# VE203
# Discrete Math
# RC4

Yucheng Huang

University of Michigan
Shanghai Jiao Tong University
Joint Institute

March 25, 2022

# Group

## Definition

A group is a pair $(G, \cdot)$, where $G$ is a set, and $\cdot : G \times G \to G$, $(g, h) \mapsto g \cdot h = gh$, is a law of composition (aka group law) that has the following properties:

- The law of composition is associative: $(ab)c = a(bc)$ for all $a, b, c \in G$.
- $G$ contains an identity element 1 , such that $1a = a1 = a$ for all $a \in G$.
- Every element $a \in G$ has an inverse, an element $b$ such that $ab = ba = 1$.

An abelian group is a group whose law of composition is commutative.

# Group

A group $\langle G, * \rangle$ is a set $G$, closed under a binary operation $*$, such that the following axioms are satisfied:

$\mathscr{S}_1$ : For all $a, b, c \in G$, we have

$$(a * b) * c = a * (b * c). \quad \text{associativity of } *$$

$\mathscr{S}_2$ : There is an element $e$ in $G$ such that for all $x \in G$,

$$e * x = x * e = x. \quad \text{identity element } e \text{ for } *$$

$\mathscr{S}_3$ : Corresponding to each $a \in G$, there is an element $a'$ in $G$ such that

$$a * a' = a' * a = e. \quad \text{inverse } a' \text{ of } a$$

# Group

1. The set $\mathbb{Z}^+$under addition is not a group. There is no identity element for $+$in $\mathbb{Z}^+$.
2. The set of all nonnegative integers (including 0 ) under addition is still not a group. There is an identity element 0 , but no inverse for 2 .
3. The familiar additive properties of integers and of rational, real, and complex numbers show that $\mathbb{Z}, \mathbb{Q}, \mathbb{R}$, and $\mathbb{C}$ under addition are abelian groups.
4. The set $\mathbb{Z}^+$under multiplication is not a group. There is an identity 1 , but no inverse of 3 .
5. The familiar multiplicative properties of rational, real, and complex numbers show that the sets $\mathbb{Q}^+$and $\mathbb{R}^+$of positive numbers and the sets $\mathbb{Q}^*, \mathbb{R}^*$, and $\mathbb{C}^*$ of nonzero numbers under multiplication are abelian groups.

# Group

6. The set of all real-valued functions with domain $\mathbb{R}$ under function addition is a group. This group is abelian.
7. (Linear Algebra) Those who have studied vector spaces should note that the axioms for a vector space $V$ pertaining just to vector addition can be summarized by asserting that $V$ under vector addition is an abelian group.
8. The set $M_{m\times n}(\mathbb{R})$ of all $m \times n$ matrices under matrix addition is a group. The $m \times n$ matrix with all entries 0 is the identity matrix. This group is abelian.
9. The set $M_n(\mathbb{R})$ of all $n \times n$ matrices under matrix multiplication is not a group. The $n \times n$ matrix with all entries 0 has no inverse.

# Group

Let $*$ be defined on $\mathbb{Q}^+$ by $a * b = ab/2$. Then

$$(a * b) * c = \frac{ab}{2} * c = \frac{abc}{4},$$

and likewise

$$a * (b * c) = a * \frac{bc}{2} = \frac{abc}{4}.$$

Thus $*$ is associative. Computation shows that

$$2 * a = a * 2 = a$$

for all $a \in \mathbb{Q}^+$, so 2 is an identity element for $*$. Finally,

$$a * \frac{4}{a} = \frac{4}{a} * a = 2,$$

so $a' = 4/a$ is an inverse for $a$. Hence $\mathbb{Q}^+$ with the operation $*$ is a group.

# Elementary Properties of Groups

**Theorem**

Given a group $G, a, b, c \in G$, then

1. there exists a unique identity element.
2. $ba = ca \Rightarrow b = c$ and $ab = ac \Rightarrow b = c$.
3. For all $a \in G$, there exists a unique element $b \in G$ such that $ab = ba = 1$.
4. $(ab)^{-1} = b^{-1}a^{-1}$.

