Algebra fact sheet

An **algebraic structure** (such as group, ring, field, etc.) is a set with some operations and distinguished elements (such as $0, 1$) satisfying some axioms. This is a fact sheet with definitions and properties of some of the most important algebraic structures.

A **substructure** of a structure A (i.e., a subgroup, subring, subfield etc.) is a subset of A that is closed under all operations and contains all distinguished elements.

Algebraic structures of the same type (e.g., groups) can be related to each other by homomorphisms. A **homomorphism** $f : A \to B$ is a map that preserves all operations and distinguished elements (e.g. $f(ab) = f(a)f(b)$). An **isomorphism** is a homomorphism which is a one-to-one correspondence (bijection); then the inverse f^{-1} is also an isomorphism. Isomorphic algebraic structures are regarded as the same, and algebraic structures of each type are classified up to an isomorphism.

Semigroup: A set G with an operation $G \times G \to G$, $(a, b) \mapsto ab$, called multiplication, which is associative: $(ab)c = a(bc)$.

Examples: Positive integers with operation of addition.

Monoid: A semigroup G with unit $1 \in G$, such that $1g = g1 = g$ for all $g \in G$.

Note that a unit is unique: $1 = 11' = 1'$.

Examples: Nonnegative integers under addition; all integers under multiplication.

Group: A monoid G with an inversion operation $G \to G$, $g \mapsto g^{-1}$, such that $gg^{-1} = g^{-1}g = 1$.

Note that inverse is unique: $g_1^{-1} = g_1^{-1}gg_2^{-1} = g_2^{-1}$. So for a semigroup, being a monoid or a group is a property, not an additional structure.

Examples: (1) All integers under addition, $\mathbf{Z}$. Integers modulo n under addition, $\mathbf{Z}_n$. (These two are called cyclic groups). The group $\mathbf{Z}^N$ (N-dimensional vectors of integers). Rational numbers $\mathbf{Q}$, real numbers $\mathbf{R}$, or complex numbers $\mathbf{C}$ under addition. Nonzero rational, real, or complex numbers under multiplication.

(2) Permutation (or symmetric) group S_n on n items. The group GL_n of invertible matrices with integer, rational, real, or complex entries, or with integer entries modulo n (e.g. $GL_n(\mathbf{Q})$). The group of symmetries of a polytope (e.g., regular icosahedron).

Abelian (commutative) group: A group G where $ab = ba$ (commutativity).

Examples: The examples from list (1) above.

If A is an abelian group, one often denotes the operation by $+$ and 1 by 0.

Action of a monoid or a group on a set: A left action of a monoid (in particular, a group) G on a set X is a multiplication map $G \times X \to X$, $(g, x) \mapsto gx$ such that $(gh)x = g(hx)$ and $1x = x$. Similarly one defines a right action, $(x, g) \mapsto xg$.

Examples. Any monoid (in particular, group) acts on itself by left and right multiplication. The symmetric group S_n acts on $\{1, ..., n\}$. Matrices act on vectors. The group of symmetries of a regular icosahedron acts on the sets of its points, vertices, edges, faces and on the ambient space.

Normal subgroup: A subgroup $H \subset G$ such that $gH = Hg$ for all $g \in G$.

Quotient group: If A is an abelian group and B a subgroup in A, then A/B is the set of subsets aB in A (where $a \in A$) with operation $a_1Ba_2B = a_1a_2B$; this defines a group structure on A/B. If A is not abelian, then in general A/B is just a set with a left action of A. For it to be a group (i.e., for the formula $a_1Ba_2B = a_1a_2B$ to make sense), B needs to be a normal subgroup. This is automatic for abelian groups A.

Examples. $\mathbf{Z}/n\mathbf{Z} = \mathbf{Z}_n$. $S_3/\mathbf{Z}_3 = \mathbf{Z}_2$.

