ALGEBRAIC STRUCTURES I

JOAQUÍN MORAGA

Olga Radko Math Circle.

Section 1: Magmas.

Today, we will study a concept called "Algebraic Structures". Starting from a set S, we will slowly introduce more structures to it, trying to mimic the natural operations that we have in the integers $\mathbb{Z}$, the rational $\mathbb{Q}$, and the real numbers $\mathbb{R}$. The concept of Algebraic Structures will allow us to find new objects that are alike $\mathbb{Z}, \mathbb{Q}$ and $\mathbb{R}$.

Definition 1. A *binary operation* on a set X is an operation $*$ that transforms two elements x and y in the set X into a new element $x * y$. The element $x * y$ may or may not belong to X. For instance, the addition in $\mathbb{Z}$ is a binary operation defined as

$$\mathbb{Z} \times \mathbb{Z} \to \mathbb{Z}$$
$$(a, b) \mapsto a + b.$$

Similarly, the addition in $\mathbb{R}$ and the addition in $\mathbb{Q}$ are binary operations. The division in $\mathbb{Z}$, defined by

$$\mathbb{Z} \times \mathbb{Z} \to \mathbb{Q}$$
$$(a, b) \mapsto \frac{a}{b},$$

is also a binary operation on $\mathbb{Z}$. However, the values that this binary operation takes are not necessarily in $\mathbb{Z}$.

Problem 1: Consider the set $\mathbb{Z}^2$ and the binary operation:

$$(x_1, y_1) * (x_2, y_2) \mapsto (x_1 y_2, x_2 y_1).$$

We say that a subset $X \subseteq \mathbb{Z}^2$ is closed under the operation $*$ if $x * y \in X$ whenever x and y are contained in X.

- Find the smallest subset $X \subseteq \mathbb{Z}^2$ that contains $\mathcal{F} = \{(-1, -1), (0, 0), (2, 2)\}$ and is closed under the operation $*$.
- Find the smallest subset $Y \subseteq \mathbb{Z}^2$ that contains $\mathcal{F} = \{(2, 1), (1, 2)\}$ and is closed under the operation $*$.
- Let $\mathcal{F} \subset \mathbb{Z}^2$ be a finite set as above and $Z \subset \mathbb{Z}^2$ be the smallest subset of $\mathbb{Z}^2$ which contains $\mathcal{F}$ and is closed under the operation $*$. Can you find $\mathcal{F}$ such that $Z = \mathbb{Z}^2$?

Solution 1:

Definition 2. A *magma* is a set X with an operation

$$*\colon X \times X \to X,$$
$$(x, y) \mapsto x * y \in X.$$

In other words, a magma is a set which is closed under a *binary operation* $*$. Sometimes, we say that $(X, *)$ is a magma, to emphasize the set and the operation. In other words, a magma is a set X with a binary operation so that the outcome of the binary operation is always in X.

Problem 2: Is $(\mathbb{Z}, +)$ a magma?
Is $(\mathbb{R}, +)$ a magma?
Is $(\mathbb{Q}, -)$, with the binary operation subtraction, a magma? Write two different examples of magmas that you know. Write two different examples of set with binary operations are not magmas.

Solution 2:

Problem 3: Consider $\mathcal{P}([0, 1])$ the set of polynomial functions $f\colon [0, 1] \to \mathbb{R}$. We can consider two different operations $\otimes_1$ and $\otimes_2$ given by

$$f(x) \otimes_1 g(x) := f(x)^2 g(x) + f(x) g(x)^2, \text{ and}$$
$$f(x) \otimes_2 g(x) := f(x) g(x).$$

- Is $(\mathcal{P}([0, 1]), \otimes_1)$ a magma?

- Is $(\mathcal{P}([0,1]), \otimes_2)$ a magma?
- Can you find a function $i(x) \in \mathcal{P}([0,1])$ that satisfies:
$$i(x) \otimes_1 f(x) = f(x) \otimes_1 i(x) = f(x)$$
for every $f(x) \in \mathcal{C}([0,1])$?
- Can you find a function $i(x) \in \mathcal{P}([0,1])$ that satisfies:
$$i(x) \otimes_2 f(x) = f(x) \otimes_2 i(x) = f(x)$$
for every $f(x) \in \mathcal{C}([0,1])$?

Solution 3:

Definition 3. A *unital magma* is a magma $(X, *)$ with an element $i \in X$ that satisfies:
$$i * x = x * i = x,$$
for every element $x \in X$. The element i is called the *identity element* or *unit*. Sometimes, people use 1 or e to denote the unit.

Problem 4: Show that a unital magma must have a unique unit. This means that two units i and j must satisfy $i = j$ in the magma.