# Theorem 2

If $G$ is a group with binary operation $*$, then the left and right cancellation laws hold in $G$, that is, $a * b = a * c$ implies $b = c$, and $b * a = c * a$ implies $b = c$ for all $a, b, c \in G$.
Prove: Suppose $a * b = a * c$. Then by $\mathscr{S}_3$, there exists $a'$, and

$$a' * (a * b) = a' * (a * c).$$

By the associative law,

$$\left(a' * a\right) * b = \left(a' * a\right) * c.$$

By the definition of $a'$ in $\mathscr{S}$, $a' * a = e$, so

$$e * b = e * c.$$

By the definition of $e$ in $\mathscr{S}_2$,

$$b = c.$$

Similarly, from $b * a = c * a$ one can deduce that $b = c$ upon multiplication on the right by $a'$ and use of the axioms for a group.

# Theorem 3

There is only one element $a'$ in $G$ such that

$$a' * a = a * a' = e.$$

In summary, the identity element and inverse of each element are unique in a group.
Prove: Turning to the uniqueness of an inverse, suppose that $a \in G$ has inverses $a'$ and $a''$ so that $a' * a = a * a' = e$ and $a'' * a = a * a'' = e$. Then

$$a * a'' = a * a' = e$$

and, by Theorem 2,

$$a'' = a',$$

so the inverse of $a$ in a group is unique.

# Theorem 4

Note that in a group $G$, we have

$$(a * b) * \left(b' * a'\right) = a * \left(b * b'\right) * a' = (a * e) * a' = a * a' = e.$$

Let $G$ be a group. For all $a, b \in G$, we have $(a * b)' = b' * a'$.

# Exercise 1

In Exercises 1 through 6, determine whether the binary operation $*$ gives a group structure on the given set. If no group results, give the first axiom in the order $\mathscr{S}_1, \mathscr{S}_2, \mathscr{S}_3$ from Definition that does not hold.

1. Let $*$ be defined on $\mathbb{Z}$ by letting $a * b = ab$.
2. Let $*$ be defined on $2\mathbb{Z} = \{2n \mid n \in \mathbb{Z}\}$ by letting $a * b = a + b$.
3. Let $*$ be defined on $\mathbb{R}^+$by letting $a * b = \sqrt{ab}$.
4. Let $*$ be defined on $\mathbb{Q}$ by letting $a * b = ab$.
5. Let $*$ be defined on the set $\mathbb{R}^*$ of nonzero real numbers by letting $a * b = a/b$.
6. Let $*$ be defined on $\mathbb{C}$ by letting $a * b = |ab|$.

# Exercise 1 Solution

1. No. $G_3$ fails.
2. Yes
3. No. $G_1$ fails.
4. No. $G_3$ fails.
5. No. $G_1$ fails.
6. No. $G_2$ fails.

# Exercise 2

Let $S$ be the set of all real numbers except $-1$. Define $*$ on $S$ by

$$a * b = a + b + ab.$$

a. Show that $*$ gives a binary operation on $S$.
b. Show that $\langle S, * \rangle$ is a group.
c. Find the solution of the equation $2 * x * 3 = 7$ in $S$.

# Exercise 2 Solution

a. We must show that $S$ is closed under $*$, that is, that $a+b+ab \neq -1$ for $a, b \in S$. Now $a+b+ab = -1$ if and only if $0 = ab+a+b+1 = (a+1)(b+1)$. This is the case if and only if either $a = -1$ or $b = -1$, which is not the case for $a, b \in S$.
b. Associative: We have $a*(b*c) = a*(b+c+bc) =$ $a+(b+c+bc)+a(b+c+bc) = a+b+c+ab+ac+bc+abc$ and $(a*b)*c = (a+b+ab)*c =$ $(a+b+ab)+c+(a+b+ab)c = a+b+c+ab+ac+bc+abc$.
Identity: 0 acts as identity element for $*$, for $0*a = a*0 = a$.
Inverses: $\frac{-a}{a+1}$ acts as inverse of $a$, for

$$a * \frac{-a}{a+1} = a + \frac{-a}{a+1} + a\frac{-a}{a+1} = \frac{a(a+1)-a-a^2}{a+1} = \frac{0}{a+1} = 0$$

