isomorphic

a function for *graph*
there exist a function $\varphi : V(G) \to V(H)$ that
injective: no two nodes in V mapped to the same node in H
surjective : every node in H are mapped by G
(all together called bijective, one-to-one correspond)
$v_{1,}v_2 \in E(G) \iff \varphi(v_{1)}\varphi(v_2)$ if two nodes adjacent in G, the corresponding nodes should also be adjacent in H and vice versa
the function is called isomorphism

homomorphism

homomorphism is to find a structural similarity between two *groups*
suppose we have two groups

$G*\ H\diamond$
$x, y \in G$
$x * y = z$
and a map function
$f : G \to H$

$$\begin{aligned} x &\mapsto f(x) \\ y &\mapsto f(y) \\ z &\mapsto f(z) \end{aligned}$$

f is homomorphism if

$$\begin{aligned} x * y = z &\Rightarrow f(x) \diamond f(y) = f(z) \\ &\Rightarrow f(x) \diamond f(y) = f(x * y) \end{aligned}$$

example one:

$G = \mathbb{R}$ under $+$

$\text{ abelian, identity } = 0$

$H = \mathbb{R}^{+}$under $\times$

$\text{ abelian, identity} = 1$

$f : G \rightarrow H$

$x \mapsto e^{x}$

$f(x+y) = f(x) \times f(y)$

$e^{x+y} = e^{x} \times e^{y}$

example two:

$G = \mathbb{R}$ under $+$

$H = \{\text{z} \in \mathbb{C} : |\text{z}| = 1\}$

$\quad = \text{ Group under } \times$

Hint:

Every $z \in \mathbb{C}$ with $|z| = 1$ can be written as $z = e^{i\theta}$.

$$f : G \rightarrow H$$

$$x \mapsto e^{ix}$$

show $f(x+y) = f(x) \times f(y)$

$$e^{i(x+y)} = e^{ix} \times e^{iy}$$

$$e^{ix+iy} = e^{ix} \times e^{iy}$$

$$e^{ix} \times e^{iy} = e^{ix} \times e^{iy}$$

note that $f(2\pi n) = 1$, so homomorphism don't necessary 1 to 1

homo(same) + morph(shape)

Kernel

a subgroup, but the property of homomorphism function

homomorphism send identities to identities , and inverses to inverses

$f\left(1_{G}\right) = 1_{H}$

$f\left(x^{-1}\right) = y^{-1}$

$G *\ H \diamond$

suppose $f : G \rightarrow H$ is not one to one

$f\left(x_{1}\right) = y \Rightarrow f\left(x_{1}\right) \diamond f\left(x_{1}^{-1}\right) = y \diamond f\left(x_{1}^{-1}\right)$

$f\left(x_{2}\right) = y \Rightarrow f\left(x_{2}\right) \diamond f\left(x_{1}^{-1}\right) = y \diamond f\left(x_{1}^{-1}\right)$

$$f\left(x_1\right)=y \Rightarrow f\left(x_1\right) \diamond f\left(x_1^{-1}\right)=y \diamond y^{-1}$$
$$f\left(x_2\right)=y \Rightarrow f\left(x_2\right) \diamond f\left(x_1^{-1}\right)=y \diamond y^{-1}$$

$$f\left(x_1\right)=y \Rightarrow f\left(x_1\right) \diamond f\left(x_1^{-1}\right)=1_H$$
$$f\left(x_2\right)=y \Rightarrow f\left(x_2\right) \diamond f\left(x_1^{-1}\right)=1_H$$

$$f\left(x_1\right)=y \Rightarrow f\left(x_1 * x_1^{-1}\right)=1_H$$
$$f\left(x_2\right)=y \Rightarrow f\left(x_2 * x_1^{-1}\right)=1_H$$

this means there are multiple elements in G which all map to the identity in H, these *elements* are called kernel of f
$\operatorname{ker}(f)=\{x \in G \mid f(x)=1_H\}$
kernel is the property of homomorphism, not the groups
if f is not 1-1, then $\operatorname{ker}(f)$ has more than 1 element
for homomorphism, we have $f\left(1_G\right)=1_H \Rightarrow 1_G \in \operatorname{ker}(f)$
this means the kernel is never empty, it always contains the identity 1_G
$\operatorname{ker}(f)=\{1_G\} \Rightarrow \text{f is } 1-1$
the kernel is the subset of G, also a subgroup of G.