Lagrange's theorem: The order (i.e., number of elements) of a subgroup H of a finite group G divides the order of G (the quotient $|G|/|H|$ is $|G/H|$).

The **order** of $g \in G$ is the smallest positive integer n such that $g^n = 1$ (∞ if there is none). Equivalently, the order of g is the order of the subgroup generated by g. Thus by Lagrange's theorem, the order of g divides the order of G. This implies that any group of order p (a prime) is $\mathbf{Z}_p$.

Direct (or Cartesian) product (of semigroups, monoids, groups): $G \times H$ is the set of pairs (g, h), $g \in G, h \in H$, with componentwise operation.

One can also define a direct product of more than two factors. For abelian groups, the direct product is also called the direct sum and denoted by $\oplus$.

Generators: A group G is generated by a subset $S \subset G$ if any element of G is a product of elements of S and their inverses. A group is finitely generated if it is generated by a finite subset.

Classification theorem of finitely generated abelian groups. Any finitely generated abelian group is a direct sum of infinite cyclic groups ($\mathbf{Z}$)

and cyclic groups of prime power order. Moreover, this decomposition is unique up to order of factors (and up to isomorphism).

(Unital) ring: An abelian group A with operation $+$ which also has another operation of multiplication, $(a,b) \mapsto ab$, under which A is a monoid, and which is distributive: $a(b+c) = ab + ac$, $(b+c)a = ba + ca$.

Examples: (1) The integers $\mathbf{Z}$. Rational, real, or complex numbers. Integers modulo n ($\mathbf{Z}_n$). Polynomials $\mathbf{Q}[x], \mathbf{Q}[x,y]$.

(2) Matrices n by n with rational, real, or complex entries, e.g. $\mathrm{Mat}_n(\mathbf{Q})$.

Commutative ring: A ring in which $ab = ba$.

Examples: List (1) of examples of rings.

Division ring: A ring in which all nonzero elements are invertible (i.e., form a group).

Examples: Rational, real, complex numbers. Integers modulo a prime ($\mathbf{Z}_p$). Quaternions.

Field: A commutative division ring.

Examples: Rational, real, complex numbers. Integers modulo a prime ($\mathbf{Z}_p$).

Characteristic of a field F: The smallest positive integer p such that $1 + ... + 1$ (p times) is zero in F. If there is no such p, the characteristic is said to be zero. If the characteristic is not zero then it is a prime.

Examples: The characteristic of $\mathbf{Z}_p$ is p. The characteristic of $\mathbf{Q}$ is zero.

Algebra over a field F: A ring A containing F such that elements of F commute with all elements of A.

Examples: $\mathbf{Q}[x], \mathbf{Q}[x,y]$, $\mathrm{Mat}_2(\mathbf{Q})$ (2 by 2 matrices with rational enties) are algebras over $\mathbf{Q}$.

(Left) module over a ring A: An abelian group A with a multiplication $A \times M \to M$, $(a,m) \mapsto am$ which is associative ($(ab)m = a(bm)$) and distributive ($a(m_1 + n_2) = am_1 + am_2, (a_1 + a_2)m = a_1m + a_2m$), and such that $1m = m$ (i.e., the monoid A acts on M, and the action is distributive in both arguments). Similarly one defines right modules (with multiplication $(m,a) \mapsto ma$). Note that for a commutative ring, a left module is the same thing as a right module.

Examples: A module over $\mathbf{Z}$ is the same thing as an abelian group. Also, for any ring A, $A^n = A \oplus ... \oplus A$ (n times) is a module over A, left and right (called free module of rank n). More generally, if S is a set, then the **free A-module** $A[S]$ with basis S is the set of formal finite sums $\sum_{s \in S} a_s s$, $a_s \in A$, where all a_s but finitely many are zero.

Quotient module: If $N \subset M$ are A-modules, then so is the quotient M/N.

Vector space: A module over a field.

Examples: F^n, where F is a field. The space of complex-valued functions on any set X.