# Exercise 2 Solution

c. Because the operation is commutative,
$2 * x * 3 = 2 * 3 * x = 11 * x$. Now the inverse of 11 is $-11/12$ by Part(**b**). From $11 * x = 7$, we obtain

$$x = \frac{-11}{12} * 7 = \frac{-11}{12} + 7 + \frac{-11}{12}7 = \frac{-11 + 84 - 77}{12} = \frac{-4}{12} = -\frac{1}{3}$$

# Subgroup

## Definition

A subset $H$ of a group $G$ is a subgroup if it has the following properties:

1. Closure: If $a, b \in H$, then $ab \in H$.
2. Identity: $1 \in H$.
3. Inverses: If $a \in H$, then $a^{-1} \in H$.

## Concept

If $G$ is a group, then the subgroup consisting of $G$ itself is the improper subgroup of $G$. All other subgroups are proper subgroups. The subgroup $\{e\}$ is the trivial subgroup of $G$. All other subgroups are nontrivial.

# Subgroup

Subgroups of the Additive Group $(\mathbb{Z}, +)$

A subset $S$ of $(\mathbb{Z}, +)$ is a subgroup if

1. Closure: If $a, b \in S$, then $a + b \in S$.
2. Identity: $0 \in S$.
3. Inverses: If $a \in S$, then $-a \in S$.

For $a \in \mathbb{Z}$, a subgroup of $(\mathbb{Z}, +)$ is given by

$$a\mathbb{Z} = \{n \in \mathbb{Z} \mid n = ka \text{ for some } k \in \mathbb{Z}\}$$

# Subgroup

Subgroups of the Additive Group $(\mathbb{Z}, +)$

A subset $S$ of $(\mathbb{Z}, +)$ is a subgroup if

1. Closure: If $a, b \in S$, then $a + b \in S$.
2. Identity: $0 \in S$.
3. Inverses: If $a \in S$, then $-a \in S$.

For $a \in \mathbb{Z}$, a subgroup of $(\mathbb{Z}, +)$ is given by

$$a\mathbb{Z} = \{n \in \mathbb{Z} \mid n = ka \text{ for some } k \in \mathbb{Z}\}$$

# Exercise 3

In Exercises 1 through 6, determine whether the given subset of the complex numbers is a subgroup of the group $\mathbb{C}$ of complex numbers under addition.

1. $\mathbb{R}$
2. $\mathbb{Q}^+$
3. $7\mathbb{Z}$
4. The set $i\mathbb{R}$ of pure imaginary numbers including 0
5. The set $\pi\mathbb{Q}$ of rational multiples of $\pi$
6. The set $\{\pi^n \mid n \in \mathbb{Z}\}$

# Exercise 3 Solution

1. Yes
2. No, there is no identity element.
3. Yes
4. Yes
5. Yes
6. No, the set is not closed under addition.

# Cyclic Group

If $G$ is a group and $a \in G$, then

$$H = \{a^n \mid n \in \mathbb{Z}\}$$

is a subgroup of $G$. This group is the cyclic subgroup $\langle a \rangle$ of $G$ generated by $a$. Also, given a group $G$ and an element $a$ in $G$, if

$$G = \{a^n \mid n \in \mathbb{Z}\},$$

then $a$ is a generator of $G$ and the group $G = \langle a \rangle$ is cyclic. We introduce one new bit of terminology. Let $a$ be an element of a group $G$. If the cyclic subgroup $\langle a \rangle$ of $G$ is finite, then the order of $a$ is the order $|\langle a \rangle|$ of this cyclic subgroup. Otherwise, we say that $a$ is of infinite order. We will see in this section that if $a \in G$ is of finite order $m$, then $m$ is the smallest positive integer such that $a^m = e$.

