ITC8190
Mathematics for Computer Science
Group Theory

Aleksandr Lenin

December 4th, 2018

The simplest algebraic structures are sets associated with single operations that satisfy certain reasonable axioms.

Such a set with a single operation is called a **group**.

Some examples of groups:

- Integers $\mathbb{Z}_n$ with operation of addition or multiplication – modular groups
- 2×2 matrices with operation of matrix multiplication – matrix groups
- symmetries of a body with operation of composition – symmetic groups
- rigid motions of a body with operation of composition – dihedral groups
- permutations on a set with operation of composition – permutation groups

A group $(G, \circ)$ is a set G together with a law of composition, which is a function $G \times G \to G$ defined by $(a, b) \mapsto a \circ b$ that satisfies the following axioms:

1. The group operation is associative

$$\forall a, b, c \in G : a \circ (b \circ c) = (a \circ b) \circ c \ .$$

2. There exists an identity element $e \in G$ such that

$$\forall a \in G : e \circ a = a \circ e = a \ .$$

3. For every element $a \in G$ there exists an inverse element $a^{-1} \in G$ such that

$$a \circ a^{-1} = a^{-1} \circ a = e \ .$$

4. G is closed under $\circ$.

$$a, b \in G : a \circ b \in G \ .$$

Groups with the property that for all $a, b \in G$

$$a \circ b = b \circ a \ ,$$

is called **abelian** or **commutative**.

Groups that do not have this property are called **nonabelian** or **noncommutative**.

I.e., matrix groups are nonabelian, since the group operation, the matrix multiplication, is not commutative – $A \times B \neq B \times A$.

A group is **finite** or has **finite order** if it contains a finite number of elements. Otherwise, the group is **infinite** or has **infinite order**.

The **order** of a finite group G (denoted as $|G|$ or ord G) is the number of elements in contains. If group G contains n elements, then $|G| = n$.

Example 1

The set of integers $\mathbb{Z}$ is a group under the operation of addition.

Addition operation is associative

$$\forall a, b, c \in \mathbb{Z} : a + (b + c) = (a + b) + c \ .$$

The additive identity is 0, since for any integer a, it holds that $a + 0 = 0 + a = a$. For every integer a there is an inverse element $-a$ such that $a + (-a) = -a + a = 0$.

Since addition is commutative, meaning that for all $a, b \in \mathbb{Z}$ it holds that $a + b = b + a$, then $(\mathbb{Z}, +)$ is an Abelian group.

The set $\mathbb{Z}_n$ is a group under modular addition.

Figure: Cayley table for $(\mathbb{Z}_5, +)$

$+$	0	1	2	3	4
0	0	1	2	3	4
1	1	2	3	4	0
2	2	3	4	0	1
3	3	4	0	1	2
4	4	0	1	2	3

The set $\mathbb{Z}_6$ together with operation of multiplication does not form a group, for the following reasons:

- Element 0 is not invertible, i.e. the equation $0 \cdot k = 1 \pmod 6$ is not solvable
- Elements $2, 4$ are not invertible, since the equations $2 \cdot k = 1 \pmod 6$ and $4 \cdot k = 1 \pmod 6$ are not solvable.

Previously in this course we proved a theorem that says "**An element $a \in \mathbb{Z}_n$ is invertible iff** $\gcd(a, n) = 1$".

The set of invertible elements of $\mathbb{Z}_n$ is a group under the operation of multiplication. Such a group is called **group of units** and denoted as $U(n)$.

The set of invertible elements in $\mathbb{Z}_8$ is a group $U(8)$ under modular multiplication.

Figure: Cayley table for $U(8)$

$\times$	1	3	5	7
1	1	3	5	7
3	3	1	7	5
5	5	7	1	3
7	7	5	3	1

Theorem 1

The identity element in a group G is unique.

Proof.

Suppose e and e' are both identity elements in G. Then

$$e = e \circ e' = e' \quad .$$

Therefore, there exists only one element $e \in G$ such that $e \circ g = g \circ e = g$ for all $g \in G$. $\square$

Theorem 2

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

Proof.

