Groups Review

Yichen Xu

November 9, 2019

Outline

Outline of today's lecture

1. Fundamentals
2. Definition and properties of semigroup, monoid, and group
3. Subalgebra, quotient algebra & product algebra
4. Homomorphism & isomorphism
5. Application: group codes

Fundamentals

1. What is mathematical structures?
2. About binary operations

Semigroup, monoid & group

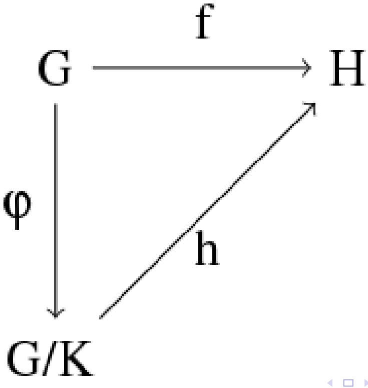
1. Definitions
2. properties & important theorems

Subalgebra, quotient algebra & product algebra

1. Definitions & properties
2. Ways to find them
3. Important: quotient algebra

Homomorphism & isomorphism

1. Definition & properties
2. Fundemantal homomorphism
3. Normal subgroups



What is mathematical structures?

- Another name: space
- In mathematics, a structure on a set is an additional mathematical object that, in some manner, attaches (or relates) to that set to endow it with some additional meaning or significance.
- Two main elements:
  1. A set of objects
  2. An operation

Binary operations on a set

- Definition: An operation defined on a set K that combines two objects
- $f : K \times K \to K$

Example (Common binary operations)

- $+, -, \cdot, /$
- $\cap, \cup$ (Defined on the set of sets)

Properties of a binary operation

Commutative

$$x \cdot y = y \cdot x$$

Notes: $\cdot$ is commutative $\Leftrightarrow$ $x_1 \cdot_2 \cdots \cdot x_n$ can be arranged in arbitary order.

Associative

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

Distributive

$$x(y + z) = xy + xz$$

Identity for a binary operation

Definition (Identity)

Given a binary operation $\cdot$defined on S, if $e \in S$ satisfis

$$x \cdot e = e \cdot x = x,$$

then e is an identity.

Theorem (Uniqueness)

The identity e for a binary operation $\cdot$ is unique.

Proof.

Assume that there exist two identity e_1, e_2 for the operation,

$$e_1 = e_1 \cdot e_2 = e_2.$$

Inverse under a binary operation

Definition (Inverse)

If a binary operation $\cdot$ has an identity e, we call y a 2-inverse of x if $xy = yx = e$. y is often denoted x^{-1}.

Theorem (Uniqueness)

If x has a 2-inverse, then it is unique.

Proof.

$$y_1 = y_1 e = y_1(xy_2) = (y_1 x)y_2 = ey_2 = y_2.$$

□

Closed binary operation

A binary operation $\cdot$ is called closed when

$$\forall x, y \in S, x \cdot y \in S.$$

Summary

- Mathematical structure: set + operation
- Binary operation
  - Properties: commutative, associative, dirtributive
  - Indentity & inverse
  - Closed binary operation

Semigroups, monoids and groups

Core of group theory: homomorphism & isomorphism.
In `Algebra`:

> *Groups which are, from the point of view of algebraic structure, essentially the same are said to be isomorphic. Ideally the goal in studying groups is to classify all groups up to isomorphism, which in practice means finding necessary and sufficient conditions for two groups to be isomorphic.*

Semigroups & monoids

Semigroup

A semigroup is a nonempty set G together with a binary operation on G which is associative:

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

Monoid

A monoid is a semigroup G whose binary operation has a (two-sided) identity element:

$$ea = ae = a \forall a \in G.$$

Groups

Group

A group is a monoid G such that

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

Property: theorem of identity

Theorem

If $c \in G$ and $cc = c$, then $c = e$.

Proof.

$$c = cc \Leftrightarrow c^{-1}c = c^{-1}cc \Leftrightarrow e = (c^{-1}c)c \Leftrightarrow e = c.$$

□

Property: left and right cancellation

Theorem

$$\forall a, b, c \in G, ca = cb \Leftrightarrow a = b \Leftrightarrow ac = bc.$$

We can also deduce that $ax = b$ has unique solution.

Other properties

- ${a^{-1}}^{-1} = a$
- $(ab)^{-1} = b^{-1}a^{-1}$

Examples

Example (I)

Let G be a semigroup. Then G is a group iff it has a left identity and $\forall a \in G$ has a left inverse.

Proof.

$(\Rightarrow)$ is trivial.
$(\Leftarrow)$: Observe that $(aa^{-1})(aa^{-1}) = a(a^{-1}a)a^{-1} = aea^{-1} = aa^{-1}$, thus $aa^{-1} = e$. a^{-1} is a two-sided inverse. Also, $ae = a(a^{-1}a) = (aa^{-1})a = ea = a$, e is a two-sided inverse. □

Examples

Example (II)

Let G be a semigroup. Then G is a group iff $\forall a, b \in G$ the equations $ax = b, ya = b$ have solutions in G.

