Groups

Doan Nhat Quang

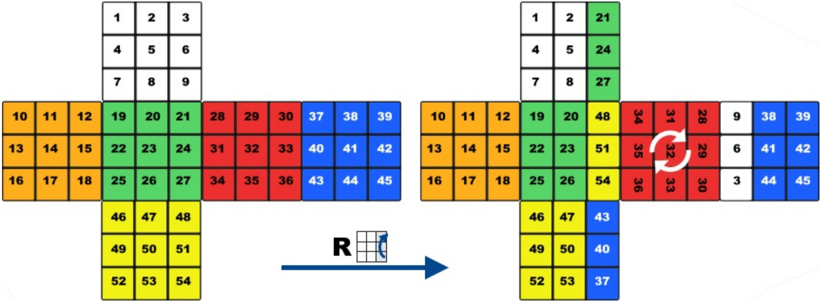
doan-nhat.quang@usth.edu.vn
University of Science and Technology of Hanoi
ICT department

Algebraic Structure

Definition

In mathematics, an algebraic structure consists of a non-empty set A, a collection of operations on A (typically binary operations such as addition and multiplication), and a finite set of identities, known as axioms, that these operations must satisfy.

- Groups, Rings, Fields
- Lattice, Module



Group Permutation: `https://ruwix.com/the-rubiks-cube/mathematics-of-the-rubiks-cube-permutation-group/`

Group Applications

- Ring and Fields: Define more advanced algebraic structures
- Group Theory
- Chromatic circle in music theory: the twelve equal-tempered pitch classes can be represented by the cyclic group of order twelve, or, equivalently, the residue classes modulo twelve.
- etc.

Group Applications

- Coding Theory
  - Error Correcting Code: a simple example is to transmit each data bit 3 times
  - Hamming Distance
- Information theory: Manchester code
- Crystallography (Chemistry): Symmetry groups consist of symmetries of given mathematical objects, principally geometric entities.
- and more.....

Binary operations

$$\star : S \times S \to S, (a, b) \to a \star b$$

A map is called a binary operation on S. So $\star$ takes 2 inputs a, b from S and produces a single output $a \star b \in S$.

Properties

Let $\star$ be a binary operation on a set S. There exists several properties:

- $\star$ is *commutative* if, $\forall a, b \in S$

$$a \star b = b \star a$$

- $\star$ is *associative* if, $\forall a, b, c \in S$

$$(a \star b) \star c = a \star (b \star c)$$

Example 1

Addition, $+$, is a commutative and associative binary operation in $\mathbb{N}, \mathbb{Z}, \mathbb{Q}, \mathbb{R}, \mathbb{C}, M \in \mathbb{R}^{m\times n}$

Example 1

Addition, $+$, is a commutative and associative binary operation in $\mathbb{N}, \mathbb{Z}, \mathbb{Q}, \mathbb{R}, \mathbb{C}, M \in \mathbb{R}^{m\times n}$

Example 2

Is Addition, $+$, a commutative and associative binary operation in $S = \{0, 1\}$?

Example 1

Addition, $+$, is a commutative and associative binary operation in $\mathbb{N}, \mathbb{Z}, \mathbb{Q}, \mathbb{R}, \mathbb{C}, M \in \mathbb{R}^{m \times n}$

Example 2

Is Addition, $+$, a commutative and associative binary operation in $S = \{0, 1\}$?

Example 3

Is Subtraction, -, is a commutative and associative binary operation in $\mathbb{N}, \mathbb{Z}, \mathbb{Q}, \mathbb{R}, \mathbb{C}$?

Example 4

Multiplication, ., is a commutative and associative binary operation in $\mathbb{N}, \mathbb{Z}, \mathbb{Q}, \mathbb{R}, \mathbb{C}$ but not $M \in \mathbb{R}^{m \times n}$

Example 4

Multiplication, ., is a commutative and associative binary operation in $\mathbb{N}, \mathbb{Z}, \mathbb{Q}, \mathbb{R}, \mathbb{C}$ but not $M \in \mathbb{R}^{m\times n}$

Example 5

Scalar product on $\mathbb{R}^2$ is given by $(a_1, a_2).(b_1, b_2) = a_1b_1 + a_2b_2$. Is it binary operation and commutative or associative?

Example 4

Multiplication, ., is a commutative and associative binary operation in $\mathbb{N}, \mathbb{Z}, \mathbb{Q}, \mathbb{R}, \mathbb{C}$ but not $M \in \mathbb{R}^{m \times n}$

Example 5

Scalar product on $\mathbb{R}^2$ is given by $(a_1, a_2).(b_1, b_2) = a_1 b_1 + a_2 b_2$. Is it binary operation and commutative or associative?