Lagrange's Theorem

a group G always two standard subgroups:
1 G
2 Trivial Group = {e}

Lagrange's Theorem:
If $H \leq G$, then the *order* of H divides the *order* of G.
Order of group: $G=\#$ of elements in G = $|G|$
Lagrange's Theorem:

$$H \leq G \Longrightarrow |H| \text{ divides } |G|$$

this means the order of a subgroup must be a factor of its group, but not any factor can form a subgroup.

order of element

NOTE: different with order of group
the order of $x \in G$ is the smallest positive integer n such that $x^n = e$
Notation: $|x| = n$

example
the non-zero real numbers form a group under multiplication, because 0 doesn't have a multiplicative inverse
$\mathbb{R}^\times$ multiplication
identity = 1
$|1| = 1$
$|-1| = 2$

example
$\mathbb{C}^\times$ multiplication
infinite z where $z^n = 1$, they are 'roots of unity'
$i = \sqrt{-1}$
$|i| = 4$

example
Elements: $\begin{pmatrix} a & b \\ c & d \end{pmatrix}$ where $a, b, c, d \in \mathbb{R}$
Operation: matrix multiplication
To have an inverse, $\begin{vmatrix} a & b \\ c & d \end{vmatrix} \neq 0$
"General Linear Group": $\mathrm{GL}_2(\mathbb{R})$
Identity element: $I = \begin{pmatrix} 1 & 0 \\ 0 & 1 \end{pmatrix}$
$M = \begin{pmatrix} \frac{\sqrt{3}}{2} & \frac{-1}{2} \\ \frac{1}{2} & \frac{\sqrt{3}}{2} \end{pmatrix}$
$|M| = 12$

Normal Subgroups and Quotient Groups

consider integers mod 5
$\mathbb{Z} \bmod 5 = \{\bar{0}, \bar{1}, \bar{2}, \bar{3}, \bar{4}\}$
these 5 sets called congruence classes, they also form a group under addition

identity element: $\bar{0}$
each set has an inverse $\bar{1}+\bar{4}=\bar{0}\,\bar{2}+\bar{3}=\bar{0}$
if a, b in the same congruence class $a \equiv b(\mod n)$, means a and b have the same remainder when you divide by n

example:
the group $\mathbb{Z}$ under + has infinite subgroups. now we only consider $5\mathbb{Z}$
we use the subgroup $5\mathbb{Z}$ to partition the group $\mathbb{Z}$ into cosets
$1+5\mathbb{Z}$, $2+5\mathbb{Z}$, $3+5\mathbb{Z}$, $4+5\mathbb{Z}$
note that coset is not group
so the original group $\mathbb{Z}$ is covered by one subgroup $5\mathbb{Z}$ and 4 cosets. (you can also think the subgroup $5\mathbb{Z}$ as coset $0+\mathbb{Z}$)
because that the 5 cosets form a group, we call $5\mathbb{Z}$ a normal subgroup.
the group of cosets is called quotient group $\mathbb{Z}/5\mathbb{Z}$
note: we have a group $\mathbb{Z}$ and a normal group $5\mathbb{Z}$, we use it to form a quotient group $\mathbb{Z}/5\mathbb{Z}$, but the quotient group is not a subgroup of $\mathbb{Z}$, it is a entirely different group

generalize:
Group G, and subgroup N
we can use N to generate a collection of non-overlapping coset
$N,\ g_1N,\ g_2N,\ g_3N\ \ldots$

> but do the cosets always form a group?