Solution 4:

Problem 5: Consider the set $\mathcal{C} := \{red, blue, green\}$. We will define a binary operation $\times$ with the following rules:
$$\text{green} \times \text{red} = \text{red} \times \text{green} = \text{blue},$$

$$\text{green} \times \text{blue} = \text{blue} \times \text{green} = \text{red},$$

$$\text{red} \times \text{blue} = \text{blue} \times \text{red} = \text{green},$$

$$\text{red} \times \text{red} = \text{blue}, \ \text{blue} \times \text{blue} = \text{green}, \text{ and } \text{green} \times \text{green} = \text{red}.$$

For the set $\mathcal{C}$ and the operation $\times$, does the order of multiplication matters? For instance, given three colors color 1, color 2, and color 3, do we have that

$$[(\text{color 1}) \times (\text{color 2})] \times (\text{color 3}) = (\text{color 1}) \times [(\text{color 2}) \times (\text{color 3})]?$$

If this property does not hold, list all the triples for which the property fails.

Solution 5:

Definition 4. A magma $(X, *)$ is called a *semigroup* if the operation $*$ is *associative*, this means that the order of the operation does not matter:

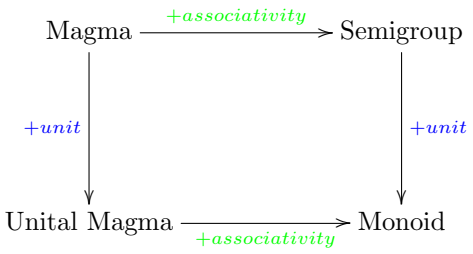
$$(x * y) * z = x * (y * z),$$

for every three elements x, y, and z in X. In the previous case, we say that $*$ is an associative operation or that the operation satisfies associativity.

Problem 6: Decide if $(\mathbb{Z}, +)$ and $(\mathbb{Z}, -)$ are semigroups or not.

Solution 6:

Definition 5. A semigroup with a unit element is called a *Monoid*. Observe that monoid is the same as a unital magma that satisfies associativity. We have the following diagram of definitions:



Problem 7: Write down an example of a monoid. Find a semigroup that is not a monoid and a unital magma that is not a monoid.

Solution 7:

Problem 8: The *Quaternion* number system extends the complex numbers. Quaternions were first introduced by the Irish mathematician William Hamilton in 1843 and applied to mechanics and three-dimensional spaces. A quaternion number can be written as

$$a + b\vec{i} + c\vec{j} + d\vec{k},$$

where the $\vec{i}, \vec{j}$, and $\vec{k}$ are called the *basic quaternion numbers*. Here, the numbers a, b, c and d are just real numbers. They satisfy the folowing rules:

$$\vec{i}^2 = \vec{j}^2 = \vec{k}^2 = \vec{i}\vec{j}\vec{k} = -1.$$

We represent the set of quaternion numbers by $\mathcal{Q}$.

Let α and β be two quaternion numbers, different from zero. Prove that there exist δ and $\gamma \in \mathcal{Q}$ for which the following equations are satisfied $\alpha\delta = \beta$ and $\gamma\alpha = \beta$.

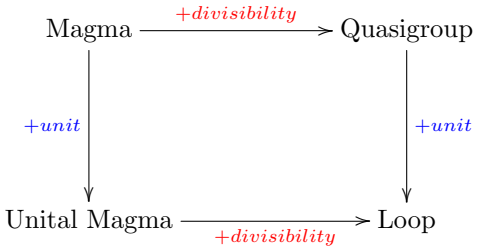
Solution 8:

Definition 6. Let $(X, *)$ be a magma. We say that $*$ has the *divisibility* property if for every pair $a, b \in X$, we can find $x, y \in X$ so that

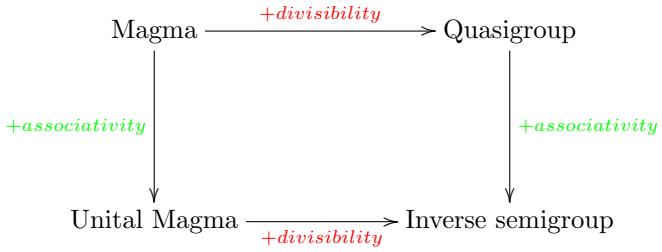
$$a * x = b \qquad \text{and} \qquad y * a = b.$$

The element x is called the *left division* of b by a and the element y is called the *right division* of b by a. A magma with the divisibily property is called a *quasigroup*. The divisibility property is often called the *invertibility property* as well.

Definition 7. A quasigroup with an identity is called a *loop*. A loop can also be described as a unital magma that satisfies the divisibility property. We have the two following diagrams of definitions. The first is related to the concepts of divisibily and identity:



The second is related to the concepts of associativity and divisibility:



Problem 9: The *hyperbolic quaternions* denoted by $\mathcal{H}$ are numbers of the form

$$a + b\vec{i} + c\vec{j} + d\vec{k},$$

where the squares $\vec{i}^2 = \vec{j}^2 = \vec{k}^2 = 1$ and different elements of $\{\vec{i}, \vec{j}, \vec{k}\}$ multiply with the anti-commutative property, i.e., $\vec{i}\vec{j} = \vec{k}$ and $\vec{j}\vec{i} = -\vec{k}$. Show that the hyperbolic quaternions $\mathcal{H}$ do not form a loop.