Example 6

Vector product on $\mathbb{R}^2$ is given by $(a_1, a_2).(b_1, b_2) = (a_1 b_1, a_2 b_2)$. Is it binary operation and commutative or associative?

Definition 1

Let G be a non-empty set and let $\star$ be a binary operation on G:

$$\star : G \times G \to G, (a, b) \to a \star b$$

Then $(G; \star)$ is a group if the following axioms are satisfied:

- G1 - **associative**: $\forall a, b, c \in G$, $(a \star b) \star c = a \star (b \star c)$
- G2 - **identity element:** there exists $e \in G$ such that $a \star e = e \star a = a, \forall a \in G$
- G3 - **inverse element**: for any $a \in G$, there exists a^{-1} such that $a \star a^{-1} = a^{-1} \star a = e$

$(G; \star)$ is called an abelian group, or simply a *commutative group if* $\forall a, b \in G, a \star b = b \star a$

Example 1

$(\mathbb{Z}, +)$

- G1 - $+$ is **associative**: $\forall a, b, c \in \mathbb{Z}$, $(a + b) + c = a + (b + c)$
- G2 - 0 is **identity element:** $a + 0 = 0 + a = a, \forall a \in \mathbb{Z}$
- G3 - **inverse element**: for any $a \in \mathbb{Z}$, there exists $-a$ such that $a + (-a) = (-a) + a = 0$
- G4 - $+$ is **commutative** $\forall a, b \in \mathbb{Z}, a + b = b + a$

Example 2

Same for $(\mathbb{Z}, +)$, all $(\mathbb{R}, +)$, $(\mathbb{Q}, +)$, and $(\mathbb{C}, +)$.

Example 3

$(\mathbb{Z}, .)$, $(\mathbb{R}, .)$, $(\mathbb{Q}, .)$, and $(\mathbb{C}, .)$ are abelian groups?

Example 4

We use $\mathbb{M}_2(\mathbb{R})$ to denote the set of all 2×2 matrices.

- $(\mathbb{M}_2(\mathbb{R}), +)$ is an abelian group?
- $(\mathbb{M}_2(\mathbb{R}), .)$ is an abelian group?

Proposition 1

The **identity element** in a group G is unique; that is, there exists only one element $e \in G$ such that $e \star g = g \star e = g$, $\forall g \in G$.

Proposition 1

The **identity element** in a group G is unique; that is, there exists only one element $e \in G$ such that $e \star g = g \star e = g$, $\forall g \in G$.

Proof

if e is not unique, we suppose to have another identity element e' then we have both:

$$e \star g = g \star e = g \text{ and } e' \star g = g \star e' = g$$

so

- if e is identity element then $e \star e' = e'$
- if e' is identity element then $e' \star e = e$
- G is a group then $e = e \star e' = e' \star e = e'$ (Q.E.D.)

Proposition 2

If g is any element in a group G, then the inverse of g, g', is unique.

Proposition 2

If g is any element in a group G, then the inverse of g, g', is unique.

Proof

if the inverse of g is not unique, we suppose to have g' and g'' are inverses of g:

$$g \star g' = g' \star g = e \text{ and } g \star g'' = g'' \star g = e$$

but we have associative property in G, thus:

$$g' = g' \star e = g' \star (g \star g'') = (g' \star g) \star g'' = e \star g'' = g''$$

Proposition 3

Let G be a group. If $a, b \in G$, then $(a \star b)^{-1} = b^{-1} \star a^{-1}$

Proposition 3

Let G be a group. If $a, b \in G$, then $(a \star b)^{-1} = b^{-1} \star a^{-1}$

Proof

We have

$$a \star b \star b^{-1} \star a^{-1} = a \star e \star a^{-1} = a \star a^{-1} = e$$

Similarly, we have

$$(a \star b) \star (a \star b)^{-1} = e$$

Due to Proposition 2, inverse is unique

$$(a \star b)^{-1} = b^{-1} \star a^{-1}$$

Proposition 4

Let x be an element of a group G , then $x^{m+n} = x^m \star x^n$ for all integers m, n. We also define $x^0 = e$.
We denote here $x^n = x \star x \star ... \star x$ (n times).

Proposition 4

Let x be an element of a group G , then $x^{m+n} = x^m \star x^n$ for all integers m, n. We also define $x^0 = e$.
We denote here $x^n = x \star x \star ... \star x$ (n times).

Proof

Hint: Use induction

Definition 2

The order of an algebraic structure $(G, \star)$ is the cardinality of its underlying set, and is denoted $|G|$.

For a finite set G, the order of $(G, \star)$ is the number of elements in G.

For a finite set G, the order of $(G, \star)$ is the smallest integer number such that $a^m = e, \forall a \in G$.