Let g' and g'' both be the inverse elements of g. Then

$$g \circ g' = g \circ g'' = e \ .$$

Multiplying both sides by g^{-1} we have

$$g^{-1} \circ g \circ g' = g^{-1} \circ g \circ g'' = g^{-1} \circ e \implies g' = g'' = g^{-1} \ .$$

□

Theorem 3

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

Proof.

Let $a, b \in G$. Then

$$ab(ab)^{-1} = abb^{-1}a^{-1} = aa^{-1} = e \ ,$$
$$(ab)^{-1}ab = b^{-1}a^{-1}ab = b^{-1}b = e \ .$$

□

Theorem 4

Let G be a group. For any $a \in G, (a^{-1})^{-1} = a$.

Proof.

Observe that $a^{-1}(a^{-1})^{-1} = e$. Multiplying both sides by a we have

$$(a^{-1})^{-1} = e(a^{-1})^{-1} = aa^{-1}(a^{-1})^{-1} = ae = a \ .$$

Proposition 1 (Left and right cancellation laws)

Let G be a group, let $a, b, c \in G$. Then $ba = ca \implies b = c$ and $ab = ac \implies b = c$.

Proof.

$$ba = ca \implies baa^{-1} = caa^{-1} \implies b = c \ ,$$
$$ab = ac \implies a^{-1}ab = a^{-1}ac \implies b = c \ .$$

$\square$

In a group, the usual laws of exponents hold. For all $g, h \in G$,

1. $g^m g^n = g^{m+n}$ for all $m, n \in \mathbb{Z}$
2. $(g^m)^n = g^{mn}$ for all $m, n \in \mathbb{Z}$
3. If G is abelian, then $(gh)^n = g^n h^n$

Let $(G, \circ)$ be a group. When the group operation $\circ$ is restricted to a subset $H \subseteq G$, and H forms a group under $\circ$, then $(H, \circ)$ is a **subgroup** of $(G, \circ)$.

I.e., consider the set $2\mathbb{Z} = \{\ldots, -4, -2, 0, 2, 4 \ldots\}$. $(2\mathbb{Z}, +)$ is a subgroup of $(\mathbb{Z}, +)$.

Note that

- $H = \{e\}$ is a subgroup of every group G. It is called a **trivial subgroup**.
- If G is a group, then it is the subgroup of itself. Such a subgroup is called **improper subgroup**.
- If $H \subset G$ (H is a proper subset of G) and forms a group under the group operation of G, then H is a **proper subgroup** of G.

Group $(\mathbb{Z}_4, +)$ has one single nontrivial proper subgroup $H = \{0, 2\}$.

Figure: Cayley table for $(\mathbb{Z}_2 \times \mathbb{Z}_2, +)$

$+$	$(0,0)$	$(0,1)$	$(1,0)$	$(1,1)$
$(0,0)$	$(0,0)$	$(0,1)$	$(1,0)$	$(1,1)$
$(0,1)$	$(0,1)$	$(0,0)$	$(1,1)$	$(1,0)$
$(1,0)$	$(1,0)$	$(1,1)$	$(0,0)$	$(0,1)$
$(1,1)$	$(1,1)$	$(1,0)$	$(0,1)$	$(0,0)$

Group $(\mathbb{Z}_2 \times \mathbb{Z}_2, +)$ has three nontrivial proper subgroups:

$$H_1 = \{(0,0), (0,1)\}$$
$$H_2 = \{(0,0), (1,0)\}$$
$$H_3 = \{(0,0), (1,1)\}$$

Theorem 5

Let G be a group and let $a \in G$. Then the set

$$\langle a \rangle = \{a^k : k \in \mathbb{Z}\}$$

is a subgroup of G. Furthermore, $\langle a \rangle$ is the smallest subgroup of G that contains a.

Proof.

The identity $a^0 = e \in \langle a \rangle$. Let $g, h \in \langle a \rangle$. Then $g = a^m$ and $h = a^n$ with $m, n \in \mathbb{Z}$. So $gh = a^m a^n = a^{m+n} \in \langle a \rangle$. If $g = a^n \in \langle a \rangle$, its inverse $g^{-1} = a^{-n} \in \langle a \rangle$. Hence, $\langle a \rangle$ is a subgroup of G. If any subgroup H of G contains a, it contains all powers of a by closure. Hence, it contains $\langle a \rangle$. Therefore, $\langle a \rangle$ is the smallest subgroup of G containing a. □

For $a \in G$, $\langle a \rangle$ is called the **cyclic subgroup** generated by a.

