COMPUTATIONAL MATHEMATICS
TOPIC 32 - ALGEBRAIC CATEGORIES

PAUL L. BAILEY

Abstract. We state the pertinent definitions regarding some of the algebraic categories.

1. Categories

The study of category theory helped structure mathematics during the latter half of the twentieth century, in a manner similar to the way that mathematics was rewritten using set theory in the first half of the twentieth century.

For our purposes, an *object* is a set together with some additional structure, and a *morphism* is a structure preserving function between two objects. A *category* consists of all of the objects of the same type, together with the morphisms between objects of that type.

For example, consider sets which have an order relation on them. We could consider the collection of such objects to be a category; the morphism would be order-preserving (i.e. increasing) functions between the sets.

As another example, a metric space is a set in which any two points have a distance between them. We could form the category of metric spaces by saying that morphisms between metric spaces must be distance preserving functions.

An *algebraic category* is a category in which the objects admit one or more binary operations, and the morphisms preserve these operations. In this document, we briefly outline some of the main algebraic categories. Later we will study some of these in more detail.

2. Magmas

The simplest algebraic category is a magma. This is a good place to start.

Definition 1. A *magma* $(M, *)$ consists of a nonempty set M together with a binary operation $* : M \times M \to M$.

Is is typical to say that M is a magma, where the reader assumes that M is endowed with a binary operation.

We may say that the magma is commutative or associative, depending if the binary operation is commutative or associative. The magma may or may not have an identity or inverses. The key property of a magma is closure of the binary operation.

Example 1. Let $\mathbb{N} = \{0, 1, 2, 3, \dots\}$ be the set of natural numbers. In some contexts, it is more convenient to let the natural numbers start at 1, but for algebra, it is usually better to let them start at 0. Then $(\mathbb{N}, +)$ and $(\mathbb{N}, \cdot)$ are magmas.

Date: Friday, April 5, 2019.

Example 2. The set of three dimensional vectors over $\mathbb{R}$, together with cross-product, is the magma $(\mathbb{R}^3, \times)$. This magma is neither commutative nor associative.

Example 3. Let $\mathcal{F}(X)$ denote the set of all functions from X into itself. Then composition is a binary operation on this set, and $(\mathcal{F}(X), \diamond)$ is an associative magma.

Definition 2. Let $(M, *)$ be a magma, and let $N \subset M$. We say that N is a *submagma* of M if

(a) N is nonempty;
(b) $a, b \in N$ implies $a * b \in N$.

So, a nonempty $N \subset M$ is a submagma if the binary operation of M is closed on N. Indeed, N is a submagma if N is itself a magma with respect to the same binary operation.

Example 4. The set of even integers greater than eleven is closed under multiplication, so it is a submagma of $(\mathbb{N}, \cdot)$.

The set of three dimensional vectors with rational coefficients is closed under cross product, so it is a submagma of $(\mathbb{R}^3, \times)$.

Definition 3. Let $(M, *)$ and $(N, \diamond)$ be magmas. A *magma homomorphism* from M to N is a function $f : M \to N$ with the property that, for every $a, b \in M$, we have

$$f(a * b) = f(a) \diamond f(b).$$

Example 5. Let $M = \mathbb{R}$ denote the set of real numbers, and let $* = +$ be addition. Then $(M, *) = (\mathbb{R}, +)$ is a magma.

Let $N = \mathbb{R}_{>0} = (0, \infty)$ denote the set of positive real numbers, and let $\diamond = \cdot$ denote multiplication. Then $(N, \diamond) = (\mathbb{R}_{>0}, \cdot)$ is a magma.

Define $f : \mathbb{R} \to \mathbb{R}_{>0}$ by $f(x) = e^x$. Then

$$f(x_1 + x_2) = e^{x_1 + x_2} = e^{x_1} e^{x_2} = f(x_1) \cdot f(x_2),$$

so f is a magma homomorphism.

