A module is called a cyclic module if it is generated by one element.

Free. A free module is a module that has a basis, or equivalently, one that is isomorphic to a direct sum of copies of the scalar ring R. These are the modules that behave very much like vector spaces.

Projective. Projective modules are direct summands of free modules and share many of their desirable properties.

Injective. Injective modules are defined dually to projective modules.

Flat. A module is called flat if taking the tensor product of it with any exact sequence preserves exactness.

Simple. A simple module S is a module that is not $\{0\}$ and whose only submodules are $\{0\}$ and S. Simple modules are sometimes called *irreducible*.[1]

Indecomposable. An indecomposable module is a non-zero module that cannot be written as a direct sum of two non-zero submodules. Every simple module is indecomposable.

Faithful. A faithful module M is one where the action of each $r \neq 0$ in R on M is nontrivial (i.e. $rx \neq 0$ for some x in M). Equivalently, the annihilator of M is the zero ideal.

Noetherian. A Noetherian module is a module such that every submodule is finitely generated. Equivalently, every increasing chain of submodules becomes stationary after finitely many steps.

Artinian. An Artinian module is a module in which every decreasing chain of submodules becomes stationary after finitely many steps.

Graded. A graded module is a module decomposable as a direct sum $M = \oplus_x M_x$ over a graded ring $R = \oplus_x R_x$ such that $R_x M_y \subset M_{x+y}$ for all x and y.

Relation to representation theory

If M is a left R-module, then the *action* of an element r in R is defined to be the map $M \to M$ that sends each x to rx (or xr in the case of a right module), and is necessarily a group endomorphism of the abelian group $(M,+)$. The set of all group endomorphisms of M is denoted $\mathrm{End}_{\mathbf{Z}}(M)$ and forms a ring under addition and composition, and sending a ring element r of R to its action actually defines a ring homomorphism from R to $\mathrm{End}_{\mathbf{Z}}(M)$.

Such a ring homomorphism $R \to \mathrm{End}_{\mathbf{Z}}(M)$ is called a *representation* of R over the abelian group M; an alternative and equivalent way of defining left R-modules is to say that a left R-module is an abelian group M together with a representation of R over it.

A representation is called *faithful* if and only if the map $R \to \mathrm{End}_{\mathbf{Z}}(M)$ is injective. In terms of modules, this means that if r is an element of R such that $rx=0$ for all x in M, then $r=0$. Every abelian group is a faithful module over the integers or over some modular arithmetic $\mathbf{Z}/n\mathbf{Z}$.

Generalizations

Any ring *R* can be viewed as a preadditive category with a single object. With this understanding, a left *R*-module is nothing but a (covariant) additive functor from *R* to the category **Ab** of abelian groups. Right *R*-modules are contravariant additive functors. This suggests that, if *C* is any preadditive category, a covariant additive functor from *C* to **Ab** should be considered a generalized left module over *C*; these functors form a functor category *C*-**Mod** which is the natural generalization of the module category *R*-**Mod**.

Modules over *commutative* rings can be generalized in a different direction: take a ringed space (X, O_X) and consider the sheaves of O_X-modules. These form a category O_X-**Mod**, and play an important role in the scheme-theoretic approach to algebraic geometry. If *X* has only a single point, then this is a module category in the old sense over the commutative ring $O_X(X)$.

One can also consider modules over a semiring. Modules over rings are abelian groups, but modules over semirings are only commutative monoids. Most applications of modules are still possible. In particular, for any semiring *S* the matrices over *S* form a semiring over which the tuples of elements from *S* are a module (in this generalized sense only). This allows a further generalization of the concept of vector space incorporating the semirings from theoretical computer science.

Notes

[1] Jacobson (1964), p. 4 (http://books.google.com.br/books?id=KlMDjaJxZAkC&pg=PA4), Def. 1; *Irreducible Module* (http://planetmath.org/encyclopedia/IrreducibleModule.html) at PlanetMath.

References

- F.W. Anderson and K.R. Fuller: *Rings and Categories of Modules*, Graduate Texts in Mathematics, Vol. 13, 2nd Ed., Springer-Verlag, New York, 1992, ISBN 0-387-97845-3, ISBN 3-540-97845-3
- Nathan Jacobson. *Structure of rings*. Colloquium publications, Vol. 37, 2nd Ed., AMS Bookstore, 1964, ISBN 9780821810378

Article Sources and Contributors

Module (mathematics) *Source*: http://en.wikipedia.org/w/index.php?oldid=417821728 *Contributors*: AHMartin, Almit39, Aretakis, Ashley Y, AxelBoldt, Bgohla, CRGreathouse, Catfive, Charles Matthews, CyborgTosser, D stankov, Dawynn, DefLog, Dmharvey, Druiffic, Dysprosia, El C, Eric Kvaalen, Esqg, Fropuff, Gaius Cornelius, Gauge, Giftlite, Grafen, Guardian of Light, Hans Adler, Harold f, Helder.wiki, Hellisp, Hillman, JPD, JackSchmidt, Jonathanrcoxhead, Jorge Stolfi, Jorgen W, Lethe, Linas, Markjoseph125, MathMartin, Matikkapoika, MaximalIdeal, Mikecrumley, Monterey Bay, Movementarian, Msh210, Ntmatter, Oleg Alexandrov, Paul August, PhotoBox, Phys, RandomP, Reyk, Robinh, Salgueiro, Salix alba, ScipioJ, Sendhil, Simetrical, Sxtr, Tchoř, Thomas Bliem, Thorwald, Tobias Bergemann, Waltpohl, WhiteHatLurker, Xantharius, YouRang?, Yuyo 84, Zundark, 48 anonymous edits

License

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