Let g be an element of a group G, we say that g has finite order if $g^n = e$ $(o(g) = |g| = n)$for some positive integer n.

Otherwise, if g is said to have the infinite order, $o(g) = \infty$

SubGroups

Definition 1

Let G be a group, a subset H of G is a **subgroup** if and only if it satisfies the following conditions:

- the identity e of G is in H
- if $h_1, h_2 \in H$ then $h_1 \star h_2 \in H$ as well
- if $h \in H$ then $h^{-1} \in H$

SubGroups

- A subgroup H of G is said to be *proper* if $H \neq G$.
- The subgroup $H = \{e\}$ of a group G is called the *trivial* subgroup.

Proposition 1

Let H and K be subgroups of a group G, then $H \cap K$ is also a subgroup of G.

Proof

- H and K must have the same identity from G, then the identity element belong to $H \cap K$.
- if x and y are elements of $H \cap K$ then $x \star y$ is an element of H since x and y are elements of H. Same goes for $x \star y \in K$. Thus, $x \star y \in H \cap K$
- Same proof for the inverse x^{-1} of an element as required.

SubGroups

Example 1

The group of integers is a subgroup of the groups of rational numbers, real numbers and complex numbers under addition.

Example 1

The group of integers is a subgroup of the groups of rational numbers, real numbers and complex numbers under addition.

Example 2

Consider the set of non-zero real numbers, $\mathbb{R}^*$, with the group operation of multiplication. The identity of this group is 1 and the inverse of any element $a \in \mathbb{R}^*$ is just $1/a$.
$\mathbb{Q}^*$ is a subgroup of $\mathbb{R}^*$.

- the identity of $\mathbb{Q}^*$ is $1/1 = 1 \in \mathbb{R}^*$
- let 2 numbers q/r and $s/t \in \mathbb{Q}^*$, then $q/r.s/t \in \mathbb{Q}^*$
- the inverse of q/r is $(q/r)^{-1} = r/q \in \mathbb{Q}^*$

Example 3

The group of all 2×2 matrices of real numbers with determinant equal to 1 is a subgroup of the group of all 2×2 matrices of real numbers with non-zero determinant under the operation of matrix multiplication.

Example 3

The group of all 2×2 matrices of real numbers with determinant equal to 1 is a subgroup of the group of all 2×2 matrices of real numbers with non-zero determinant under the operation of matrix multiplication.

Example 4

Let $H = \{-1, 1, i, -i\}$ is a subgroup of $\mathbb{C}$ under multiplication.

Cyclic Groups

Definition 1

The order of a group G, denoted by $|G|$, is the cardinality of G, that is the number of elements in G.

Definition 2

A group G is said to be cyclic, with generator g, if every element of G is of the form $g^n = g \star g \star ... \star g$ for some integer n. We often denote $G =< g >$ or (g)

Cyclic Groups

Example 1

The group $\mathbb{Z}$ of integers under addition is a cyclic group, generated by 1 and -1.

Example 1

The group $\mathbb{Z}$ of integers under addition is a cyclic group, generated by 1 and -1.

Example 2

Let n be a positive integer. The set $\mathbb{Z}_n$ of integers modulo n is a cyclic group of order n with respect to the operation of addition.

$$\mathbb{Z}_n = \{0, 1, 2, ..., n - 1\}$$

For example:

$$\mathbb{Z}_9 = \{0, 1, 2, ..., 8\}$$

Example 3

Let a subgroup $U_9 \in \mathbb{Z}_9$ with $U_9 = \{1, 2, 4, 5, 7, 8\}$ is a cyclic group under multiplication. Every member of this set is generated by 2.

$$2^1 = 2 \pmod 9, 2^2 = 4 \pmod 9$$

$$2^3 = 8 \pmod 9, 2^4 = 7 \pmod 9$$

$$2^5 = 5 \pmod 9, 2^6 = 1 \pmod 9$$

Proposition 1

Every cyclic group is abelian.

Proof

Let G be a cyclic group and $a \in G$ be a generator for G. If $g, h \in G$, then they can written as powers of a, denoted by $g = a^m$ and $h = a^n$

If G is abelian thus, $g \star h = h \star g$. We have here:

$$g \star h = a^m \star a^n = a^{m+n} = a^{n+m} = a^n \star a^m = h \star g$$

Cosets

Definition 1

Let H be a subgroup of a group G. A **left coset** of H in G is a subset of G that is of the form $x \star H$, where $x \in G$ and

$$x \star H = \{y \in G : y = x \star h \text{ for some } h \in H\}$$

Definition 2

Similarly, a **right coset** of H in G is a subset of G that is of the form $H \star x$, where $x \in G$ and

$$H \star x = \{y \in G : y = h \star x \text{ for some } h \in H\}$$

Example 1

Let H be a subgroup of $\mathbb{Z}_6$ consisting of elements 0 and 3 or $H = \{0, 3\}$, the cosets are:

$$0 + H = 3 + H = \{0, 3\}$$

$$1 + H = 4 + H = \{1, 4\}$$

$$2 + H = 5 + H = \{2, 5\}$$

Definition 3

The index of a subgroup H in G is the number of right (left) cosets. It is a positive number or ∞ and is denoted by $[G : H]$.