Hints

First, fix a to show that G has a right identity. Then prove the existence of left identity similarly.

Examples

Proof.

For $a \in G$, we can show that $\exists e_a \in G, ae_a = a$. Then for $\forall b \in G, \exists y, b = ya$,

$$be_a = yae_a = y(ae_a) = ya = b.$$

e_a is a right inverse. Similarly, we have a left inverse e_b.

$$e_a = e_b e_a = e_b.$$

G is a monoid. And $\forall a \in G, ax = e$ has solution. By the previous example, G is a group. □

Subalgebras

Subsemigroup

A subsemigroup $H \subseteq G$ is a subset of semigroup G which is closed.

Submonoid

A monoid H is a subsemigroup of monoid G with $e \in H$.

Subgroup

A subgroup H is a submonoid of group G such that $\forall a \in H, a^{-1} \in H$.

Finding subalgebras I

If G is a group, then

- $H = \{a^i \mid i \in Z^+\}$ is a subsemigroup of G.
- $H = \{a^i \mid i \in N\}$ is a submonoid of G.
- $H = \{a^i \mid i \in Z\} isasubgroupofG$ (generated by a).

Finding subalgebras II

If G is a group, H is a subset of G, then if $\forall a, b \in H$, $a^{-1}b \in H$, then H is a subgroup of G.

Proof.

1. $a^{-1}a = e \in H$;
2. $\forall a \in H, a^{-1}e = a^{-1} \in H$;
3. $\forall a, b \in H, a^{-1} \in H, (a^{-1})^{-1}b = ab \in H$.

□

Product algebra

Theorem

If S, T is a groupoid (shorthand for semigroup, monoid or group), then $S \times T$ is also a groupoid.

Quotient algebra

Divide a algebra by a congruence relation defined on it.

- What is a congruence relation?
- How to define a new algebra based on the relation?

Recall: equivalence relation

A equivalence relation R is a relation that is

1. Reflexive: $\forall a \in S, aRa$;
2. Symmetric: $\forall a, b \in S, aRb \Rightarrow bRa$;
3. Transitive: $\forall a, b, c \in S, aRb, bRc \Rightarrow aRc$.

Congruence relation

A congruence relation R is a equivalence relation defined on a semigroup G that satisfies

$$\forall a, a', b, b' \in G, aRa', bRb' \Rightarrow abRa'b'.$$

Quotient group

Given a congruence relation R defined on a group G, then the set G/R with a binary operation $\odot$ defined as

$$\forall [a], [b] \in G/R, [a] \odot [b] = [a \cdot b].$$

Proof.

- $[a] \odot [b] \odot [c] = [abc] = [a(bc)] = [a] \odot [bc] = [a] \odot ([b] \odot [c]);$
- $[e] \in G/R$ is an identity:
  $[e] \odot [a] = [ea] = [a] = [ae] = [a] \odot [e];$
- $\forall [a] \in G/R, \exists [a^{-1}] \in G/R, [a] \odot [a^{-1}] = [a^{-1}] \odot [a] = [e].$

□

Summary

- Semigroup, monoid & group
  - Definition
  - Properties
- Subalgebra
  - Definition: subsemigroup, submonoid & subgroup
  - Finding subalgebras
- Product algebra
- Quotient algebra
  - Congruence relation
  - Definition

Outline

- Some definitions
  - Homomorphism
  - Coset
  - Normal subgroups
- Equivalent statements
  - A onto homomorphism
  - A congruence relation
  - A normal subgroup
- Fundamental homomorphism theorem

What is homomorphism?

- In short, homomorphism is a mapping that preserves the structure of an algebra.
- Definition: Let G, H be semigroups. A function $f : G \to H$ is a homomorphism if

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

- f is injective: monomorphism; f is surjective: epimorphism (onto homomorphism); f is bijective: isomorphism.

What is coset?

If H is a subgroup of G, and $a \in G$, the left and right coset of H in G determined by a is the sets

$$aH = \{ah \mid h \in H\}; Ha = \{ha \mid h \in H\}.$$

What is normal subgroup?

A subgroup N is called normal when $\forall a \in G, aH = Ha$.

To prove that they are all equivalent

1. Onto homomorphism
2. Congruence relation
3. Normal subgroup

First prove that: onto homomorphism $\Leftrightarrow$ congruence relation;
Then: congruence relation $\Leftrightarrow$ normal subgroup.

Onto homomorphism $\Leftrightarrow$ congruence relation

Onto homomorphism $\Rightarrow$ congruence

If G is a groupoid, and f is an onto homomorphism from G to G', then the relation R defined by aRb iff $f(a) = f(b)$ is a congruence relation.

Onto homomorphism ⇔ congruence relation

Congruence ⇒ onto homomorphism

Given a semigroup G, and a congruence relation R defined on it. Then the map

$$f(a) = [a]$$

is a homomorphism, called natural homomorphism.

Proof.

We have known that G/R is a semigroup.

$$f(ab) = [ab] = [a] \odot [b] = f(a) \odot f(b).$$

□

Homomorphism ⇔ congruence relation

Remarks

It can be shown that there is a bijection between onto homomorphism and congruence relation. It means that, onto homomorphism and congruence relations are actually the same thing.

