

8/26/2019

$\mathbb{Z} = \{-\dots, -2, -1, 0, 1, 2, \dots, 3\}$ $(\mathbb{Z}, +)$ is a group

$\mathbb{Q} = \left\{ \frac{m}{n} \mid m, n \in \mathbb{Z}, n \neq 0 \right\}$ $(\mathbb{Q}, +)$ is a group

A group G is abelian if $ab = ba$ for all a, b in G .

Real numbers.

$(\mathbb{R}, +)$ is a group. 0 is the identity

inverse of a is $-a$. since $a+b = b+a$, they are abelian.

ex: $\{1, 3, -1, -3, 1, -1, i, -i\}$

Are abelian groups of complex numbers under multiplication

ex: $(-1)(-1) = 1$ -1 is self inverse.

$i(-i) = -i^2 = -(-1) = 1$ i and $-i$ are inverses

ex: $C = \{a+bi \mid a, b \in \mathbb{R}, i^2 = -1\}$

$(a+bi) + (c+di) = (a+c) + (b+d)i$ $(C, +)$ is an abelian group

$$\begin{aligned}(a+bi) \cdot (c+di) &= ac + adi + bci + bd i^2 \\ &= (ac - bd) + (ad + bc)i\end{aligned}$$

$$\frac{1}{a+bi} \cdot \frac{a-bi}{a-bi} = \frac{a-bi}{a^2+b^2} = \frac{a}{a^2+b^2} - \frac{b}{a^2+b^2}i$$

Abelian groups:

$$\mathbb{Q}^\times = (\mathbb{Q} - \{0\}, \cdot)$$

$$\mathbb{R}^\times = (\mathbb{R} - \{0\}, \cdot)$$

$$C^\times = (C - \{0\}, \cdot)$$

Example (same matrix group):

$M(n, \mathbb{R}) = n \times n$ matrix over \mathbb{R}

$(M(n, \mathbb{R}), +)$ is an abelian group

the identity is the zero matrix

the inverse of $A = (a_{ij})$ is $-A = (-a_{ij})$

Matrix multiplication

$M(2, \mathbb{R}) = \left\{ \begin{pmatrix} a & b \\ c & d \end{pmatrix} \mid a, b, c, d \in \mathbb{R} \right\}$ closed under matrix multiplication.

Determinant:

$$\det(A) = \det \begin{pmatrix} a & b \\ c & d \end{pmatrix} = ad - bc$$

General linear group

$GL(2, \mathbb{R}) = \left\{ \begin{pmatrix} a & b \\ c & d \end{pmatrix} \mid ad - bc \neq 0 \right\}$ closed under matrix multiplication

if $A, B \in GL(2, \mathbb{R})$,

then $\det(AB) = \det A \cdot \det B \neq 0$

since $\det A \neq 0$ & $\det B \neq 0$

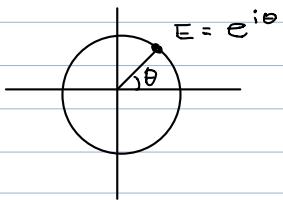
$$\text{Identity } I = \begin{pmatrix} 1 & 0 \\ 0 & 1 \end{pmatrix}$$

$A(BC) = (AB)C$ matrix mult is assoc.

$$A = \begin{pmatrix} a & b \\ c & d \end{pmatrix} \quad A^{-1} = \frac{1}{ad-bc} \begin{pmatrix} d & -b \\ -c & a \end{pmatrix}$$

$GL(2, \mathbb{R})$ is nonabelian

Example - Circle group



$$S^1 = \{E \mid |E| = 1\}$$

$$S^1 = \{E = e^{i\theta} \mid \theta \in \mathbb{R}\}$$

$$e^{i\theta} = \cos \theta + i \sin \theta$$

$$E_1 \cdot E_2 = e^{i\theta_1} \cdot e^{i\theta_2} = e^{i(\theta_1 + \theta_2)}$$

$$E = e^{i\theta}, \quad E^{-1} = e^{-i\theta}$$

Example - n^{th} roots of unity

for $n \geq 1$,

$$\text{let } U_n = \{E \in S^1 \mid E^n = 1\}$$

$$= \{E = e^{\frac{2k\pi i}{n}} \mid k = 0, 1, \dots, n-1\}$$

abelian group under complex multiplication.

