Group

November 5, 2019

1 Algebraic System and Operation

Let A, B be two non-empty sets.
An operation on A is a map from A^n to B.
An algebraic system includes a set A and some operations defined on A. An algebraic system is denoted as $(A, f_1, f_1, \cdots f_k)$.

1.1 Properties of Operations

Let $(A, \circ)$ be an algebraic system.

1. Closure.
$$\forall x, y \in A \quad x \circ y \in A$$
2. Associativity.
$$\forall x, y, z \in A \quad (x \circ y) \circ z = x \circ (y \circ z)$$
3. Commutativity.
$$\forall x, y \in A \quad x \circ y = y \circ x$$

Let $(A, \circ, *)$ be an algebraic system.

1. Distributivity.
$$\forall x, y, z \in A \quad x \circ (y * z) = (x \circ y) * (x \circ z) \text{ and } x * (y \circ z) = (x * y) \circ (x * z)$$
2. Absorption.
$$\forall x, y \in A \quad x \circ (x * y) = x \text{ and } x * (x \circ y) = x$$

1.2 Identity

Let $(A, \circ)$ be an algebraic system.

1. Left identity $e_l \in A$. For all $x \in A$, $e_l \circ x = x$.
2. Right identity $e_r \in A$. For all $x \in A$, $x \circ e_r = x$.
3. An algebraic system can contain none or several left identities. An algebraic system can also contain none or several right identities. However, if an algebraic system contains at least one left identity and at least one right identity, then the left identities and right identities are the same, and the identity is unique.

1.3 Inverse

Let $(A, \circ)$ be an algebraic system and e is the identity of $(A, \circ)$.

1. b is a left Inverse of a. $b \circ a = a$.
2. b is a right Inverse of a. $a \circ b = a$.
3. If b is a left Inverse of a and it is also a right Inverse of a, then b is an inverse of a, and a is also an inverse of b.

Let $(A, \circ)$ be an algebraic system and the operator $\circ$ satisfies associativity. If for all $x \in A$, there exists the left inverse of x, $x_l^{-1} \circ x = e$, then the left inverse of x is also its right inverse. (I.e. $x_l^{-1} = x_r^{-1}$) Meanwhile, the inverse of x is unique.

Proof. Let $x_l^{-1} \circ x = e$, and $b \circ x_l^{-1} = e$.

$$x \circ x_l^{-1} = (b \circ x_l^{-1}) \circ x \circ x_l^{-1} = b \circ x_l^{-1} = e$$

and if x_1^{-1}, x_2^{-1} are both inverses of x, then

$$x_1^{-1} = x_1^{-1} \circ (x \circ x_2^{-1}) = x_2^{-1}$$

2 Group

A *group* is a pair $(G, \cdot)$ where G is a set and $\cdot : G \times G \to G$, called the group operation and pronounced as "the product", that satisfies:
(i) for all $x, y, z \in G$, $x \cdot (y \cdot z) = (x \cdot y) \cdot z$ (Associativity)
(ii) there exists $e \in G$, called an identity, such that for all $x \in G$,

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

and for all $x \in G$, there exists $y \in G$ such that

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

where the element y is called an inverse of x. (Closure. Associativity. Unique identity. Every element is invertible.)

Let $(G, \cdot)$ be a group. The element $e \in G$ such that for all $x \in G, x \cdot e = e \cdot x = x$ is unique. Moreover, for all $x \in G$, there exists a unique $y \in G$ such that $x \cdot y = y \cdot x = e$. (We will write x^{-1} for the unique inverse of x in $(G, \cdot)$.)

Let $(G, \cdot)$ be a group. We say that $(G, \cdot)$ is *abelian*, if for all $x, y \in G, x \cdot y = y \cdot x$.

3 Algebra in Groups

Let $(G, \cdot)$ be a group. If $a, b, c \in G$ and $a \cdot b = a \cdot c$, then $b = c$.
Proof: If $a \cdot b = a \cdot c.$, then

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

Let $(G, \cdot)$ be a group and $a \in G$. If $a \cdot a = a$, then $a = e$. $(a \cdot a = a = a \cdot e)$

Let $(G, \cdot)$ be a group and let $x \in G$. If $y \in G$ is such that $y \cdot x = e$, then $x \cdot y = e$.
Proof:

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

4 The Symmetric Group

Let $X = \{f : [n] \to [n] | f \text{ is a bijection}\}$. The group $(X, \circ)$ is call the symmetric group on n elements and is written S_n.

