Group Theory

Lecture 1, Sunday October 23, 2022
Ari Feiglin

1.1 Introduction to Algebraic Structures

Definition 1.1.1:

A **Magma** is a set S with a *binary operation*:
$$\circ\colon S\times S\longrightarrow S$$

Notice then that a Magma has no requirements on its binary operation, thus for a magma of size n there are n^{n^2} possible magmas. Despite this, some of these Magmas are equivalent in some sense, as a renaming of the elements of one magma produces the other. For example of a magma: $M=\{0,1\}$:

$$\begin{array}{c|cc} \circ & 0 & 1 \\ \hline 0 & 1 & 1 \\ 1 & 1 & 1 \end{array} \cong \begin{array}{c|cc} \circ & 0 & 1 \\ \hline 0 & 0 & 0 \\ 1 & 0 & 0 \end{array}$$

We say a magma is *associative* if for every $x,y,z\in S$ it follows that:

$$x\circ(y\circ z)=(x\circ y)\circ z$$

Example:

Given a set X, the set X^X is an associative magma under function composition.

Definition 1.1.2:

A **Semigroup** is an associative magma.

So the set X^X is a semigroup. The set $M_n(\mathbb{F})$, the set of matrices of size $n\times n$, is also a semigroup under both addition and multiplication.

Definition 1.1.3:

Let $(S,\circ)$ be a semigroup. An element $e\in S$ is a **left-identity** if for every $a\in S$: $e\circ a=a$. Similarly, e is a **right-identity** if for every $a\in S$: $a\circ e=a$. e is an **identity** if it is both a left and right identity.

Proposition 1.1.4:

If S is a semigroup with e a left-identity and e' a right-identity. Then $e=e'$.

Proof:

This is trivial. By definition of the left-identity: $e\circ e'=e'$, but by the definition of the right-identity, $e\circ e'=e$. So $e=e'$.

$\blacksquare$

Example:

Let:
$$S\coloneqq\left\{\begin{pmatrix}a & b\\ 0 & 0\end{pmatrix}\;\middle|\; a,b\in\mathbb{R}\right\}$$

equipped with the operation of multiplication. Note that if we alter the definition of S slightly:

$$S^* := \left\{ \begin{pmatrix} a & b \\ c & d \end{pmatrix} \middle| \, a, b, c \in \mathbb{R} \right\}$$

this is not a magma, as multiplication is not well-defined over this set:

$$\begin{pmatrix} 1 & 1 \\ 1 & 0 \end{pmatrix} \cdot \begin{pmatrix} 1 & 1 \\ 1 & 0 \end{pmatrix} = \begin{pmatrix} * & * \\ * & 1 \end{pmatrix} \notin S^*$$

But S is a semigroup. Notice that:

$$\begin{pmatrix} a & b \\ 0 & 0 \end{pmatrix} \cdot \begin{pmatrix} a' & b' \\ 0 & 0 \end{pmatrix} = \begin{pmatrix} aa' & ab' \\ 0 & 0 \end{pmatrix}$$

So in order for a matrix to be a left-identity, we must have that $aa' = a'$, so $a = 1$. But there are no requirements for b and so any matrix of the form

$$\begin{pmatrix} 1 & b \\ 0 & 0 \end{pmatrix}$$

is a left-identity. But for a matrix to be a right-identity, we must have that $aa' = a$ and $ab' = b$. But for any a and b we can find a b' where this doesn't hold. So S has an infinite number of left identities, but no right identities.

Notice that if a semigroup has multiple left (or right) identities, it cannot have any right (or left) identities. Suppose $e \neq e'$ are left identities and t is a right identity. Then by our proposition above $e = t$ and $e' = t$, so $e = e'$, which is a contradiction. $\lightning$

Left \ Right	None	One	Many
None	✓	✓	✓
One	✓	✓	✗
Many	✓	✗	✗

Definition 1.1.5:

A semigroup S is a **Monoid** if it has an identity element.

Proposition 1.1.6:

If S is a monoid, its identity element is unique.

Proof:

This too is trivial, as if e and e' are both identities, $e \circ e' = e = e'$.

■

Example:

$(\mathbb{N}, \cdot)$ is a monoid whose identity is 1.
$(\mathbb{Z}, -)$ is not even a semigroup as subtraction is not associative.