If G contains some element a such that $\langle a \rangle = G$, then G is a **cyclic group** and a is the **generator** of G.

If $a \in G$, the **order** of a (denoted as $|a|$ or ord a) is the smallest positive integer n such that $a^n = e$. If there is no such integer n, then $|a| = \infty$.

A cyclic group may have more than a single generator. I.e., $\mathbb{Z}_6$ is generated by 1 and 5. Hence, $\mathbb{Z}_6$ is a cyclic group.

Not every element in a cyclic group is a generator of the group. I.e., the order of $2 \in \mathbb{Z}_6$ is 3. The cyclic subgroup generated by 2 is $\langle 2 \rangle = \{0, 2, 4\}$.

Groups $\mathbb{Z}$ and $\mathbb{Z}_n$ are cyclic groups. $\mathbb{Z}$ is generated by 1 and -1. We can certainly generate any $\mathbb{Z}_n$ with 1, but there are may be other generators of $\mathbb{Z}_n$.

Group $U(9) = \{1, 2, 4, 5, 7, 8\}$ is a cyclic group. 2 is a generator for $U(9)$, since $\langle 2 \rangle = \{2, 4, 8, 7, 5, 1\} = U(9)$.

The order of $U(n)$ is $\varphi(n)$, where $\varphi(n)$ is the Euler's phi (totient) function.

Theorem 6

Every cyclic group is abelian.

Proof.

Let G be a cyclic group, let $a \in G$ be a generator for G. If $g, h \in G$, then $g = a^r$ and $h = a^s$ for some nonnegative integers r, s. Since

$$gh = a^r a^s = a^{r+s} = a^{s+r} = a^s a^r = hg \ ,$$

G is abelian. $\square$

Theorem 7

Every subgroup of a cyclic group is cyclic.

Proof.

Let $G = \langle a \rangle$, let H be a subgroup of G. If $H = \{e\}$, then trivially, H is cyclic. Suppose $g \in H, g \neq e$. Then $g = a^n$ for some nonnegative integer n. Let m be the smallest natural number such that $a^m \in H$. Such an m exists by the Principle of Well Ordering. We need to show that a^m is the generator of H. That is, every $h \in H$ can be written as a power of a^m.

Proof continues on the next slide...

Theorem 7

Every subgroup of a cyclic group is cyclic.

Proof.

Since $h \in H$ and H is a subgroup of G, then $h = a^k$ for some positive integer k. By the division algorithm, $k = mq + r$, where $0 \leqslant r < m$. Then

$$a^k = a^{mq+r} = (a^m)^q \cdot a^r \quad ,$$

so $a^r = a^k(a^m)^{-q}$. Since $a^k \in H$ and $(a^m)^{-q} \in H$, by closure $a^r \in H$. However, m was the smallest positive integer such that $a^m \in H$. A contradiction. Consequently, $r = 0$ and so $k = mq$. Therefore, $h = a^k = a^{mq} = (a^m)^q$, which means that H is generated by a^m, and therefore, H is cyclic. $\square$

The subgroups of $\mathbb{Z}$ are exactly $n\mathbb{Z}$ for $n = 0, 1, 2, \ldots$.

Theorem 8

Let G be a cyclic group of order n. Let a be a generator for G. Then $a^k = e$ iff $n|k$.

Proof.

Suppose $a^k = e$. By the division algorithm, $k = nq + r$ with $0 \leqslant r < n$. Hence

$$e = a^k = a^{nq+r} = (a^n)^q a^r = e^q a^r = a^r \quad .$$

Since the smallest positive integer m such that $a^m = e$ is n, then $r = 0$. Therefore, $a^k = a^{nq}$ and hence $n|k$. Conversely, if $n|k$, then $k = ns$ for some integer s. Consequently,

$$a^k = a^{ns} = (a^n)^s = e^s = e \quad .$$

$\square$

Theorem 9

Let G be a cyclic group of order n, and suppose $a \in G$ is a generator of G. If $b = a^k$, then the order of b is n/d, where $d = \gcd(k, n)$.

