Categories & Algebras 1

Semigroups and Groups

Graham Campbell

Summer 2017

Binary Operations

Definition (Binary operation)

If G is a non-empty set, then a binary operation on G is a (partial) function from $G \times G$ to G.

Binary Operations

Definition (Binary operation)

If G is a non-empty set, then a binary operation on G is a (partial) function from $G \times G$ to G.

Definition (Groupoid)

If we have non-empty G and binary operation $*$, then we have groupoid $(G, *)$. We write $a * b = c$ when $(a, b) \in G \times G$ is mapped to $c \in G$ under the binary operation.

Binary Operations

Definition (Binary operation)

If G is a non-empty set, then a binary operation on G is a (partial) function from $G \times G$ to G.

Definition (Groupoid)

If we have non-empty G and binary operation $*$, then we have groupoid $(G, *)$. We write $a * b = c$ when $(a, b) \in G \times G$ is mapped to $c \in G$ under the binary operation.

Definition (Magma)

A magma is a groupoid where the binary operation is total.

Semigroups

Definition (Associativity)

Multiplication is associative iff:

$$\forall a, b, c \in G, a(bc) = (ab)c.$$

Semigroups

Definition (Associativity)

Multiplication is associative iff:

$$\forall a, b, c \in G, a(bc) = (ab)c.$$

Definition (Semigroup)

A magma $(G, *)$ is a semigroup iff the binary operation $*$ is associative.

Semigroups

Definition (Associativity)

Multiplication is associative iff:

$$\forall a, b, c \in G, a(bc) = (ab)c.$$

Definition (Semigroup)

A magma $(G, *)$ is a semigroup iff the binary operation $*$ is associative.

Definition (Commutative)

Semigroup G is commutative when $\forall a, b \in G, ab = ba$.

Monoids

Definition (Identity)

Element $1 \in G$ is called a two-sided identity iff:

$$\forall a \in G, a1 = 1a = a.$$

Monoids

Definition (Identity)

Element $1 \in G$ is called a two-sided identity iff:

$$\forall a \in G, a1 = 1a = a.$$

Definition (Monoid)

A monoid G is a semigroup with an identity.

Monoids

Definition (Identity)

Element $1 \in G$ is called a two-sided identity iff:

$$\forall a \in G, a1 = 1a = a.$$

Definition (Monoid)

A monoid G is a semigroup with an identity.

Lemma (Uniqueness)

If G is a monoid, then 1 is unique.

Groups

Definition (Inverses)

Element $a \in G$ has a two-sided inverse iff:

$$\exists a^{-1} \in G, aa^{-1} = a^{-1}a = 1.$$

Groups

Definition (Inverses)

Element $a \in G$ has a two-sided inverse iff:

$$\exists a^{-1} \in G, aa^{-1} = a^{-1}a = 1.$$

Definition (Group)

A group G is a monoid such that each $a \in G$ has an inverse $a^{-1} \in G$.

Groups

Definition (Inverses)

Element $a \in G$ has a two-sided inverse iff:

$$\exists a^{-1} \in G, aa^{-1} = a^{-1}a = 1.$$

Definition (Group)

A group G is a monoid such that each $a \in G$ has an inverse $a^{-1} \in G$.

Lemma

In a monoid, the inverse of a, a^{-1}, is unique if it exists.

Remarks

It turns out that if we simply assume a left identity and left inverses, then this implies the existence of right inverses and a right identity.

Remarks

It turns out that if we simply assume a left identity and left inverses, then this implies the existence of right inverses and a right identity.

Lemma

We can replace the two-sided axioms for a one-sided axioms in the definition of a group.

Remarks

It turns out that if we simply assume a left identity and left inverses, then this implies the existence of right inverses and a right identity.

Lemma

We can replace the two-sided axioms for a one-sided axioms in the definition of a group.

Lemma

In a group, if a is idempotent ($a^2 = a$), then $a = 1$.

Remarks

It turns out that if we simply assume a left identity and left inverses, then this implies the existence of right inverses and a right identity.

Lemma

We can replace the two-sided axioms for a one-sided axioms in the definition of a group.

Lemma

In a group, if a is idempotent ($a^2 = a$), then $a = 1$.

Remark: Amazingly, all finite monoids with exactly one idempotent element, are actually groups!