-- NO
if the cosets do not form a group we do not call N a normal subgroup. so we can not make a quotient group

> what properties N must have in order for the cosets to be a group?

assume N partition G into t cosets
each left coset = gN for some $g \in G$
pick two cosets : $xN\ yN$
Since $e \in N, x \cdot e = x \in xN$ and $y \cdot e = y \in yN$
for cosets act like a group, we need $x \cdot y \in (xN)(yN)$, i.e. $(xN)(yN) = xyN$

under this condition,
Pick element from coset $xN \to x \cdot n_1$
Pick element from coset $yN \to x \cdot n_2$
if the cosets are group,
$(x \cdot n_1) \cdot (y \cdot n_2) \in xyN \Longrightarrow (x \cdot n_1) \cdot (y \cdot n_2) = x \cdot y \cdot n_3$
$(x \cdot n_1) \cdot (y \cdot n_2) = x \cdot y \cdot n_3$
$x^{-1} \cdot (x \cdot n_1) \cdot (y \cdot n_2) = x^{-1} \cdot (x \cdot y \cdot n_3)$
$n_1 \cdot y \cdot n_2 = y \cdot n_3$
$y^{-1} \cdot (n_1 \cdot y \cdot n_2) = y^{-1} \cdot (y \cdot n_3)$
$y^{-1} \cdot n_1 \cdot y \cdot n_2 = n_3$
$\left(y^{-1} \cdot n_1 \cdot y \cdot n_2\right) \cdot n_2^{-1} = n_3 \cdot n_2^{-1}$
$y^{-1} \cdot n_1 \cdot y = n_3 \cdot n_2^{-1} \in N$
$y^{-1} \cdot n_1 \cdot y \in N$
this means $y^{-1}Ny \subseteq N$
try to proof $y^{-1}Ny \supseteq N$ yourself
so, If $(xN) \cdot (yN) = xyN$, then $y^{-1} \cdot N \cdot y = N$
we call $y^{-1} \cdot N \cdot y$ conjugate
now we check the coset form a group:
the identity group is $N = eN$ because $(eN)(gN) = (eg)N = gN$
the inverse group is $(gN)^{-1} = g^{-1}N$ because
$\left(g^{-1}N\right)(gN) = \left(g^{-1} \cdot g\right)N = eN = N$

we just proofed that if $N \leq G$ and cosets form a group, then
$y^{-1}Ny = N \; |\forall y \in G$
we can proof that the converse is also true
Assume $y^{-1}Ny = N$ for any $y \in G$
claim: the cosets form a group
Pick two cosets: xN, yN

$$\begin{aligned}
&(x \cdot n_1)\,(y \cdot n_2) \\
=&x \cdot \left(y \cdot y^{-1}\right) \cdot n_1 \cdot y \cdot n_2 \\
=&x \cdot y \cdot \left(y^{-1} \cdot n_1 \cdot y\right) \cdot n_2 \\
=&x \cdot y \cdot n_3 \cdot n_2 \\
=&x \cdot y \cdot n_4 \in xyN
\end{aligned}$$

$\therefore (xN)(yN) = xyN$

we just proofed that Let $N \leq G$, cosets form a group $\Leftrightarrow y^{-1}Ny = N$ for any $y \in G$
when this is true, we call N is normal subgroup of G, notation: $N \trianglelefteq G$
the cosets group called factor group, aka quotient group, Notation: G/N
the identity for quotient group is N
the inverse of $x \cdot N$ is $x^{-1} \cdot N$

Every group G has at least 2 subgroups {e} and G, they are all normal group
if the only normal subgroup of G are {e} and G, then G is a simple group
a simple group does not have any factor groups, and they are the building blocks of other groups.

symmetric group

S_n means group of permutations on a set with n elements, permutation means rearrangement of the set.

permutation of {1, 2, 3} is {123} {132} {213} {231} {312} {321}
the permutation acts a bijection function from the set {123} to itself, e.g. $1 \rightarrow 2,\ 2 \rightarrow 3,\ 3 \rightarrow 1$ $\mathrm{f} : \{1, 2, 3\} \rightarrow \{1, 2, 3\}$ f(1)=2 f(2)=3 f(3)=1

> how define Multiplication?