(Cycle Notation) Let $n \in N$. Let $m \leqslant n$ and let $k_1, \cdots, k_m < n$ all distinct. We use $(k_1 k_2 k_m)$ to denote the bijection $f : [n] \to [n]$ defined by

$$\begin{cases} f(k_i) = f(k_{i+1}) & i < m \\ f(k_m) = f(k_1) & \\ f(x) = x & x \neq k_i, \forall i \end{cases}$$

4.1 Cycles

$(k_1 \cdots k_m)(p_1 \cdots p_q)$ meas $(k_1 \cdots k_m) \circ (p_1 \cdots p_q)$.

What is (132)(21) in S_4?

4.2 Another Notation For Cycles

In S_4 (102) can be written as

$$\begin{pmatrix} 0 & 1 & 2 & 3 \\ 2 & 0 & 1 & 3 \end{pmatrix}$$

In S_4 (132)(21) can be written as

$$\begin{pmatrix} 0 & 1 & 2 & 3 \\ 0 & 3 & 1 & 2 \end{pmatrix} \begin{pmatrix} 0 & 1 & 2 & 3 \\ 0 & 2 & 1 & 3 \end{pmatrix}$$

How to calculate S_4 (132)(21)?
Remember that composition acts on the right first, so cycles need to be read from right to left.

4.3 Theorem

Let $n \in \mathbb{N}\backslash\{0\}$. The group S_n is not abelian if and only if $n \geqslant 3$. (The proof is very easy.)

4.4 Disjoint Cycles

Let $k_1 \cdots, k_m$ all be distinct natural numbers. We say that $(k_1, k_2 \cdots k_m)$ is a cycle of *length* m, or that $(k_1, k_2 \cdots k_m)$ is an m-*cycle*.

We say that cycles $(k_1, \cdots, k_m)$ and $(p_1, \cdots, p_q)$ are disjoint if $\{k_1, \cdots, k_m\} \cap \{p_1, \cdots, p_q\} = \emptyset$

If α and β are disjoint cycles in S_n then $\alpha\beta = \beta\alpha$ in S_n.

Every element of S_n can be written as a product of disjoint cycles.
Proof. For any $x \in [n]$, there exists $1 \leqslant p \leqslant n$, such that $f^p(x) = x$. An element of S_n can be written as

$$(x_1 f(x_1) \cdots f^{p_1}(x_1))(x_2 f(x_2) \cdots f^{p_2}(x_2)) \cdots (x_1 f(x_1) \cdots f^{p_m}(x_m))$$

where $f(f^{p_i}(x_i)) = x_i$.

Let $n \geqslant 2$. Every element of S_n can be written as the product of 2-cycles.
Proof: $(k_1 \cdots k_{m+1}) = (k_1 k_{m+1})(k1 \cdots k_m)$

Convert (124)(1352) in S_n into product of 2-cycles.

Let $\sigma \in Sn$. If σ can be written as a product of an odd number of 2-cycles, then we say that σ is odd. If σ can be written as a product of an even number of 2-cycles, then we say that σ is even. *The identity is even.*

5 Order

Let $(G, \cdot)$ be a group and let $x \in G$. For $n \in \mathbb{N}$, recursively define x^n by: $x^0 = e$ and $x^{n+1} = x \cdot x^n$.

Let $(G, \cdot)$ be a group and let $x \in G$. If there exists an $n \geqslant 1$ such that $x^n = e$, then we say that x has finite order and we define the order of x to be the least $n \geqslant 1$ such that

$x^n = e$. If x does not have finite order, then we say that x has infinite order.

If $(G, \cdot)$ is a finite group, then every element of G has finite order.

6 Subgroup

Let $(G, \cdot)$ be a group and let $H \subseteq G$. Then H is a subgroup if $(H, \cdot)$ is a group.

1. If H is a subgroup of G, then H keeps the same identity. $(e \cdot x = x)$

2. Let $(G, \cdot)$ be a group and H be a finite subset of G. If for all $x, y \in H$, $x \cdot y \in H$, then $(H, \cdot)$ is a subgroup of H. $(b^j = e$ and $b \cdot b^{j-1} = e)$

3. Let $(G, \cdot)$ be a group. $H \subseteq G$ is a non-empty subgroup of $(G, \cdot)$, if and only if for all $x, y \in H$, $x \cdot y^{-1} \in H$.

Let $(G, \cdot)$ be a group. If G is finite, then we call the cardinality of G the order of G.

7 The Dihedral Groups

Let $n \geqslant 3$. The Dihedral Group D_n is the subgroup of S_n of all symmetries of a regular $n-$gon.