Congruence relation ⇔ normal subgroup

Congruence relation ⇒ normal subgroup

If R is a congruence relation defined on a groupoid G, then $[e]$ is a normal subgroupoid of G.

Proof

- First, show that $H = [e]$ is normal. To prove that, we show that $[a] = aH = Ha$. $\forall b \in [a]$,

$$
\begin{aligned}
& b \in [a] \\
\Leftrightarrow & [b] = [a], \\
\Leftrightarrow & [e] = [a]^{-1}[a] = [a^{-1}b] = H, \\
\Leftrightarrow & a^{-1}b \in H, \\
\Leftrightarrow & b \in aH, \\
\Leftrightarrow & [a] = aH.
\end{aligned} \tag{1}
$$

Congruence relation $\Leftrightarrow$ normal subgroup

Congruence relation $\Rightarrow$ normal subgroup

Proof (Cont.)

Similarly, we can prove that $[a] = Ha$. Thus H is normal.

- Then, show that H is a subgroupoid. That is, show that H is closed. As shown in Eq. 1, $\forall a, b, [a] = [b] \Rightarrow a^{-1}b \in [e]$. Then

$$\forall a \in H = [e], a^{-1}e = a^{-1} \in H.$$

And

$$\forall x, y \in H, x^{-1} \in H, {x^{-1}}^{-1}y = xy \in H. \square$$

Congruence relation ⇔ normal subgroup

Normal subgroup ⇒ congruence relation

Let N be a normal subgroup of a group G, R be the relation on G defined by

$$aRb \Leftrightarrow a^{-1}b \in N,$$

then R is a congruence relation on G, and N is the equivalent class [e].

Proof

(1) R is a equivalent relation. Ommited. (2) R is a congruence relation. $\forall aRb, cRd$, we have $a^{-1}b \in N, c^{-1}d \in N$. We are to prove that $(ac)^{-1}bd \in N$. $(ac)^{-1}bd = c^{-1}a^{-1}bd$. We can use the 'associativity' of normal subgroups to rearrange the equation in the form of the multiplication of two elements in the subgroup.

Congruence relation ⇔ normal subgroup

Normal subgroup ⇒ congruence relation

Proof (Cont.)

Since N is a normal subgroup, $Nd = dN$. Then $\exists n \in N, a^{-1}bd = dn$. $(ac)^{-1}bd = c^{-1}(a^{-1}bd) = c^{-1}dn \in N$. $acRbd$.

Congruence relation $\Leftrightarrow$ normal subgroup

Remarks

It can also be proven that, there is a bijection between congruence relations and normal subgroups. Congruence relations and normal subgroups are actually the same thing.
Now we prove that, a homomorphism, a congruence relation and a normal subgroup on a group is essentially the same thing. All we've done before actually proved the following theorem: *the fundamental theorem on homomorphism*.

Fundamental theorem on homomorphism

If $\varphi : G \rightarrow G'$ is an onto homomorphism, then $Ker(\varphi)$ is a normal subgroup of G, and $G/Ker(\varphi)$ is isomorphic to $\varphi(G)$.

Kernel of a homomorphism

Kernel of a homomorphism $\varphi : G \rightarrow G'$ is defined as

$$Ker(\varphi) = \{a \in G \mid \varphi(a) = e\}.$$

Proof

- $Ker(\varphi)$ is a normal subgroup. As proven before: there is a congruence relation R defined by the homomorphism as aRb iff $\varphi(a) = \varphi(b)$. Observe that the equivalent class $[e]$ is the kernel of the homomorphism $Ker(\varphi)$. And $[e]$ is a normal subgroup.

Fundamental theorem on homomorphism

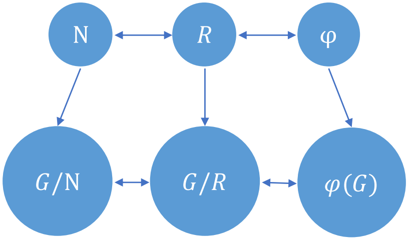
Proof (Cont.)

- The isomorphism (one-to-one homomorphism) can be easily found with the congruence relation bridging the normal subgroup and the homomorphism. Note that the congruence relation defined by the homomorphism φ is also the one divided by the normal subgroup $Ker(\varphi)$. And there is a bijection between the equivalence classes and the image of φ.

Summary

- Homomorphism
- Coset, normal subgroup
- They are equivalent:
  - Homomorphism (Defined by the congruence relation, defined by the normal subgroup)
  - Congruence relation (Defined by the homomorphism, divided by the normal subgroup)
  - Normal subgroup (Kernel of the homomorphism, $[e]$ of the congruence relation)
- Fundemental theorem on homomorphism
  - Definitely! We've seen that the homomorphism and the normal subgroup are essentially the same thing. The image of the homomorphism and the quotient group divided by the normal subgroup should be isomorphic.

Summary



Thank you!

- Slides available at `http://tinyurl.com/y6cqqbco`
- Slides made with Emacs & LaTeX