subgroup of the circle group

$$U_1 = \{1\}$$

$$U_2 = \{1, -1\}$$

:

$$U_4 = \{E = e^{\frac{2k\pi i}{4}} \mid k = 0, 1, 2, 3\}$$

$$= \{1, e^{\frac{2\pi i}{4}}, e^{\frac{4\pi i}{4}}, e^{\frac{6\pi i}{4}}\}$$

$$= \{1, i, -1, -i\}$$



:

$$U_6 = \{E = e^{\frac{2k\pi i}{6}} \mid k = 0, 1, 2, 3, 4, 5\}$$

$$= \{1, e^{\frac{2\pi i}{6}}, e^{\frac{4\pi i}{6}}, e^{\frac{6\pi i}{6}}, e^{\frac{8\pi i}{6}}, e^{\frac{10\pi i}{6}}\}$$

8/28/2019

A group G is a set with binary operation

$$G \times G \longrightarrow G$$

such that :

(1) Associativity : $(ab)c = a(bc)$ for all $a, b, c \in G$

(2) There exists $e \in G$ the identity

so $ae = ea = a$ for all $a \in G$

(3) Inverse : for each $a \in G$, there some $b \in G$

st $ab = ba = e$

Example: $(\mathbb{Z}, +)$, $(\mathbb{Q}, +)$, $(\mathbb{R}, +)$, $(\mathbb{C}, +)$ $(M(n, \mathbb{R}), +)$

General linear group: $GL(n, \mathbb{R})$, $A \in GL(n, \mathbb{R})$ if $\det A \neq 0$
group under matrix multiplication.

n^{th} root of unity: $U_n = \{E \mid E^n = I\} = \{e^{\frac{2k\pi i}{n}} \mid k=0, \dots, n-1\}$
group under complex product

Euclidean n -space:

for $n \geq 1$.

Let $\mathbb{R}^n = \{(a_1, \dots, a_n) \mid a_1, \dots, a_n \in \mathbb{R}\}$

\mathbb{R}^n is an abelian group under vector addition.

$$(a_1, a_2, \dots, a_n) + (b_1, b_2, \dots, b_n) = (a_1+b_1, a_2+b_2, \dots, a_n+b_n)$$

identity: $\vec{0} = (0, \dots, 0)$

inverse of $\vec{a} = (a_1, a_2, \dots, a_n)$ is $-\vec{a} = (-a_1, -a_2, \dots, -a_n)$

Elementary properties of groups.

Theorem: In a group G , there is only one identity element.

proof: Suppose e and e' are identities in G .

Then since e is an identity, $e'e = e'$

Since e' is an identity $e'e = e$

so $e = e'$

■

Cancellation law

let G be a group and a, b, c in G

1) If $ba = ca$ then $b = c$ right cancellation.

2) If $ab = ac$ then $b = c$ left cancellation.

proof: 1) Suppose $ba = ca$ and a^{-1} is the inverse of a

$$(ba)a^{-1} = (ca)a^{-1}$$

$$b(aa^{-1}) = c(aa^{-1})$$

$$be = ce \quad \text{so } b = c$$

2) $a^{-1}(ab) = a^{-1}(ac)$

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

$$eb = ec \quad \text{so } b = c$$

Theorem (Uniqueness of inverse)

let G be a group. for each a in G

there is a unique b in G such that $ab = ba = e$

proof: Suppose b and c are inverses of a .

then $ab = e$ and $ac = e$

so $cab = ac$ by left cancellation $b = c$

8/30/2019.

Elementary properties of groups. cont'd.

Theorem: Let a, b be elements of a group G .