Let $n \geqslant 3$. The group D_n has order $2n$.
Explanation. Consider n rotations $(01 \cdots (n-1)), (12 \cdots (n-1)0) \cdots ((n-1)01 \cdots (n-2))$, and n foldings around its symmetrical axis.

List the group D_5.

Find all the subgroups D_4.

8 Lagrange's Theorem

Let $(G, \cdot)$ be a group. Let $H \leqslant G$ and let $a \in G$. We define the a *left coset* of H, denoted aH, to be

$$aH = \{a \cdot x | x \in H\}$$

We define the a *right coset* of H, denoted Ha, to be

$$Ha = \{x \cdot a | x \in H\}$$

8.1 Theorems

1. Let $(G, \cdot)$ be a group, and $H \leqslant G$. For all $a, b \in G$, we can find either $aH = bH$ or $aH \cap bH = \emptyset$.
Proof. If there exists $h \in aH \cap bH$, then there exists $h_1, h_2 \in H$, such that $ah_1 = ah_2 = h$. Therefore, $a = bh_2h_1^{-1}$. For any arbitrary $x \in aH$, $x = ah_3 = bh_2h_1^{-1}h_3 = bh_4 \in bH$.

2. $|aH| = |H| = |Ha|$
Proof. $h_1 \neq h_2 \Rightarrow ah_1 \neq ah_2$

3. Let $(G, \cdot)$ be a group, and $H \leqslant G$. The set of all the left cosets of H is a partition of G. All the blocks have the same cardinality.

4. Let $(G, \cdot)$ be a group, and $H \leqslant G$. We can define the relation $\sim$ as

$$a \sim b := a^{-1}b \in H$$

The relation $\sim$ is an equivalence relation.

8.2 Lagranges Theorem

Let $(G, \cdot)$ be a finite group. If $H \leqslant G$, then the order of H divides the order of G. (It can be easily deduced from 3.)

9 Normal Subgroup

Let $(G, \cdot)$ be a group, and $H \leqslant G$. If for all $g, h \in H$, $g^{-1}hg \in H$, then we call H a normal subgroup of G.

Let $(G, \cdot)$ be a group, and $H \leqslant G$. H is a normal subgroup of G if and only if $gH = Hg$ for all $g \in G$.

Let $(G, \cdot)$ be a group, and H be a normal subgroup of G. Let $\widetilde{G} = \{g_1H, g_2H, \cdots\}$, and $\circ$ be an operator defined on $\widetilde{G}$.

$$(gH) \circ (g'H) = (g \cdot g')H$$

Show that $(\widetilde{G}, \circ)$ is a group.
(Note that $(gH) \circ (g'H) = \{(gh_1)(g'h_2) | h_1, h_2 \in H\} = \{(gg')(h_3h_2) | h_3, h_2 \in H\} = (g \cdot g')H$, the identity of $\widetilde{G}$ is eH, the inverse of gH is $g^{-1}H$.)

10 The Division Algorithm

Let $a \in \mathbb{Z}$ and let $b \in \mathbb{N}$ with $b \neq 0$. There exists a unique $q, r \in \mathbb{Z}$ such that

$$a = q \cdot b + r \text{ and } 0 \leqslant r < b$$

The number q is called the *quotient* and r is called the *remainder* in the division of a by b.

11 Generated Subgroups

Let $(G, \cdot)$ be a group and let $A \subseteq G$. We define the subgroup generated by A, denoted $\langle A \rangle_G$, to be the $\subseteq -$least $H \subseteq G$ such that $A \cup \{e\} \subseteq H$ and for all $x, y \in H, x \cdot y^{-1} \in H$.

12 Cyclic Groups

Let $(G, \cdot)$ be a group and let $n \in \mathbb{N}\backslash\{0\}$. Let $a \in G$ have order n. We call the the group $\langle a \rangle \leqslant G$ the Cyclic Group of order n and denote this group C_n. Let $b \in G$ have infinite order. We call the the group $\langle b \rangle \leqslant G$ the Cyclic Group of infinite order and denote this group C_∞.

12.1 Theorems

Let $(G, \cdot)$ be a group. If $a \in G$, then

$$\langle a \rangle = \{a^m | m \in \mathbb{Z}\}$$

Let $n \in \mathbb{N}\backslash\{0\}$ or $n = \infty$. The group C_n is abelian.