$\{\, 1 \rightarrow 2,\ 2 \rightarrow 3,\ 3 \rightarrow 1 \,\} * \{\, 1 \rightarrow 3,\ 2 \rightarrow 1,\ 3 \rightarrow 2 \,\}$
$f(1) = 2$
$f(2) = 3$
$f(3) = 1$
and
$g(1) = 3$
$g(2) = 1$
$g(3) = 2$
so
$f \circ g(1) = 1$
$f \circ g(2) = 2$
$f \circ g(3) = 3$
$\mathrm{f} \circ \mathrm{g} =$ identity element

or we can write permutation in a impact way
$\begin{pmatrix} 1 & 2 & 3 & 4 \\ 1 & 3 & 4 & 2 \end{pmatrix} \quad \begin{pmatrix} 1 & 2 & 3 & 4 \\ 4 & 3 & 2 & 1 \end{pmatrix}$

note that do calculate from right to left
$\begin{pmatrix} 1 & 2 & 3 & 4 \\ 1 & 3 & 4 & 2 \end{pmatrix} * \begin{pmatrix} 1 & 2 & 3 & 4 \\ 4 & 3 & 2 & 1 \end{pmatrix} = \begin{pmatrix} 1 & 2 & 3 & 4 \\ 2 & 4 & 3 & 1 \end{pmatrix}$

it is different when we switch the order, so S_4 is not commutative, it is a non-abelian group
every finite group is a subgroup of a symmetric group

cyclic groups

a group G is 'cyclic' if it's generated by a single element $G = \langle x \rangle$

Let G be a group with operation $\times$
pick $x \in G$
what is the smallest subgroup of G that contains x?
$$\begin{aligned} \langle x \rangle &= \{\dots, x^{-4}, x^{-3}, x^{-2}, x^{-1}, 1, x, x^2, x^3, x^4, \dots\} \\ &= \text{ Group generated by } x \end{aligned}$$
If $G = \langle x \rangle$ for some x, then we call G a cyclic group.

example
Group: integers $\mathbb{Z}$ under +
claim: $\mathbb{Z} = \langle 1 \rangle$
$\langle 1 \rangle$ must contains itself 1, identity 0, and inverse -1, and all multiples of 1 and -1
so $\langle 1 \rangle = \{\dots - 4, -3, -2, -1, 0, 1, 2, 3, 4 \dots\}$ covers all integers
so the $\mathbb{Z}$ is cyclic group

let's now look at the finite cyclic group
Group: G = Integers mod n under addition
elements: {0 1 2 3.. n-1}
G also can be generated by 1, $G = \langle 1 \rangle$, so G is cyclic
the group generated by 1 is repeat. so it called cyclic

cyclic group:
$\mathbb{Z}, +$ infinite
$\mathbb{Z}/n\mathbb{Z}, +$ finite
they are all cyclic groups

the fundamental theorem of finitely generated Abelian groups: any Abelian group that is finitely generated can be broken apart into a finite number of cyclic groups, and every cyclic group is either the integers, or the integers mod N. So cyclic groups are the fundamental building blocks for finitely generated Abelian groups.

cycle notation for permutation

$\begin{pmatrix} 1 & 2 & 3 & 4 & 5 \\ 3 & 5 & 4 & 1 & 2 \end{pmatrix}$
(1 3 4)(2 5) each bracket is one cycle and each bracket can be seen as a map function, the 2-cycle is also called transposition
note: cycles with no numbers in common *commute* with each other

dihedral group

dihedral means two faces
the symmetry means it looks the same after transition
when the shape is a regular polygon, the group of symmetry is called dihedral group
1 identity e, means do nothing
2 clockwise rotation with angle $\frac{2\pi}{n}$ denoted by r, note that $r^n = e$
3 reflection f, note that $f^2 = e$
4 r+f note $r \cdot f \neq f \cdot r$
the dihedral group is not commutative
symmetry groups of triangle: $\{e \quad r \quad r^2\ f \quad rf \quad r^2f\}$