Homomorphisms 1

Definition (Homomorphism)

Let G and H be semigroups. A function $f : G \to H$ is a homomorphism iff:

$$\forall a, b \in G, f(ab) = f(a)f(b).$$

Homomorphisms 1

Definition (Homomorphism)

Let G and H be semigroups. A function $f : G \to H$ is a homomorphism iff:

$$\forall a, b \in G, f(ab) = f(a)f(b).$$

Definition (Epimorphism)

A surjective (onto) homomorphism is called an epimorphism.

Homomorphisms 1

Definition (Homomorphism)

Let G and H be semigroups. A function $f : G \to H$ is a homomorphism iff:

$$\forall a, b \in G, f(ab) = f(a)f(b).$$

Definition (Epimorphism)

A surjective (onto) homomorphism is called an epimorphism.

Definition (Monomorphism)

An injective (1-1) homomorphism is called a monomorphism.

Homomorphisms 2

Definition (Isomorphism)

A bijective (1-1 and onto) homomorphism is called a isomorphism.

Homomorphisms 2

Definition (Isomorphism)

A bijective (1-1 and onto) homomorphism is called a isomorphism.

Definition (Isomorphic)

We say that $G \cong H$ iff there exists an isomorphism $G \to H$.

Homomorphisms 2

Definition (Isomorphism)

A bijective (1-1 and onto) homomorphism is called a isomorphism.

Definition (Isomorphic)

We say that $G \cong H$ iff there exists an isomorphism $G \to H$.

Definition (Endomorphism)

A homomorphism $f : G \to G$ is an endomorphism.

Homomorphisms 2

Definition (Isomorphism)

A bijective (1-1 and onto) homomorphism is called a isomorphism.

Definition (Isomorphic)

We say that $G \cong H$ iff there exists an isomorphism $G \to H$.

Definition (Endomorphism)

A homomorphism $f : G \to G$ is an endomorphism.

Definition (Automorphism)

An isomorphism $f : G \to G$ is an automorphism.

Image and Kernel

Let $f : G \to H$ be a group homomorphism.

Image and Kernel

Let $f : G \to H$ be a group homomorphism.

Definition (Kernel)

The kernel of f is $Ker(f) = \{g \in G \mid f(g) = 1_H\}$.

Image and Kernel

Let $f : G \to H$ be a group homomorphism.

Definition (Kernel)

The kernel of f is $Ker(f) = \{g \in G \mid f(g) = 1_H\}$.

Definition (Image)

The image of f is $Im(f) = f(G) = \{f(g) \mid g \in G\}$.

Image and Kernel

Let $f : G \to H$ be a group homomorphism.

Definition (Kernel)

The kernel of f is $Ker(f) = \{g \in G \mid f(g) = 1_H\}$.

Definition (Image)

The image of f is $Im(f) = f(G) = \{f(g) \mid g \in G\}$.

Lemma

f is a monomorphism iff $Ker(f) = \{1_G\}$.

Algebraic structures

So, we've seen groupoids, and how we can build "group-like" structures with them. We can abstract this concept.

Algebraic structures

So, we've seen groupoids, and how we can build "group-like" structures with them. We can abstract this concept.

Definition (Algebraic structure)

An algebraic structure is a non-empty set, with zero or more binary operations.

Algebraic structures

So, we've seen groupoids, and how we can build "group-like" structures with them. We can abstract this concept.

Definition (Algebraic structure)

An algebraic structure is a non-empty set, with zero or more binary operations.

For example, a **set** is a degenerate algebraic structure, with no binary operations.

Examples

Examples of structures with two operations are:

Examples

Examples of structures with two operations are:

1. Ring-like structures (semirings, rings, fields)

Examples

Examples of structures with two operations are:

1. Ring-like structures (semirings, rings, fields)
2. Lattice structures (distributive lattices, boolean algebras)

Examples

Examples of structures with two operations are:

1. Ring-like structures (semirings, rings, fields)
2. Lattice structures (distributive lattices, boolean algebras)
3. Module-like structures (modules, vector spaces)

Examples

Examples of structures with two operations are:

1. Ring-like structures (semirings, rings, fields)
2. Lattice structures (distributive lattices, boolean algebras)
3. Module-like structures (modules, vector spaces)

Examples of structures with four operations are bialgebras.

Unfortunately, we don't have time to explore these in any detail, but it's good to know they exist.