- 1) The equation $ax = b$ has unique solution $x = a^{-1}b$ in G .
- 2) The equation $xa = b$ has unique solution $x = ba^{-1}$ in G .

proof. 1) let $x = a^{-1}b$

$$\text{then } ax = a(a^{-1}b) = (aa^{-1})b = eb = b$$

Suppose $ay = b$ for some y in G .

since $ax = b$, we have $ay = ax$

by left cancellation $y = x$

2) let $x = ba^{-1}$

$$\text{then } xa = (ba^{-1})a = b(a^{-1}a) = be = b$$

if $ya = b$, then $xa = ya$

so $x = y$ by right cancellation.

Cayley tables

An operations table for a group is called a Cayley table.

$$\begin{array}{l} U_4 = \{1, -1, i, -i\} \\ i^4 = 1 \end{array}$$

	1	-1	i	-i
1	1	-1	i	-i
-1	-1	1	-i	i
i	i	-i	-1	1
-i	-i	i	1	-1

Corollary: every row and column of the Cayley table through group G contains every element of G exactly once.

proof: consider some a in G .

the row of the table corresponding to a consists of the elements ax as x ranges over G .

this row contains every b in G , because $ax = b$ has unique solution for each b , and it contains b exactly once because the solution is unique.

→ A similar argument applies to columns.

Theorem: Let G be a group and suppose that $a, b \in G$.

$$\text{then } (ab)^{-1} = b^{-1}a^{-1}$$

proof: we have that $(ab)(a^{-1}b^{-1}) = e$

$$\text{also } (ab)b^{-1}a^{-1} = a(bb^{-1})a^{-1} = aea^{-1} = aa^{-1} = e$$

$$\text{so } (ab)(a^{-1}b^{-1}) = (ab)(b^{-1}a^{-1})$$

by left cancellation,

$$(ab)^{-1} = b^{-1}a^{-1}$$

Integers modulo n

let $a, b \in \mathbb{Z}$ with $a \neq 0$. a divides b written $a|b$

if $b = ka$ for some $k \in \mathbb{Z}$.

Let $n \geq 2$ be an integer.

We say $a, b \in \mathbb{Z}$ are congruent mod n

written $a \equiv b \pmod{n}$ if n divides $a-b$

or equivalently if a and b have the same remainder

upon division by n

$$\text{ex: } 10 \equiv 4 \pmod{2} \rightarrow 10 - 4 = 6$$

$$11 \equiv 17 \pmod{2}$$

$$12 \equiv 7 \pmod{5} \rightarrow 12 - 7 = 5$$

Theorem: Congruence mod n is an equivalence relation on \mathbb{Z} .

Proof: **reflexive**: let $a \in \mathbb{Z}$.

We show $a \equiv a \pmod{n}$

$a - a = 0$ and n divides 0

$$0 = n(0), 0 \in \mathbb{Z}$$

$$\text{so } a \equiv a \pmod{n}$$

Symmetry: suppose $a \equiv b \pmod{n}$,

then n divides $a - b$

$$\text{so } a - b = nk \text{ for some } k \in \mathbb{Z}$$

$$\text{But } b - a = n(-k), -k \in \mathbb{Z}.$$

$$\text{so } n \text{ divides } b - a,$$

$$\text{therefore } b \equiv a \pmod{n}$$

transitivity: suppose $a \equiv b \pmod{n}$

and $b \equiv c \pmod{n}$

$$\text{so } a - b = nk \text{ and } b - c = nl \text{ for some } k, l \in \mathbb{Z}.$$

$$\text{then } a - c = a - b + b - c = nk + nl = n(k + l), k + l \in \mathbb{Z}.$$

$$\text{thence } a \equiv c \pmod{n}$$

Let A be a set and n an equivalence relation on A .