matrix group

$\mathrm{GL_n}(\mathbb{R})$: General Linear Group, need $\det(M) \neq 0$
$\mathrm{SL_n}(\mathbb{R})$: Special Linear Group, means $n \times n$ matrices with determinant 1

direct product

the direct product combine two groups
$G_1 \times G_2 = \{(x, y) \mid x \in G_1, y \in G_2\}$

the direct product is component-wise
Let $(a, b), (x, y) \in G_1 \times G_2$
$(a, b) \cdot (x, y) = (a \cdot x, b \cdot y)$
Identity element $= (e_1, e_2)$
$e_1 =$ identity in G_1
$e_2 =$ identity in G_2

example
$G_1 = \mathbb{Z}$ under $+$
$G_2 = \{1, -1, i, -i\}$ under $\times$
$G_1 \times G_2 = \{(x, y) \mid x \in \mathbb{Z}, y = \pm 1 \text{ or } \pm i\}$
group operation:
$(7, -1) \cdot (-3, i) = (7 - 3, -1 \cdot i) = (4, -i)$
the identity is (0, 1)

simple group

recall normal group:
$g \cdot N \cdot g^{-1} = N$ for all $g \in G \Rightarrow N \leq G$ is normal
the important feature of normal group is that you can use N to split G into a bunch of cosets, and you can treat these cosets as factor group. in this factor group N is the identity element

normal series:
$1 \lhd \cdots \lhd N_4 \lhd N_3 \lhd N_2 \lhd N_1 \lhd G$
the subgroups need to be maximal and proper, i.e. pick as big a normal subgroup of G as possible

we call a normal series as long as possible a composition series
Jordan-Holder theorem: 2 series for one group G are equivalent
in a Composition series , each quotient group is simple group.

there are 4 sets of simple groups

1. $\mathbb{Z}/p\mathbb{Z}$ where p is prime (abelian)
2. alternating group A_n for $n \geq 5$ (non-abelian)
3. groups of Lie type
4. 26 Sporadic Group

Ring

A RING is a set R which is CLOSED under two operations + and $\times$ and satisfying the following properties:
(1) R is an abelian group under +
(2) Associativity of $\times$, i. e. - For every $a, b, c \in R$, $a \times (b \times c) = (a \times b) \times c$
(3) Distributive Properties i.e. - For every $a, b, c \in R$ the following identities hold: $a \times (b + c) = (a \times b) + (a \times c)$ and $(b + c) \times a = b \times a + c \times a$.

if a ring is commutative , we call it 'commutative ring'
if a ring with inverses for $\times$ we call it 'division ring'
commutative division ring = Field

example of ring :
integer $\mathbb{Z}$
real polynomials $\mathbb{R}[x] = \{a_n x^n + a_{n-1} x^{n-1} + \cdots + a_1 x + a_0 \mid a_i \in \mathbb{R}\}$
it means polynomials with coefficients in $\mathbb{R}$
$\mathbb{R}(x) = \left\{ \frac{f(x)}{g(x)} \mid f, g \in \mathbb{R}[x] \right\}$
means rational functions

a ring without identity for $\times$ is $2\mathbb{Z}$ means the set of even integers

example of finite ring: $\mathbb{Z}/n\mathbb{Z}$
if n is prime, $\mathbb{Z}/p\mathbb{Z}$ is a field
every field is a ring but not every ring is a field

in a ring R, every element has additive inverses but not every element has multiplicative inverses

Units is elements in R with a inverse under multiplication. Unites form a group under $\times$, denoted as $R^\times$

example:
the integers $\mathbb{Z}$ is a commutative ring
integers with multiplicative inverse : 1, -1
no other integer has an inverse
e.g. $3^{-1} = \frac{1}{3}$ not a integer
so $\mathbb{Z}^\times = \{1, -1\}$ is group of unites
and Integer $\times$ Unit = Associate

ring: $\mathbb{Z}/12\mathbb{Z}$
units: {1 5 7 11}

The fundamental theorem of Arithmetic : every integer n has a prime factorization that is unique up to order and associates.