# Cyclic Group

**Theorem:** Every cyclic group is abelian.
**Proof:** Let $G$ be a cyclic group and let $a$ be a generator of $G$ so that

$$G = \langle a \rangle = \{a^n \mid n \in \mathbb{Z}\}.$$

If $g_1$ and $g_2$ are any two elements of $G$, there exist integers $r$ and $s$ such that $g_1 = a^r$ and $g_2 = a^s$. Then

$$g_1 g_2 = a^r a^s = a^{r+s} = a^{s+r} = a^s a^r = g_2 g_1,$$

so $G$ is abelian.

# Cyclic Group

**Theorem:**A subgroup of a cyclic group is cyclic.
**Proof:** Let $G$ be a cyclic group generated by $a$ and let $H$ be a subgroup of $G$. If $H = \{e\}$, then $H = \langle e \rangle$ is cyclic. If $H \neq \{e\}$, then $a^n \in H$ for some $n \in \mathbb{Z}^+$. Let $m$ be the smallest integer in $\mathbb{Z}^+$such that $a^m \in H$. We claim that $c = a^m$ generates $H$; that is,

$$H = \langle a^m \rangle = \langle c \rangle.$$

We must show that every $b \in H$ is a power of $c$. Since $b \in H$ and $H \leq G$, we have $b = a^n$ for some $n$. Find $q$ and $r$ such that

$$n = mq + r \quad \text{for} \quad 0 \leq r < m$$

in accord with the division algorithm. Then

$$a^n = a^{mq+r} = (a^m)^q \, a^r,$$

So

$$a^r = (a^m)^{-q} \, a^n.$$

# Cyclic Group

**Proof:**

Now since $a^n \in H, a^m \in H$, and $H$ is a group, both $(a^m)^{-q}$ and $a^n$ are in $H$. Thus $(a^m)^{-q} a^n \in H$; that is, $a^r \in H$.

Since $m$ was the smallest positive integer such that $a^m \in H$ and $0 \leq r < m$, we must have $r = 0$. Thus $n = qm$ and

$$b = a^n = (a^m)^q = c^q.$$

so $b$ is a power of $c$.

# Theorem

If $a$ is a generator of a finite cyclic group $G$ of order $n$, then the other generators of $G$ are the elements of the form $a^r$, where $r$ is relatively prime to $n$.

# Cyclic Group

Let us find all subgroups of $\mathbb{Z}_{18}$ and give their subgroup diagram. All subgroups are cyclic. The elements $1, 5, 7, 11, 13$, and 17 are all generators of $\mathbb{Z}_{18}$. Starting with 2 ,

$$\langle 2 \rangle = \{0, 2, 4, 6, 8, 10, 12, 14, 16\}$$

is of order 9 and has as generators elements of the form $h2$, where $h$ is relatively prime to 9 , namely, $h = 1, 2, 4, 5, 7$, and 8 , so $h2 = 2, 4, 8, 10, 14$, and 16 . The element 6 of $\langle 2 \rangle$ generates $\{0, 6, 12\}$, and 12 also is a generator of this subgroup.
We have thus far found all subgroups generated by $0, 1, 2, 4, 5, 6, 7, 8, 10, 11, 12, 13, 14, 16$, and 17 . This leaves just 3,9 , and 15 to consider.

$$\langle 3 \rangle = \{0, 3, 6, 9, 12, 15\},$$

and 15 also generates this group of order 6 , since $15 = 5 \cdot 3$, and the gcd of 5 and 6 is 1 . Finally,

$$\langle 9 \rangle = \{0, 9\}.$$

# Exercise 4

In Exercises 1 through 5, find all orders of subgroups of the given group.