Proof.

We wish to find the smallest integer m such that $e = b^m = a^{km}$. By Theorem 8, this is the smallest integer m such that $n|km$. Since $d = \gcd(k, n)$, then $(n/d)|m(k/d)$ and $\gcd(k/d, n/d) = 1$. Hence, $(n/d)|m(k/d)$ iff $(n/d)|m$. The smallest such m is n/d. $\square$

From Theorem 9 it follows that

Corollary 1

The generators of $\mathbb{Z}_n$ are the integers r such that $1 \leqslant r < n$ and $\gcd(r, n) = 1$.

Example 2

Consider $\mathbb{Z}_{16}$. Elements $1, 3, 5, 7, 9, 11, 13, 15$ are coprime to 16, and hence each of them generates $\mathbb{Z}_{16}$. I.e., take 9:

$$\mathbb{Z}_{16} = \langle 9 \rangle = \{9, 2, 11, 4, 13, 6, 15, 8, 1, 10, 3, 12, 5, 14, 7, 0\} \ .$$

Theorem 10

Let $U(n)$ be a group of units in $\mathbb{Z}_n$. Then $|U(n)| = \varphi(n)$.

Proof.

The group of units consists of invertible elements $a \in \mathbb{Z}_n$ such that $\gcd(a, n) = 1$. There are $\varphi(n)$ of them. $\square$

Theorem 11 (Euler theorem)

Let a, n be integers such that $n > 0$ and $\gcd(a, n) = 1$. Then $a^{\varphi(n)} \equiv 1 \pmod{n}$.

Proof.

By Theorem 10, $|U(n)| = \varphi(n)$. Therefore, for all $a \in U(n)$ it holds that $a^{\varphi(n)} = 1$. Therefore, $a^{\varphi(n)} \equiv 1 \pmod{n}$. $\square$

A special case of Euler theorem in which n is a prime number. If n is prime, then $\varphi(n) = n - 1$. This result is known as Fermat little theorem.

Theorem 12 (Fermat little theorem)

Let p be any prime number, and suppose that $\gcd(p, a) = 1$, *then* $a^{p-1} \equiv 1 \pmod{p}$.

Definition 1 (Coset)

Let G be a group and H be a subgroup of G. The **left coset** of H with **representative** $g \in G$ is the set

$$gH = \{gh : h \in H\} \ .$$

Right cosets can be defined similarly by

$$Hg = \{hg : h \in H\} \ .$$

Example 3

Consider a subgroup $H = \{0, 3\}$ of $\mathbb{Z}_6$. The cosets are:

$$\begin{aligned} 0 + H = 3 + H = \{0, 3\} \\ 1 + H = 4 + H = \{1, 4\} \\ 2 + H = 5 + H = \{2, 5\} \end{aligned}$$

Lemma 1

Let H be a subgroup of a group G. Let $g_1, g_2 \in G$. If $g_2 \in g_1 H$, then $g_1 H = g_2 H$.

Proof.

Let $a \in g_1 H$.

$$g_2 \in g_1 H \implies g_2 = g_1 h \implies g_1 = g_2 h^{-1}$$
$$a = g_1 h' = g_2 h^{-1} h' \implies a \in g_2 H \implies g_1 H \subseteq g_2 H$$

Let $a \in g_2 H$.

$$g_2 \in g_1 H \implies g_2 = g_1 h$$
$$a = g_2 h' = g_1 h h' \implies a \in g_1 H \implies g_2 H \subseteq g_1 H$$

Therefore, $g_1 H = g_2 H$. $\square$

Theorem 13

Let H be a subgroup of G. Then the left cosets of H in G partition G. That is, the group G is the disjoint union of the left cosets of H in G.

Proof.