Let $(G, \cdot)$ be a group and let $n \in \mathbb{N}\backslash\{0\}$. If $a \in G$ has order n, then $|\langle a \rangle| = n$. $(\langle a \rangle = \{e, a, a^2, ..., a^{n-1}\})$

Let $n \in N\backslash\{0\}$ and let $m \leqslant n$. Let $k_1, \cdots, k_m \in [n]$ be distinct. The $m-$cycle $(k_1 \cdots k_m)$ has order m in S_n.

Let $n \in \mathbb{N}\backslash\{0\}$. For all $0 < k \leqslant n$, $C_k \leqslant S_n$. (C_k is a cyclic group of order k generated by $a \in S_n$.)

(A refinement of Lagranges Theorem) If $(G, \cdot)$ is a finite group and $x \in G$, then the order of x divides the order of G.

Let p be prime. Let $(G, \cdot)$ be a finite group of order p. Then $(G, \cdot)$ is the the group C_p.

If $(G, \cdot)$ is a finite group with order a prime order, then the only subgroups of G are $\{e\}$ and G.

12.2 More about Lagranges Theorem

Let $(G, \cdot)$ be a group and let $g \in G$ have order n. If there exists $m, k \in \mathbb{N}\backslash\{0\}$ with $n = mk$, then the order of g^m is k.

If $(G, \cdot)$ is a finite group with order n, then for all $g \in G, g^n = e$.

Let A_4 be the group of all even bijections in S_4. There is no $\sigma \in A_4$ with order 6. (The only products of disjoint cycles in S_4 that are even are $3-$cycles and products of two disjoint $2-$cycles.)

List all the elements of A_4.

If $(G, \cdot)$ is a group of order 6, then there exists $g \in G$ with order 2.
(Proof. For all $g \in G$ with $g \neq e$,the order of g must be 3. If $p \neq e$, then $|\langle p \rangle| = 3$, and $\langle p \rangle = \langle p^2 \rangle = \{e, p, p^2\}$. Let $q \in G - \langle p \rangle$. $\langle q \rangle = \langle q^2 \rangle = \{e, q, q^2\}$. $q^2 \notin \langle p \rangle$. Why? There are exactly 5 elements in $\langle p \rangle \cup \langle q \rangle$. Let $g \in G - \langle p \rangle \cup \langle q \rangle$. $g \neq e$, then g^2 must in $\{p, p^2, q, q^2\}$. $\langle g \rangle$ contains at least 4 elements.)

Does A_4 have a subgroup of order 6?

13 Isomorphisms and Homomorphisms

Let $(G, \cdot)$ and $(K, \star)$ be algebraic systems. We say that $f : G \to K$ is a *homomorphism* if for all $a, b \in G$,

$$f(a \cdot b) = f(a) \star f(b)$$

We say that $f : G \to K$ is a isomorphism if f is a bijection. If there exists an isomorphism between the $(G, \cdot)$ and $(K, \star)$, then we say that $(G, \cdot)$ and $(K, \star)$ are isomorphic and write $G \cong K$ or $(G, \cdot) \cong (K, \star)$.

13.1 Theorems

Let $(A, \cdot)$ and $(B, \star)$ be algebraic systems, and $A \cong B$.

1. If e is the identity of $(A, \cdot)$, then $f(e)$ is the identity of $(B, \star)$.
   (Proof. For all $b \in B$, $b = f(a)$, and $b \star f(e) = f(a) \star f(e) = f(a \cdot e) = f(a) = b = f(e \cdot a) = f(e) \star f(a) = f(e) \star b$)

2. If a^{-1} is the inverse of a, then $f(a^{-1})$ is the inverse of $f(a)$.
   (Proof. $f(a^{-1}) \star f(a) = f(a^{-1} \cdot a) = f(e)$)

3. If $(A, \cdot)$ satisfies associativity, then $(B, \star)$ satisfies associativity.

4. If $(A, \cdot)$ is a group, then $(B, \star)$ is a group.

13.2 Group Isomorphism

Let $(G, \cdot)$ be a group. Let $g, h \in G$ both have order n. Then $\langle g \rangle \cong \langle h \rangle$. (Define $f : \langle g \rangle \to \langle h \rangle$, $f(g^k) = h^k$.)

Consider the group $(\mathbb{Z}, +)$. If $n \in \mathbb{N} \backslash \{0\}$, define

$$n\mathbb{Z} = \{m \in \mathbb{Z} | (\exists k \in \mathbb{Z})(m = nk)\}$$

Then $n\mathbb{Z} \leqslant \mathbb{Z}$ and $n\mathbb{Z} \cong \mathbb{Z}$.