1. $\mathbb{Z}_6$
2. $\mathbb{Z}_8$
3. $\mathbb{Z}_{12}$
4. $\mathbb{Z}_{20}$
5. $\mathbb{Z}_{17}$

# Exercise 4 Solution

1. $1, 2, 3, 6$
2. $1, 2, 4, 8$
3. $1, 2, 3, 4, 6, 12$
4. $1, 2, 4, 5, 10, 20$
5. 1,17

# Permutation Group

Let $A$ be a set, and let $\sigma$ and $\tau$ be permutations of $A$ so that $\sigma$ and $\tau$ are both one-to-one functions mapping $A$ onto $A$. The composite function $\sigma \circ \tau$ defined schematically by

$$A \xrightarrow{\tau} A \xrightarrow{\sigma} A,$$

gives a mapping of $A$ into $A$. Rather than keep the symbol o for permutation multiplication, we will denote $\sigma \circ \tau$ by the juxtaposition $\sigma\tau$, as we have done for general groups. Now $\sigma\tau$ will be a permutation if it is one to one and onto A. Remember that the action of $\sigma\tau$ on A must be read in right-to-left order: first apply $\tau$ and then $\sigma$. Let us show that $\sigma\tau$ is one to one. If

$$(\sigma\tau)(a_1) = (\sigma\tau)(a_2)$$

then

$$\sigma(\tau(a_1)) = \sigma(\tau(a_2)),$$

# Permutation Group

Suppose that

$$A = \{1, 2, 3, 4, 5\}$$

and that $\sigma$ is the permutation. We write $\sigma$ in a more standard notation, changing the columns to rows in parentheses and omitting the arrows, as

$$\sigma = \begin{pmatrix} 1 & 2 & 3 & 4 & 5 \\ 4 & 2 & 5 & 3 & 1 \end{pmatrix}$$

# Permutation Group

so that $\sigma(1) = 4, \sigma(2) = 2$, and so on. Let

$$\tau = \begin{pmatrix} 1 & 2 & 3 & 4 & 5 \\ 3 & 5 & 4 & 2 & 1 \end{pmatrix}.$$

Then

$$\sigma\tau = \begin{pmatrix} 1 & 2 & 3 & 4 & 5 \\ 4 & 2 & 5 & 3 & 1 \end{pmatrix} \begin{pmatrix} 1 & 2 & 3 & 4 & 5 \\ 3 & 5 & 4 & 2 & 1 \end{pmatrix} = \begin{pmatrix} 1 & 2 & 3 & 4 & 5 \\ 5 & 1 & 3 & 2 & 4 \end{pmatrix}.$$

For example, multiplying in right-to-left order,

$$(\sigma\tau)(1) = \sigma(\tau(1)) = \sigma(3) = 5.$$

# Exercise 5

In Exercises 1 through 5 , compute the indicated product involving the following permutations in $S_6$ :

$$\sigma = \begin{pmatrix} 1 & 2 & 3 & 4 & 5 & 6 \\ 3 & 1 & 4 & 5 & 6 & 2 \end{pmatrix}, \quad \tau = \begin{pmatrix} 1 & 2 & 3 & 4 & 5 & 6 \\ 2 & 4 & 1 & 3 & 6 & 5 \end{pmatrix}, \quad \mu = \begin{pmatrix} 1 & 2 & 3 & 4 & 5 & 6 \\ 5 & 2 & 4 & 3 & 1 & 6 \end{pmatrix}$$

1. $\tau\sigma$
2. $\tau^2\sigma$
3. $\mu\sigma^2$
4. $\sigma^{-2}\tau$
5. $\sigma^{-1}\tau\sigma$

# Exercise 5 Solution

1. $\begin{pmatrix} 1 & 2 & 3 & 4 & 5 & 6 \\ 1 & 2 & 3 & 6 & 5 & 4 \end{pmatrix}$
2. $\begin{pmatrix} 1 & 2 & 3 & 4 & 5 & 6 \\ 2 & 4 & 1 & 5 & 6 & 3 \end{pmatrix}$
3. $\begin{pmatrix} 1 & 2 & 3 & 4 & 5 & 6 \\ 3 & 4 & 1 & 6 & 2 & 5 \end{pmatrix}$
4. $\begin{pmatrix} 1 & 2 & 3 & 4 & 5 & 6 \\ 5 & 1 & 6 & 2 & 4 & 3 \end{pmatrix}$
5. $\begin{pmatrix} 1 & 2 & 3 & 4 & 5 & 6 \\ 2 & 6 & 1 & 5 & 4 & 3 \end{pmatrix}$

# Exercise 6

In Exercises 6 through 9, compute the expressions shown for the permutations $\sigma, \tau$ and $\mu$ defined prior to Exercise 1 .