Definition 1.1.7:

If M is a monoid with identity element 1. If $a, b \in M$ such that $a \circ b = 1$, then a is **right-invertible** and b is **left-invertible**. And we call a b's **left inverse** and b is a's **right inverse**.
An element $a \in M$ is **invertible** if there is a $b \in M$ such that $a \circ b = b \circ a = 1$. b is called a's inverse and is denoted a^{-1}.

Note that the inverse of a^{-1} is a, this comes directly from the definition.

Proposition 1.1.8:

An element a of a monoid is invertible if and only if it is right and left invertible.

Proof:

By definition if a is right and left invertible. For the converse suppose $a \circ b = c \circ a = 1$. Then $c \circ (a \circ b) = c$, but $c \circ (a \circ b) = (c \circ a) \circ b = b$, so $c = b$ and therefore:

$$a \circ b = b \circ a = 1$$

So a is invertible.

■

Definition 1.1.9 (Group):

If every element in a monoid M is invertible, then G is called a **Group**. This means that:

- G's binary operation $\circ$ is associative.
- G has an identity element e such that for every $a \in G$: $a \circ e = e \circ a = a$.
- For every $a \in G$, there exists an $a^{-1} \in G$ such that $a \circ a^{-1} = a^{-1} \circ a = e$.

Definition 1.1.10:

A monoid is **left reducible** if for every $a, x, y \in M$, if $a \circ x = a \circ y$ then $x = y$.

Note then that a group is left (and right) reducible.

Proposition 1.1.11:

If M is a monoid where every element is left-invertible (or every element is right-invertible) then M is a group.

Proof:

Let $a \in M$, then there is a $b \in M$ such that $b \circ a = 1$. But b itself is left invertible so there is an element c such that $c \circ b = 1$. So:

$$c = c \circ b \circ a = a$$

So $ab = ba = 1$, and thus a is invertible.

■

Theorem 1.1.12:

A finite monoid M which is left reducible is a group.

Proof:

We will show that every element is right invertible. We will define a function for every $a \in M$:

$$\ell_a \colon M \longrightarrow M, \qquad x \mapsto ax$$

Then ℓ_a is injective since M is left reducible, if $\ell_a(x) = \ell_a(y)$ then $ax = ay$ so $x = y$. Because M is finite, ℓ_a is surjective, and thus there must be an element x such that $\ell_a(x) = 1$, so $ax = 1$.
So for every $a \in M$ there is an element $x \in M$ such that $ax = 1$, so every a is right invertible. Therefore M is a group.

■

1.2 $\mathbb{Z}$ and an Introduction to Number Theory

We will now focus a bit on the integers, which are the focal point of a field of math called *number theory*.

- $(\mathbb{Z}, +)$ is a group as it has an identity (1) and inverses $(-a)$.
- $(\mathbb{Z}, \cdot)$ is a monoid but not a group since 0 doesn't have an inverse.

Definition 1.2.1:

α is the **greatest common divisor** of a and b if it is the maximum number which divides them both. We denote this as $\gcd(a, b)$. This maximum exists for every a and b unless a and b are both 0, since zero is divisible by every number. $a, b \in \mathbb{Z}$ are **coprime** if their greatest common divisor is 1.

Definition 1.2.2:

$\pm 1, 0 \neq p \in \mathbb{Z}$ is **prime** if for every $a, b \in \mathbb{Z}$, if $p \mid ab$ then $p \mid a$ or $p \mid b$. And a number $\pm 1, 0 \neq a \in \mathbb{Z}$ is **non-compound** if $a = bc$ implies $b = \pm 1$ or $c = \pm 1$.

Every prime is non-compound since if $p = ab$ then $p \mid ab$ so $p \mid a$ or $p \mid b$. Suppose that $p \mid a$, and since $a \mid p$ (since $p = ab$) then $p \mid a \mid p$ so $a = \pm p$. Therefore $b = \pm 1$.

Theorem 1.2.3:

For every $a, b \in \mathbb{Z}$ then there exists $\alpha, \beta = \mathbb{Z}$ such that:

$$\alpha a + \beta b = \gcd(a, b)$$

Proposition 1.2.4:

Every non-compound number is prime.

Proof:

Let p be non-compound. Suppose $p \mid ab$, if $p \mid a$ then we have finished. Otherwise $\gcd(p, a) = 1$ since the greatest common divisor must divide p so it must be 1 or p, and since p doesn't divide a it must be 1. So there must be α, β such that $\alpha p + \beta a = 1$, so $b = \alpha pb + \beta ab$. We know p divides αpb and βab, so $p \mid b$.

■