Define $g : \mathbb{R}_{>0} \to \mathbb{R}$ by $g(y) = \ln(y)$. Then

$$g(y_1 y_2) = \ln(y_1 y_2) = \ln(y_1) + \ln(y_2) = g(y_1) + g(y_2).$$

Indeed, f is a bijective homomorphism, and its inverse g is also a homomorphism. One sees that f sets up a correspondence between the magma structures of $\mathbb{R}$ and $\mathbb{R}_{>0}$ which causes them to be virtually identical, other than the way the points are labeled.

Definition 4. Let M and N be magmas. An *isomorphism* from M to N is a bijective magma homomorphism. We say that M and N are isomorphic, and write $M \cong N$, if there exists a magma homomorphism from M to N.

Proposition 1. *Let $(M, *)$ and $(N, \diamond)$ be magmas, and let $f : M \to N$ be a bijective magma homomorphism. Let $g : N \to M$ be the inverse of f. Then g is a magma homomorphism.*

Proof. Let $n_1, n_2 \in N$; we wish to show that $g(n_1 \diamond n_2) = g(n_1) * g(n_2)$.

Since f is bijective, there exist unique $m_1, m_2 \in M$ such that $f(m_1) = n_1$ and $f(m_2) = n_2$. Then, since f is a homomorphism,

$$n_1 \diamond n_2 = f(m_1) \diamond f(m_2) = f(m_1 * m_2).$$

Now apply g to both sides of this equation; since $g(f(m)) = m$ for all $m \in M$, we get

$$g(n_1 \diamond n_2) = g(f(m_1 * m_2)) = m_1 * m_2 = g(n_1) * g(n_2).$$

This is what we wished to show. □

Proposition 2. *Let $(M, *)$, $(N, \diamond)$, and $(O, \star)$ be magmas, and let $f : M \to N$ and $g : N \to O$ be a magma homomorphisms. Then $g \circ f : M \to O$ is a magma homomorphism. If f and g are isomorphisms, then so is $g \circ f$.*

Proof. Let $h = g \circ f$, and let $m_1, m_2 \in M$. Then

$$h(m_1 * m_2) = g(f(m_1 * m_2)) = g(f(m_1) \diamond f(m_2)) =$$
$$g(f(m_1)) \star g(f(m_2)) = h(m_1) \star h(m_2),$$

which is what we were required to show.

The last sentence follows from the fact that the composition of bijective functions is bijective. □

The next proposition indicates that isomorphism is an equivalence relation on any collection of magmas.

Proposition 3. *Let A, B, and C be magmas. Then*

(1) *$A \cong A$;*
(2) *$A \cong B$ implies $B \cong A$;*
(3) *$A \cong B$ and $B \cong C$ implies $A \cong C$.*

Proof. The identity map is an isomorphism, so $A \cong A$.

The inverse of an isomorphism is an isomorphism, so if $A \cong B$, then $B \cong A$.

The composition of isomorphisms is an isomorphism, so if $A \cong B$ and $B \cong C$, then $A \cong C$. □

3. Monoids

We are particularly interested in associative binary operations with an identity, so we make that our next definition.

Definition 5. A *monoid* $(M, *, e)$ consists of a nonempty set M together with a binary operation $* : M \times M \to M$ satisfying

(M1) $a * (b * c) = (a * b) * c$ for all $a, b, c \in M$ ($*$ is associative);
(M2) there exists $e \in M$ such that $e * a = a * e = a$ for all $a \in M$ ($*$ has an identity).

Example 6. The archetypical example of a monoid is $(\mathbb{N}, +, 0)$, where $0 \in \mathbb{N}$ is the additive identity.

Let M denote the set of positive natural numbers; then $(M, \cdot, 1)$ is a monoid.

Example 7. Let $\mathcal{M}_n(\mathbb{R})$ denote the set of $n \times n$ matrices over $\mathbb{R}$. Then $\mathcal{M}_n(\mathbb{R})$ is a monoid under the operation of matrix multiplication.