integral domains

consider the equation $x^2 + 5x + 6 \equiv 0$ in the ring of $\mathbb{Z}/12\mathbb{Z}$
using factoring $(x+2)(x+3) \equiv 0 (\mod 12)$
we have solution x=10 or x=9
but in fact x=1 x=6 also a solution.
so here is a solution to the equation that we did not find by factoring.

in abstract algebra two non-zero factors can be multiplied get 0

$\mathbb{Z}/12\mathbb{Z}$ has zero divisor
but $\mathbb{Z}/11\mathbb{Z}$ have no zero divides, because 11 is prime

integral domain is a commutative ring R, with multiplicative identity 1 and no zero divisors

a non-commutative ring R with no zero divisors is a Domain

ideals

ideals to rings is likely normal subgroup to group

I is an of R ideal if
$I \leq R$ (subgroup)
for any $r \in R, x \in I$:
$x \cdot r \in I$ and $r \cdot x \in I$

Ideal $I \trianglelefteq R$ is
normal subgroup under $+$
closed under $\times$
I is almost a subring

ideals are not technically subring because they do not have multiplicative identity

example
Ring : $\mathbb{Z}[x]$
Ideal: $J = x \cdot \mathbb{Z}[x]$

field

Analogy:
$+-$ Group
$+-\times$ Ring
$+-\times\div$ Field

loosely speaking
commutative groups under $+$
have another operation multiplication which makes them rings
commutative rings
multiplicative inverses

technically speaking
Set F with 2 operations: $+ \quad \cdot$
$\langle F, + \rangle$ is a commutative group
$\langle F^{\times}, \cdot \rangle$ is a commutative group
also with distributive property
$a \cdot (b + c) = a \cdot b + a \cdot c$
$(b + c) \cdot a = b \cdot a + c \cdot a$

some famous fields:
Rational numbers
Real numbers
Complex numbers

$\mathbb{Z}$ is not a field, $\mathbb{Z}$ is an abelian group under $+$, but it has no multiplicative inverses.

Rational numbers $\mathbb{Q}$ is a field, add $\sqrt{2}$, $\mathbb{Q}(\sqrt{2})$ is an extension field of $\mathbb{Q}$

Let α be a solution to:
$a_n x^n + a_{n-1} x^{n-1} + \cdots + a_1 x + a_0 = 0$
where the coefficients a_i are fractions.
$\mathbb{Q}(\alpha)$ is an extension field of $\mathbb{Q}$, which is called algebraic extension

convergence sequence:
(1) we start with $\mathbb{Q}$
(2) find a sequence $a_1, a_2, a_3, \ldots$ converges to L
(3) add L to $\mathbb{Q}$
(4) repeat ...
Result: $\mathbb{R}$ = Real Number
any sequence in $\mathbb{R}$ converges in $\mathbb{R}$, so $\mathbb{R}$ is complete

if we add $i = \sqrt{-1}$ to $\mathbb{R}$
we get $\mathbb{R}(i) = \mathbb{C}$ = Complex Numbers
Complex Number is complete

Vector Space

Abelian group V of "vectors"
Field F of "scalars"
$f \cdot v$ is a "scaled vector"
Distributive properties:
$f \cdot (v_1 + v_2) = f \cdot v_1 + f \cdot v_2$
$(f_1 + f_2) \cdot v = f_1 \cdot v + f_2 \cdot v$
Associative property:

$(f_1 \cdot f_2) \cdot v = f_1 \cdot (f_2 \cdot v)$
$1 \cdot v = v$

the study of vector space is called Linear Algebra

Module

Abelian group M of "elements"
Ring R of "scalars"
$r \cdot m$ is a "scaled element"
Distributive properties:
$r \cdot (m_1 + m_2) = r \cdot m_1 + r \cdot m_2$
$(r_1 + r_2) \cdot m = r_1 \cdot m + r_2 \cdot m$
Associative property:
$(r_1 \cdot r_2) \cdot m = r_1 \cdot (r_2 \cdot m)$
$1 \cdot m = m$

module is a generalization of vector space.

Module = Vector Space with a ring of scalars
Vector Space = Module with a field of scalars