6. $|\langle \sigma \rangle|$
7. $|\langle \tau^2 \rangle|$
8. $\sigma^{100}$
9. $\mu^{100}$

# Exercise 6 Solution

6. Starting with 1 and applying $\sigma$ repeatedly, we see that $\sigma$ takes 1 to 3 to 4 to 5 to 6 to 2 to 1 , so $\sigma^6$ is the smallest possible power of $\sigma$ that is the identity permutation. It is easily checked that $\sigma^6$ carries $2, 3, 4, 5$ and 6 to themselves also, so $\sigma^6$ is indeed the identity and $|\langle\sigma\rangle| = 6$.

7. $\tau^2 = \begin{pmatrix} 1 & 2 & 3 & 4 & 5 & 6 \\ 4 & 3 & 2 & 1 & 5 & 6 \end{pmatrix}$ and it is clear that $\left(\tau^2\right)^2$ is the identity. Thus we have $\left|\left\langle\tau^2\right\rangle\right| = 2$.

8. Because $\sigma^6$ is the identity permutation (see Exercise 6 ), we have

$$\sigma^{100} = \left(\sigma^6\right)^{16}\sigma^4 = \sigma^4 = \begin{pmatrix} 1 & 2 & 3 & 4 & 5 & 6 \\ 6 & 5 & 2 & 1 & 3 & 4 \end{pmatrix}$$

9. We find that $\mu^2$ is the identity permutation, so $\mu^{100} = \left(\mu^2\right)^{50}$ is also the identity permutation.

# Homomorphism

**Definition**

A map $\phi$ of a group $G$ into a group $G'$ is a homomorphism if the homomorphism property

$$\phi(ab) = \phi(a)\phi(b)$$

holds for all $a, b \in G$.

# Homomorphism

Let $S_n$ be the symmetric group on $n$ letters, and let $\phi : S_n \to \mathbb{Z}_2$ be defined by $\phi(\sigma) = \begin{cases} 0 & \text{if } \sigma \text{ is an even permutation,} \\ 1 & \text{if } \sigma \text{ is an odd permutation.} \end{cases}$

Show that $\phi$ is a homomorphism.

We must show that $\phi(\sigma\mu) = \phi(\sigma) + \phi(\mu)$ for all choices of $\sigma, \mu \in S_n$. Note that the operation on the right-hand side of this equation is written additively since it takes place in the group $\mathbb{Z}_2$. Verifying this equation amounts to checking just four cases:

$\sigma$ odd and $\mu$ odd,

$\sigma$ odd and $\mu$ even,

$\sigma$ even and $\mu$ odd,

$\sigma$ even and $\mu$ even.

Checking the first case, if $\sigma$ and $\mu$ can both be written as a product of an odd number of transpositions, then $\sigma\mu$ can be written as the product of an even number of transpositions. Thus $\phi(\sigma\mu) = 0$ and $\phi(\sigma) + \phi(\mu) = 1 + 1 = 0$ in $\mathbb{Z}_2$.

# Homomorphism

The image of a homomorphism $f : G \to G'$, often denoted by im $f$, or $f(G)$, is simply the image of as a map of sets:

$$\operatorname{im} f = \left\{ x \in G' \mid x = f(a) \text{ for some } a \in G \right\}$$

The kernel of $f$, denoted by ker $f$, is the set of elements of $G$ that are mapped to the identity in $G'$ :

$$\ker f = \left\{ a \in G \mid f(a) = 1_{G'} \right\}.$$

# Homomorphism

Let $\phi$ be a homomorphism of a group $G$ into a group $G'$.