Given $a \in A$, the set $[a] = \{x \in A \mid x \sim a\}$

is the equivalence class of a

Equivalence classes under congruence mod 3

$$x, y \in \mathbb{Z} \quad x \equiv y \pmod{3} \text{ if } 3 \mid (x - y)$$

$$[0] = \{x \in \mathbb{Z} \mid x \equiv 0 \pmod{3}\}$$

$$= \{x \in \mathbb{Z} \mid 3 \mid (x - 0)\}$$

$$= \{x = 3k \mid k \in \mathbb{Z}\}$$

$$= \{\dots, -6, -3, 0, 3, 6, 9, \dots\}$$

$$[1] = \{x \in \mathbb{Z} \mid x \equiv 1 \pmod{3}\}$$

$$= \{x \in \mathbb{Z} \mid x - 1 = 3k, k \in \mathbb{Z}\}$$

$$= \{x \in \mathbb{Z} \mid x = 3k + 1\}$$

$$= \{\dots, -5, -2, 1, 4, 7, \dots\}$$

$$[2] = \{x \in \mathbb{Z} \mid x \equiv 2 \pmod{3}\}$$

$$= \{x \in \mathbb{Z} \mid x = 3k + 2\}$$

$$= \{\dots, -4, -1, 2, 5, 8, \dots\}$$

$$[3] = [0] = [6] = \dots$$

The distinct equivalence classes are $[0], [1], [2]$

Let n be an equivalence relation on A .

$$A/n = \{[a] \mid a \in A\} \text{ set of equivalence classes.}$$

for congruence module n . $\mathbb{Z}_n = \{[a] \mid a \in \mathbb{Z}\}$.

for the set of equivalence classes $(\mathbb{Z}/n\mathbb{Z}, \mathbb{Z}/n)$

ex: $\mathbb{Z}_3 = \{[0], [1], [2]\}^3 = \{0, 1, 2\}$

$$\mathbb{Z}_2 = \{0, 1\}$$

$$\mathbb{Z}_4 = \{0, 1, 2, 3\}$$

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

Modular Arithmetic

$$\mathbb{Z}_n = \{[0], [1], \dots, [n-1]\}$$

Define $[a] + [b] = [a+b]$

9/4/2018

$$\mathbb{Z}_n = \{[0], [1], \dots, [n-1]\}$$

Addition mod n $[a] + [b] = [a+b]$

Cayley table

$$\mathbb{Z}_4 = \{0, 1, 2, 3\}$$

$(\mathbb{Z}_4, +)$	0	1	2	3
0	0	1	2	3
1	1	2	3	0
2	2	3	0	1
3	3	0	1	2

$(\mathbb{Z}_n, +)$ is an abelian group

$$[a] + [b] = [a+b]$$

identity is $[0]$

inverse of $[a]$ is $[-a] = [n-a]$

Multiplication mod n

Let $[a], [b] \in \mathbb{Z}_n = \{[0], [1], \dots, [n-1]\}$

Define $[a] \cdot [b] = [ab]$

Consider $2 \in \mathbb{Z}_4$ under multiplication mod 4.

$$2 \cdot 0 = 0 \quad 2 \cdot 1 = 2 \quad 2 \cdot 2 = 4 = 0 \quad 2 \cdot 3 = 6 = 2$$

$$\mathbb{Z}_4 = \{0, 1, 2, 3\}$$

2 has no multiple inverse in \mathbb{Z}_4

In general, (\mathbb{Z}_n, \cdot) is a commutative monoid the operation is associative and has identity 1.

Let a, b be nonzero integers.

Let $\gcd(a, b)$ be the greatest common divisor.

If $\gcd(a, b) = 1$, then a and b are relatively prime.

Theorem: Let a and n be integers with $n \geq 2$

then a has a multiplicative inverse in \mathbb{Z}_n

iff a and n are relatively prime

$$\text{Let } \mathbb{Z}_n^* = \{a \in \mathbb{Z}_n \mid \gcd(a, n) = 1\}$$

then \mathbb{Z}_n^* is an abelian group under multiplication mod n ,

the group of units of \mathbb{Z}_n

example: $\mathbb{Z}_8^* = \{1, 3, 5, 7\}$

Cayley table

\mathbb{Z}_8^*	1	3	5	7
1	1	3	5	7
3	3	1	7	5
5	5	7	1	3
7	7	5	3	1

$$2^2=4, 2^3=8, 2^4=16=6, 2^5=32=2$$

$$\mathbb{Z}_{10}^* = \{1^2=1, 2^2=4, 3^2=9, 4^2=16=6, 5^2=25=1\}$$

$$6^2=36=6, 6^3=216=6$$

$$7^2=49, 7^3=343=3$$

$$2401=1$$

Note: $\mathbb{Z}_p^* = \mathbb{Z}_p - \{0\}$ iff p is prime

ex: $\mathbb{Z}_5^* = \{1, 2, 3, 4\}$

\mathbb{Z}_5^*	1	2	3	4
1	1	2	3	4
2	2	4	1	3
3	3	1	4	2
4	4	3	2	1

Finite Groups & subgroups

The number of elements of a group G is the order of G , denoted $|G|$.

