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: Tuesday, February 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*

- **(R)** $A \cong A$*;*
- **(S)** $A \cong B$ *implies* $B \cong A$*;*
- **(T)** $A \cong B$ *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* $(M, *)$ 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 archtypical example of a monoid is $(\mathbb{N}, +)$, where $0 \in \mathbb{N}$ is the additive identity.

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

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