1. If $e$ is the identity element in $G$, then $\phi(e)$ is the identity element $e'$ in $G'$.
2. If $a \in G$, then $\phi\left(a^{-1}\right) = \phi(a)^{-1}$.
3. If $H$ is a subgroup of $G$, then $\phi[H]$ is a subgroup of $G'$.
4. If $K'$ is a subgroup of $G'$, then $\phi^{-1}[K']$ is a subgroup of $G$.

# Isomorphism

To Show $\phi : G \to G'$ Is an Isomorphism
Step 1 Show $\phi$ is a homomorphism.
Step 2 Show $\text{Ker}(\phi) = \{e\}$.
Step 3 Show $\phi$ maps $G$ onto $G'$.

# Exercise 7

Determine whether the given map $\phi$ is a homomorphism.

1. Let $\phi : \mathbb{Z} \to \mathbb{R}$ under addition be given by $\phi(n) = n$.
2. Let $\phi : \mathbb{R} \to \mathbb{Z}$ under addition be given by $\phi(x) =$ the greatest integer $\leq x$.
3. Let $\phi : \mathbb{R}^* \to \mathbb{R}^*$ under multiplication be given by $\phi(x) = |x|$.

# Exercise 7 Solution

1. It is a homomorphism, because
$\phi(m+n) = m+n = \phi(m) + \phi(n)$.
2. It is not a homomorphism, because $\phi(2.6+1.6) = \phi(4.2) = 4$
but $\phi(2.6) + \phi(1.6) = 2+1 = 3$.
3. It is a homomorphism, because
$\phi(xy) = |xy| = |x||y| = \phi(x)\phi(y)$ for $x, y \in \mathbb{R}^*$.

# Coset

Given a group $G$, if $H \leq G$ is a subgroup and $a \in G$, the notation aH will stand for the set of all products ah with $h \in H$,

$$aH = \{g \in G \mid g = ah \text{ for some } h \in H\}$$

This set is called a left coset of $H$ in $G$

# Coset

Exhibit the left cosets and the right cosets of the subgroup $3\mathbb{Z}$ of $\mathbb{Z}$.

Our notation here is additive, so the left coset of $3\mathbb{Z}$ containing $m$ is $m + 3\mathbb{Z}$. Taking $m = 0$, we see that

$$3\mathbb{Z} = \{\cdots, -9, -6, -3, 0, 3, 6, 9, \cdots\}$$

is itself one of its left cosets, the coset containing 0 . To find another left coset, we select an element of $\mathbb{Z}$ not in $3\mathbb{Z}$, say 1 , and find the left coset containing it. We have

$$1 + 3\mathbb{Z} = \{\cdots, -8, -5, -2, 1, 4, 7, 10, \cdots\}.$$

These two left cosets, $3\mathbb{Z}$ and $1 + 3\mathbb{Z}$, do not yet exhaust $\mathbb{Z}$. For example, 2 is in neither of them. The left coset containing 2 is

$$2 + 3\mathbb{Z} = \{\cdots, -7, -4, -1, 2, 5, 8, 11, \cdots\}$$

# Coset

It is clear that these three left cosets we have found do exhaust $\mathbb{Z}$, so they constitute the partition of $\mathbb{Z}$ into left cosets of $3\mathbb{Z}$.
Since $\mathbb{Z}$ is abelian, the left coset $m+3\mathbb{Z}$ and the right coset $3\mathbb{Z}+m$ are the same, so the partition of $\mathbb{Z}$ into right cosets is the same.

# Coset

Every coset (left or right) of a subgroup $H$ of a group $G$ has the same number of elements as $H$.

# Theorem of Lagrange

(Theorem of Lagrange) Let $H$ be a subgroup of a finite group $G$. Then the order of $H$ is a divisor of the order of $G$.
Prove: Let $n$ be the order of $G$, and let $H$ have order $m$. The preceding boxed statement shows that every coset of $H$ also has $m$ elements. Let $r$ be the number of cells in the partition of $G$ into left cosets of $H$. Then $n = rm$, so $m$ is indeed a divisor of $n$.