Solution 9:

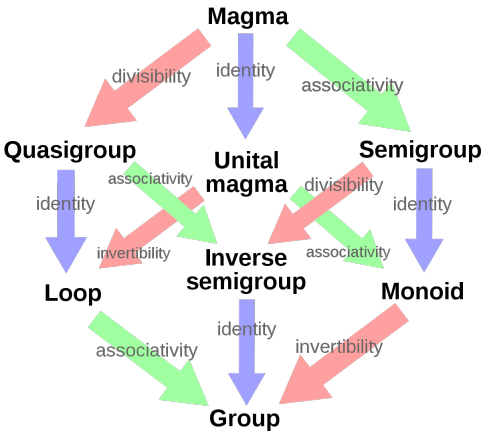
Problem 10: Let $\mathbb{Q}^\times$ be the rational numbers without the zero. Show that $(\mathbb{Q}^\times, \times)$ is a magma that satisfies the associativit and the divisibility properties, and has a unit. Can you say the same about $(\mathbb{R}^\times, \times)$? What about $(\mathbb{Z}^\times, \times)$?

Solution 10:

Definition 8. A group G is a monoid that has a unit, satisfies the associativity and the divisibility properties.

Note that a group admits other equivalent definitions. For instance, a group can also be defined as a loop that satisfies associativity. A group can also defined to be an inverse semigroup that has a unit. A group can also defined to be a monoid with the divisibility property.

All the definitions given so far can be put in the following diagram:



The red arrows represent the divisibility property, the green arrows represent the associativity property, and the blue arrows represent the existence of a unit. You can visualize the previous picture as being the vertices of a cube.

Whenever we introduce some mathematical definition, it is very important that we can give several examples of such objects as well as examples of how the new definition behaves with respect to the old ones. For instance, we have the definition of a quasigroup and the definition of a loop. We know that every loop is a quasigroup. To make

sure that the definitions do not agree, we should be able to give an example of a quasigroup that is NOT a loop. In what follows, we will try to find some of these examples.

Problem 11: Let $(G, *)$ be a group and let 1_G be its unit element. Show that for every element $g \in G$, there exists an element $b \in G$ for which

$$b * g = g * b = 1_G.$$

This element b is often called the *inverse of* G and denoted by g^{-1}.

- Show that the inverse of an element $g \in G$ is unique.
- Show that the inverse of the inverse of $g \in G$ is itself.

Solution 11:

Problem 12: Write down an example of a magma that does not have a unit, is not associative, and does not satisfy the divisibility property.

Solution 12:

Problem 13: Consider $\mathbb{Z}_m = \{0, \ldots, m-1\}$ the set of integers modulo m. Let $*$ be the multiplication in $\mathbb{Z}_m$ and let $+$ be the addition in $\mathbb{Z}_m$.

- For which values of m is $(\mathbb{Z}_m, +)$ a group?
- For which values of m is $(\mathbb{Z}_m, *)$ a group?

- If $(\mathbb{Z}_m - \{0\}, *)$ is not a group, what can we say about it? Is it a loop? Is it a semigroup with invertibility? Is it a Monoid?

Solution 13:

Problem 14: Are the complex numbers without zero $\mathbb{C} - \{0\}$ with multiplication a group? Are the quaternion numbers without zero $\mathcal{Q} - \{0\}$ with multiplication a group?

Solution 14:

Problem 15: Consider the set of integer numbers $\mathbb{Z}$ with the binary operation

$$(a, b) \mapsto a - b.$$

This operation is called the *subtraction* operation, so we may just simply denote it by $-$.

- Show that $(\mathbb{Z}, -)$ is a quasigroup.
- Show that $(\mathbb{Z}, -)$ is not a loop.
- Show that $(\mathbb{Z}, -)$ is not an inverse semigroup.

Solution 15:

Problem 16: Consider the set $\mathcal{C} := \{1, a, b\}$. We introduce an operation $*$ for which 1 is the identity element. We define

$$a * b = a, \qquad a * a = 1, \qquad b * a = b, \qquad \text{and} \qquad b * b = a.$$

- Show that $(\mathcal{C}, *)$ is a unital magma.
- Show that $(\mathcal{C}, *)$ is not a monoid.
- Show that $(\mathcal{C}, *)$ is not a loop.

Solution 16:

UCLA Mathematics Department, Box 951555, Los Angeles, CA 90095-1555, USA.
Email address: jmoraga@math.ucla.edu