Let g_1H and g_2H be two cosets of H in G. We must show that either $g_1H \cap g_2H = \emptyset$ or $g_1H = g_2H$. Suppose $g_1H \cap g_2H \neq \emptyset$ and let $a \in g_1H \cap g_2H$. Then $a = g_1h_1 = g_2h_2$ for some elements $h_1, h_2 \in H$. Hence, $g_1 = g_2h_2h_1^{-1}$ or $g_1 \in g_2H$. By Lemma 1, $g_1H = g_2H$. $\square$

NOTE: There is nothing special in this theorem about left cosets. Right cosets also partition G in exactly the same way, and the proof is very similar to the one above.

Definition 2 (Index of a subgroup)

The **index** of a subgroup H in a group G is the number of left cosets of H in G, and is denoted as $[G : H]$.

Example 4

Let $G = \mathbb{Z}_6$ and $H = \{0, 3\}$. Then $[G : H] = 3$.

Theorem 14

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 $\mathcal{L}_H$ and $\mathcal{R}_H$ denote the set of left and right cosets of H in G. Define $\phi : \mathcal{L}_H \to \mathcal{R}_H$ by $gH \mapsto Hg^{-1}$. We will show that $\phi : \mathcal{L}_H \to \mathcal{R}_H$ is a bijection. Define the inverse map $\psi : \mathcal{R}_H \to \mathcal{L}_H$ by $Hh \mapsto h^{-1}H$. Let $Hh \in \mathcal{R}_H$, then $(\phi \circ \psi)(Hh) = Hh$.

$$(\phi \circ \psi)(Hh) = \phi(h^{-1}H) = H(h^{-1})^{-1} = Hh \ .$$

Proof continues on the next slide...

Theorem 14

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 $gH \in \mathcal{L}_H$, then $(\psi \circ \phi)(gH) = gH$.

$$(\psi \circ \phi)(gH) = \psi(Hg^{-1}) = (g^{-1})^{-1}H = gH \ .$$

Therefore, $\phi : \mathcal{L}_H \to \mathcal{R}_H$ is a bijection between the sets of left and right cosets of H, and hence the number of left cosets of H in G is the same as the number of right cosets of H in G. $\square$

Proposition 2

Let H be a subgroup of G with $g \in G$ and define a map $\phi : H \to gH$ by $\phi(h) = gh$. The map ϕ is bijective, hence the number of elements in H is the same as the number of elements in gH.

Proof.

Let $\phi : H \to gH$ be defined by $h \mapsto gh$. Define an inverse mapping $\psi : gH \to H$ by $a \mapsto g^{-1}a$. First we show that ψ is well defined. Since $a \in gH$, then $a = gh$ for some $h \in H$. $g^{-1}a = g^{-1}gh = h \in H$. We show that ϕ is a bijection.

$$(\phi \circ \psi)(a) = \phi(g^{-1}a) = gg^{-1}a = a \quad ,$$
$$(\psi \circ \phi)(h) = \psi(gH) = g^{-1}gh = h \quad .$$

Therefore, ϕ is a bijection between H and gH. Hence, the number of elements in H is the same as the number of elements in gH. $\square$

Theorem 15 (Lagrange)

Let G be a finite group and let H be a subgroup of G. Then $|G|/|H| = [G : H]$ is the number of distinct left cosets of H in G. In particular, the number of elements in H must divide the number of elements in G.

Proof.

Every subset $H \subseteq G$ partitions G into $[G : H]$ distinct left cosets. Each left coset has $|H|$ elements, therefore, $|G| = [G : H]|H|$. □

From the Lagrange theorem it follows that

Corollary 2

Suppose that G is a finite group and $g \in G$. Then the order of g must divide the order of G.

Corollary 3

Let $|G| = p$ with p a prime number. Then G is cyclic and any $g \in G$ such that $g \neq e$ is a generator.

Proof.

Let $g \in G$ such that $g \neq e$. Then the order of g must divide p. Since p is prime, $|g| = 1$ or $|g| = p$. If $|g| = 1$, then $g = e$, since $\langle g \rangle = \{e\}$. If $|\langle g \rangle| > 1$, it must be p. Hence, g generates G. $\square$

?

THANK YOU
FOR
YOUR
ATTENTION
ANY QUESTIONS?