# Corollary 1

Every group of prime order is cyclic.
Prove: Let $G$ be of prime order $p$, and let $a$ be an element of $G$ different from the identity. Then the cyclic subgroup $\langle a \rangle$ of $G$ generated by $a$ has at least two elements, $a$ and $e$. But by Theorem of Lagrange, the order $m \geq 2$ of $\langle a \rangle$ must divide the prime $p$. Thus we must have $m = p$ and $\langle a \rangle = G$, so $G$ is cyclic.

# Corollary 2

The order of an element of a finite group divides the order of the group.
Prove: Remembering that the order of an element is the same as the order of the cyclic subgroup generated by the element, we see that this theorem follows directly from Theorem of Lagrange.

# Coset

Let $H$ be a subgroup of a group $G$. The number of left cosets of $H$ in $G$ is the index $(G : H)$ of $H$ in $G$.

# Exercise 8

1. Find all cosets of the subgroup $4\mathbb{Z}$ of $2\mathbb{Z}$.
2. Find all cosets of the subgroup $\langle 2 \rangle$ of $\mathbb{Z}_{12}$.
3. Find all cosets of the subgroup $\langle 4 \rangle$ of $\mathbb{Z}_{12}$.
4. Find all cosets of the subgroup $\langle 18 \rangle$ of $\mathbb{Z}_{36}$.
5. Find the index of $\langle 3 \rangle$ in the group $\mathbb{Z}_{24}$.
6. Let $\sigma = (1, 2, 5, 4)(2, 3)$ in $S_5$. Find the index of $\langle \sigma \rangle$ in $S_5$.
7. Let $\mu = (1, 2, 4, 5)(3, 6)$ in $S_6$. Find the index of $\langle \mu \rangle$ in $S_6$.

# Exercise 8 Solution

1. $4\mathbb{Z} = \{\cdots, -8, -4, 0, 4, 8, \cdots\}, 2 + 4\mathbb{Z} = \{\cdots, -6, -2, 2, 6, 10, \cdots\}$
2. $\langle 2\rangle = \{0, 2, 4, 6, 8, 10\}, 1 + \langle 2\rangle = \{1, 3, 5, 7, 9, 11\}$
3. $\langle 4\rangle = \{0, 4, 8\}, \quad 1 + \langle 4\rangle = \{1, 5, 9\}, \quad 2 + \langle 4\rangle = \{2, 6, 10\}, \quad 3 + \langle 4\rangle = \{3, 7, 11\}$
4. $\langle 18\rangle = \{0, 18\}, \quad 1 + \langle 18\rangle = \{1, 19\}, \quad 2 + \langle 18\rangle = \{2, 20\}, \quad \cdots, \quad 17 + \langle 18\rangle = \{17, 35\}$
5. $\langle 3\rangle = \{1, 3, 6, 9, 12, 15, 18, 21\}$ has 8 elements, so its index (the number of cosets) is $24/8 = 3$.
6. $\sigma = (1, 2, 5, 4)(2, 3) = (1, 2, 3, 5, 4)$ generates a cyclic subgroup of $S_5$ of order 5 , so its index (the number of left cosets) is $5!/5 = 4! = 24$.
7. $\mu = (1, 2, 4, 5)(3, 6)$ generates a cyclic subgroup of $S_6$ of order 4 , (the cycles are disjoint) so its index (the number of left cosets) is $6!/4 = 720/4 = 180$.

# Normal Subgroup

**Definition**

A subgroup $H$ of a group $G$ is normal if its left and right cosets coincide, that is, if $gH = Hg$ for all $g \in G$.
Note that all subgroups of abelian groups are normal.

**Corollary**

If $\phi : G \to G'$ is a group homomorphism, then $\mathrm{Ker}(\phi)$ is a normal subgroup of $G$.

# Q&A

Q&A