Example 1

Let H be a subgroup $\mathbb{Z}_6$ consisting of elements 0 and 3 or $H = \{0, 3\}$, the cosets are:

$$0 + H = 3 + H = \{0, 3\}$$

$$1 + H = 4 + H = \{1, 4\}$$

$$2 + H = 5 + H = \{2, 5\}$$

The index of H is 3.

Proposition 1

Let H be a subgroup of a group G. Then each left coset of H in G has the same number of elements as H.

Proposition 1

Let H be a subgroup of a group G. Then each left coset of H in G has the same number of elements as H.

Proof

Let $H = \{h_1, h_2, ..., h_m\}$ where $h_1, h_2, ..., h_m$ are distinct. Let x be element in G, then the left coset is $x \star H$. We suppose to have $x \star h_i = x \star h_j \in x \star H$ where i, j are integers from 1 to m, and we expect that $h_i \neq h_j$. But

$$h_i = x^{-1} \star x \star h_i = x^{-1} \star x \star h_j = h_j$$

Thus $i = j$ so $x \star H$ have distinct elements.

Proposition 2

Let H be a subgroup of a group G. The number of left cosets of H in G is the same as the number of right cosets of H in G.

Proposition 2

Let H be a subgroup of a group G. The number of left cosets of H in G is the same as the number of right cosets of H in G.

Proof

Let r be exactly different left cosets of H in G, thus we have the left cosets:

$$g_1 \star H, g_2 \star H, ..., g_r \star H : g_1, g_2, ..., g_r \in G$$

$$\begin{aligned}
& x \in H \star g_i^{-1} && \text{Proposition 1} \\
\iff \quad & x \star (g_i^{-1})^{-1} \in H \star g_i^{-1} \star (g_i^{-1})^{-1} && \\
\iff \quad & x \star g_i \in H \star e && \\
\iff \quad & (x^{-1})^{-1} \star g_i \in H && \\
\iff \quad & x^{-1} \in g_i \star H && \text{Proposition 1}
\end{aligned}$$

Proposition 3

Let H be subgroups of a group G, then the left cosets of H in G have the following properties:

- $x \in x \star H$, for all $x \in G$
- if x and y are elements of G, and if $y = x \star g$ for some $g \in H$ then $x \star h = y \star h$

Proposition 3

Let H be subgroups of a group G, then the left cosets of H in G have the following properties:

- $x \in x \star H$, for all $x \in G$
- if x and y are elements of G, and if $y = x \star g$ for some $g \in H$ then $x \star h = y \star h$

Proof

- Let $x \in G$, then $x = x \star e$ where e is the identity element of G and $e \in H$, thus $x \in x \star H$ (according to the subgroup definition)
- Let x and y be elements of G, where $y = x \star g$ for some $g \in H$, then $y \star h = x \star g \star h$ and $x \star h = y \star (g^{-1}) \star h$ for all $h \in H$. Moreover $g \star h \in H$, thus $y \star H \subset x \star H$ and $g^{-1} \star h \in H$ thus $x \star H \subset y \star H \iff x \star H = y \star H$.

Lagrange's Theorem

Theorem

Let G be a finite group and H be a subgroup of G, then $|H|$ divides $|G|$ where $|H|$ and $|G|$ are orders of H and G respectively. or $[G : H] = \frac{G}{H}$ where $[G : H]$ is the index of H in G.

Proof

- Each element of G belongs to at least one left coset of H in G, and no element can belong to two distinct left cosets of H in G. (Lemma 1)
- Therefore every element of G belongs to exactly one left coset of H. Moreover each left coset of H contains $|H|$ elements (Lemma 2).
- Therefore $|G| = n|H|$, where n is the number of left cosets of H in G. The result follows.

Normal Subgroups

Definition

A subgroup H of a group G is normal in G if $g \star H = H \star g$ for all $g \in G$.

A normal subgroup of a group G is one in which the right and left cosets are precisely the same.

Example 1

Let G be an abelian group. Every subgroup H of G is a normal subgroup. Since $g \star h = h \star g$ for all $g \in G$ and $h \in H$, it will always be the case that $g \star H = H \star g$.