A *submonoid* of a monoid is a subset which is closed under the operation, and which contains the same identity. A *monoid homomorphism* is a magama homomorphism between monoids which sends the identity of one to the identity of the other.

4. Groups

The most studied algebraic object with one operator is a group, which is a monoid in which each element has an inverse. For convenience, we will write generic groups using multiplicative notation.

Definition 6. A *group* $(G, \cdot, 1)$ consists of a nonempty set G together with a binary operation $\cdot : G \times G \to G$ satisfying

- **(G1)** $g_1 * (g_2 * g_3) = (g_1 * g_2) * g_3$ for all $g_1, g_2, g_3 \in G$ (associativity);
- **(G2)** there exists $1 \in G$ such that $1 \cdot g = g \cdot 1 = g$ for all $g \in G$ (existence of an identity);
- **(G3)** for every $g \in G$ there exists $g^{-1} \in G$ such that $gg^{-1} = g^{-1}g = 1$ (existence of inverses).

We recall that the identity and inverses are unique. Since a group is associative, parentheses are useless when writing operations with three or more elements. In general, groups are not commutative; we have a special name for the case that they are.

Definition 7. Let G be a group. We say the G is *abelian* if

- **(G4)** $g_1 g_2 = g_2 g_1$ for all $g_1, g_2 \in G$ (commutativity).

Obvious examples of groups include the integers, rationals, and reals under addition and the nonzero rationals and reals under multiplication. Other examples of groups we wish to explore include the additive and multiplicative groups of integers modulo n, the symmetry groups, the matrix groups, and the power set groups. Later, we will go more deeply into these examples the theory of groups. For now, we simply define subgroups and homomorphisms, for comparison with the other algebraic categories.

Definition 8. Let G be a group. A *subgroup* of G is a subset $H \subset G$ satisfying

- **(S0)** H is nonempty;
- **(S1)** $h_1, h_2 \in H$ implies $h_1 h_2 \in H$;
- **(S2)** $h \in H$ implies $h^{-1} \in H$.

We may write $H \leq G$ to indicate that H is a subgroup of G.

These are exactly the conditions which ensure that H is itself a group obtained by restricting the operation on G to H.

Definition 9. Let G and H be groups. A *group homomorphism* is a function $\phi : G \to H$ such that

$$\phi(g_1 g_2) = \phi(g_1)\phi(g_2).$$

A *group isomorphism* is a bijective group homomorphism.

5. Rings

The primary algebraic object with two operations is the ring. We take a ring to be a set which is an abelian group under addition and a monoid under multiplication. The operations are related by the distributive laws.

Definition 10. A *ring* $(R, +, \cdot, 0, 1)$ is a set R together with a pair of binary operations

$$+ : R \times R \to R \text{ and } \cdot : R \times R \to R$$

such that

(R1) $a + b = b + a$ for every $a, b \in R$;
(R2) $(a + b) + c = a + (b + c)$ for every $a, b, c \in R$;
(R3) there exists $0 \in R$ such that $a + 0 = a$ for every $a \in R$;
(R4) for every $a \in R$ there exists $-a \in R$ such that $a + (-a) = 0$;
(R5) $(ab)c = a(bc)$ for every $a, b, c \in R$;
(R6) there exists $1 \in R$ such that $a \cdot 1 = 1 \cdot a = a$ for every $a \in R$;
(R7) $a(b + c) = ab + ac$ for every $a, b, c \in R$;
(R8) $(a + b)c = ac + bc$ for every $a, b, c \in R$.

Note that multiplication is not assumed to be commutative; this is the reason that both the left and right distributive laws are given. The reason for this is to include an important class of rings, the matrix rings, under the standard definition.

Be aware that some authors give slightly different definitions of rings. In particular, it is not uncommon to leave out axiom **(R6)**, the existence of a multiplicative identity. For our purposes, it is more convenient to include this axiom.