Basis of a vector space V: A collection of elements $\{v_i\}$ such that any element (vector) $v \in V$ can be uniquely written as $v = \sum a_i v_i$, $a_i \in F$.

Basis theorem: A basis always exists and all bases have the same number of elements (which could be infinite). This number is called the dimension of V.

Theorem: Any finite field has order p^n, where p is its characteristic (which is a prime).

Indeed, such a field is a vector space over $\mathbf{Z}_p$ of some finite dimension n, so its order is p^n.

In fact, for any prime power q there is a unique finite field of order q, denoted $\mathbf{F}_q$.

Linear map: A homomorphism of vector spaces, i.e. a map $f : V \to W$ of vector spaces over a field F such that $f(a+b) = f(a) + f(b)$, and $f(\lambda a) = \lambda f(a)$ for $\lambda \in F$.

Examples: A matrix n by m over F defines a linear map $F^m \to F^n$. The derivative d/dx is a linear map from $\mathbf{C}[x]$ to itself.

Ideal: A left ideal in a ring A is a left submodule of A, i.e., a subgroup $I \subset A$ such that $AI = I$. Similarly, a right ideal is a right submodule of A ($IA = A$). A two-sided ideal is a left ideal which is also a right ideal.

Examples: $f \in A$, $I = Af$ is the ideal of all multiples of f. For example, $n\mathbf{Z}$ inside $\mathbf{Z}$.

If $I \subset A$ is a left ideal, then the quotient group A/I is a left A-module. If I is a two-sided ideal, then A/I is a ring.

Examples: $\mathbf{Z}/n\mathbf{Z} = \mathbf{Z}_n$. $\mathbf{R}[x]/(x^2+1) = \mathbf{C}$.

Lie algebra: A vector space L over a field F with a bracket operation $[,] : L \times L \to L$, which is bilinear (i.e., $[a,b]$ is linear with respect to a for fixed b and with respect to b for fixed a), skew-symmetric ($[a,a] = 0$, so $[a,b] = -[b,a]$), and satisfies the Jacobi identity $[a,[b,c]] + [b,[c,a]] + [c,[a,b]] = 0$.

Examples: Any algebra A with $[a,b] = ab - ba$ is a Lie algebra. So square matrices over a field form a Lie algebra. Other examples are the Lie algebra of matrices with trace zero and the Lie algebra of skew-symmetric matrices ($X^T = -X$).

Tensor product of modules: If A is a ring, M is a right A-module, and N a left A-module, then $M \otimes_A N$ is the quotient of the free abelian group with basis $S = \{m \otimes n, m \in M, n \in N\}$ (where $m \otimes n$ are formal symbols) by the subgroup spanned by

$$(m_1+m_2)\otimes n - m_1\otimes n - m_2\otimes n,\ m\otimes(n_1+n_2) - m\otimes n_1 - m\otimes n_2,\ ma\otimes n - m\otimes an,$$

where $a \in A$. By doing this we force the relations saying that the expressions above are zero.

Note that if A is commutative then left and right module is the same thing, and so M, N are just A-modules. Moreover, in this case the abelian group $M \otimes_A N$ is also an A-module: $a \cdot (m \otimes n) = ma \otimes n = m \otimes an$.

Example: $\mathbf{Z}_r \otimes_{\mathbf{Z}} \mathbf{Z}_s = \mathbf{Z}_{\gcd(r,s)}$. For example, $\mathbf{Z}_2 \otimes_{\mathbf{Z}} \mathbf{Z}_3 = 0$.

Theorem: If V, W are vector spaces over a field F with bases v_i and w_j then the set of elements $v_i \otimes w_j$ is a basis of $V \otimes_F W$. In particular, the dimension of $V \otimes_F W$ is the product of dimensions of V and W.

So, unlike abelian groups, the tensor product of nonzero vector spaces is nonzero.