Definition 11. Let R be a ring. We say that R is *commutative* if it satisfies the additional axiom

(R9) $ab = ba$ for every $a, b \in R$.

Examples of rings include the integers, the rationals, the reals, and the complex numbers. These rings have many subrings of interest. Also of interest for us are the rings of modular integers, the rings of square matrices, and the power set rings. All of these, except the matrix rings, are commutative. Lastly, and in some ways most importantly, we have the polynomials rings.

Definition 12. Let R be a ring. A *subring* of R is a subset $S \subset R$ such that

(S0) $1 \in S$;
(S1) $a, b \in S \Rightarrow a + b \in S$;
(S2) $a \in S \Rightarrow -a \in S$;
(S3) $a, b \in S \Rightarrow ab \in S$.

If S is a subring of R, we write $S \leq R$.

Definition 13. Let R and S be rings. A *ring homomorphism* from R to S is a function $\phi : R \to S$ such that

(H0) $\phi(1_R) = 1_S$;
(H1) $\phi(a + b) = \phi(a) + \phi(b)$ for all $a, b \in R$;
(H2) $\phi(ab) = \phi(a)\phi(b)$ for all $a, b \in R$.

A bijective ring homomorphism is called a *ring isomorphism*.

6. Fields

Definition 14. A *field* is a commutative ring F satisfying the additional axiom **(R10)** for every $a \in F \setminus \{0\}$ there exists $a^{-1} \in F$ such that $aa^{-1} = 1$.

Our first examples of fields include the rationals, the reals, the complexes, and the integers modulo p, where p is prime. There are many more, however, and the finite ones are particularly interesting for computational mathematics (e.g. cryptography). We will be particularly interested in rings of polynomials over a finite field.

A *subfield* of a field is a subring which is closed under multiplicative inverses. A *field homomorphism* of a field is simply a ring homomorphism whose domain is a field. It is possible to prove that such a function sends inverses to inverses, and is injective.

7. Domains

Domains play an important role in the theory of polynomial rings, so we include their definition here.

Definition 15. Let R be a commutative ring and let $a \in R$.

We say that a is *entire* if $ab = 0 \Rightarrow b = 0$ for every $b \in R$.

We say that a is *cancellable* if $ab = ac \Rightarrow b = c$ for every $b, c \in R$.

We say that a is *invertible* if there exists an element $a^{-1} \in R$ such that $aa^{-1} = 1$.

Problem 1. Let R be a commutative ring and let $a \in R$. Show that a is entire if and only if a is cancellable.

Problem 2. Let R be a commutative ring and let $a \in R$. Show that if a is invertible, then a is entire.

Definition 16. A *domain* is a commutative ring D in which every nonzero element is entire.

Note that a field may be defined as a ring in which every nonzero element is invertible.

Some authors allow for noncommutative domains, and called commutative domains *integral domains*. We have no use for this, so the above definition is more convenient.

8. Vector Spaces

Definition 17. Let F be a field. A *vector space over* F consists of a set V, together with two operations,

$$+ : V \times V \to V \quad \text{and} \quad \cdot : F \times V \to V,$$

known as *vector addition* and *scalar multiplication*, satisfying, for all $v, w, x \in V$ and $a \in F$,

- **(V1)** $v + w = w + v$ for all $v, w \in V$
- **(V2)** $v + (w + x) = (v + w) + x$ for all $v, w, x \in V$
- **(V3)** there exists $\vec{0} \in V$ such that $v + 0 = v$ for all $v \in V$
- **(V4)** for every $v \in V$ there exists $-v \in V$ such that $v + (-v) = \vec{0}$
- **(V5)** $1 \cdot v = v$ for all $v \in V$, where $1 \in F$
- **(V6)** $a(bv) = (ab)v$ for all $a, b \in F$ and $v \in V$

A *vector* is a member of a vector space.

The motivating example of a vector space is the set $\mathbb{R}^n$ of all ordered n-tuples of real numbers. We view these as vectors geometrically as directed line segments which may be used to model physical motion. We generalize this to an arbitrary field as follows.

Let F be any field, and let F^n denote the set of ordered n-tuples from F. Then F^n is a vector space over F, with componentwise addition and scalar multiplication.

Definition 18. Let V be a vector space over a field F. A *subspace* of V is a subset $W \subset V$ satisfying

- **(S0)** W is nonempty;
- **(S1)** $w_1, w_2 \in W$ implies $w_1 + w_2 \in W$;
- **(S2)** $w \in W$ and $a \in F$ implies $aw \in W$.

The notation $W \leq V$ means that W is a subspace of V.

Definition 19. Let V be a vector space over a field F, and let $X \subset V$.

A *linear combination* from X is a vector $v \in V$ of the form

$$v = \sum_{i=1}^{n} a_i x_i, \quad \text{where } a_i \in F \text{ and } x_i \in X.$$

The *span* of X is

$$\operatorname{span} X = \{v \in V \mid v \text{ is a linear combination from } X\}.$$

If $W = \operatorname{span} X$, we say that X *spans* W.

Fact 1. Let V be a vector space over a field F. Let $X \subset V$ and $W = \operatorname{span} X$. Then $W \leq V$.

Definition 20. Let V be a vector space over a field F, and let $X \subset V$.

We say that X is *linearly independent* if, for any $x_1, \ldots, x_n \in X$ and any $a_1, \ldots, a_n \in F$,

$$\sum_{i=1}^{n} a_i x_i = \vec{0} \quad \Rightarrow \quad a_1 = a_2 = \cdots = a_n = 0.$$

We say that X is a *basis* of V if X is a linearly independent set of vectors which spans V. The plural of basis is bases.

Fact 2. Every vector space has a basis. Any two bases have the same cardinality.

Definition 21. Let V be a vector space over a field F.

The *dimension* of V is

$$\dim V = |X|,$$

where X is any basis of V.

We say that V is finite dimensional if V has a finite basis. There are interesting vector spaces which are finite dimensional, and others which are infinite dimensional.

Note that F^n is a vector space of dimension n. The *standard basis* of F^n is $\{e_1, \ldots, e_n\}$, where e_i contains 1 in the i^{th} component, and 0 is every other component.

The morphisms in the category of vector spaces are called linear transformations.

Definition 22. Let V and W be vector spaces over a field F. A *linear transformation* from V to W is a function $T : V \to W$ satisfying

(T1) $v_1, v_2 \in V$ implies $T(v_1 + v_2) = T(v_1) + T(v_2)$;
(T2) $v \in V$ and $a \in F$ implies $T(av) = aT(v)$.

An *isomorphism* is a bijective linear transformation. Two vector spaces are *isomorphic* if there exists an isomorphism between them.

Proposition 4. *Two vector spaces over the same field are isomorphic if and only if they have the same dimension.*

In particular, if V is a finite dimensional vector space of dimension n, then V is isomorphic to F^n.

Let $T : F^n \to F^m$ be a linear transformation. The *matrix* of T is obtained by putting the destinations of the standard basis vectors into the columns of the matrix. That is, form the matrix

$$A = [T(e_1)| \cdots |T(e_n)],$$

where $T(e_i)$ if viewed as a column of the matrix. Then for $v \in F^n$, $T(v) = w$ if and only if $Av = w$, where in the second equation, v and w are viewed as column vectors.

In this way, there is a one to one correspondence between the set of linear transformations $T : F^n \to F^m$, and the set of $m \times n$ matrices over F.

The set of linear transformations from F^n to F^n is a ring, with addition being pointwise addition of functions, and multiplication being composition of functions. The set of $n \times n$ matrices over F is also a ring, under matrix addition and multiplication. The correspondence between these to sets as described above is a ring isomorphism.

Department of Mathematics and CSci, BASIS Scottsdale
Email address: paul.bailey@basised.com