ex: $\mathbb{Z}_{10}^* = \{1, 3, 7, 9\}$ $|Z_{10}^*| = 4$

$GL(2, \mathbb{R})$ has infinite order

the order of element g in a group

is the smallest positive integer n st $g^n = e$

(or $ng = 0$ additive notation) and denoted $|g| = n$.

If no such n exists, then g is infinite order. and $|g| = \infty$

ex: $\mathbb{Z}_8 = \{0, 1, 2, 3, 4, 5, 6, 7\}$

$$|0|=0, |1|=8, |2|=4, |3|=8, |4|=2, |5|=8, |6|=4, |7|=8$$

ex: group of units

$$\mathbb{Z}_{13} = \{1, 2, 3, \dots, 12\} \quad |8| = ?$$

$$\textcircled{1} \quad 8 \equiv -5 \pmod{13}$$

$$\textcircled{2} \quad 8^2 = 25 \equiv 12 \equiv -1$$

$$\textcircled{3} \quad 8^4 = (-1)^2 = 1$$

$$\textcircled{4} \quad 181 = 4$$

9/6/2019

3. Finite Groups, Subgroups

Subgroups: A subset H of a group G is a subgroup of G if H is itself a group with the operation in G .

We write $H \leq G$ if H is a subgroup of G .

ex: let G be a group.

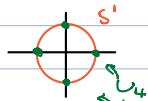
then $\{e\}$ is a subgroup of G called the trivial subgroup.

G is a subgroup of itself

If $H \leq G$ and $H \neq G$, we call H a proper subgroup.

ex: $SL(2, \mathbb{R})$ is a subgroup of $GL(2, \mathbb{R})$

$U_4 = \{1, -1, i, -i\}$ is a subgroup of $S^1 = \{z \in \mathbb{C} \mid |z|=1\}$



Theorem (subgroup test): A subset H of a group G is a subgroup

iff ① $e \in H$

② if $a, b \in H$, then $ab \in H$

③ if $a \in H$ then $a^{-1} \in H$

Proof: First, suppose 1, 2, and 3 hold.

then H is closed under binary operation (by 2)
 that has an identity (by 1)
 and every element has an inverse (by 3)
 since the operation is associative in G , it is associative in H .
 conversely if $H \subseteq G$, then 1, 2 and 3 hold.

ex: If $n \geq 0$, let $n\mathbb{Z} = \{nk \mid k \in \mathbb{Z}\}$
 then $n\mathbb{Z} \subseteq \mathbb{Z}$.

pf: the identity of \mathbb{Z} is 0,
 and $0 = n \cdot 0$ so $0 \in n\mathbb{Z}$.
 suppose $a, b \in n\mathbb{Z}$.

$a = nk, b = nl$, for some $n, l \in \mathbb{Z}$.

$a+b = nk+nl = n(k+l)$, $k+l \in \mathbb{Z}$.

therefore $a+b \in n\mathbb{Z}$

If $a \in n\mathbb{Z}$, then $a = nk$, $k \in \mathbb{Z}$

so $-a = n(-k)$, $-k \in \mathbb{Z}$

hence $-a \in n\mathbb{Z}$.

By the subgroup test, $n\mathbb{Z} \subseteq \mathbb{Z}$. \blacksquare

Definition: Let G be a group, the center of G is defined by
 $Z(G) = \{g \in G \mid zg = gz \text{ for all } g \in G\}$
 elements in $Z(G)$ are central in G .

Theorem: If G is a group, then $Z(G)$ is an abelian subgroup of G .

pf: By using the subgroup test:

$$eg = ge = g \quad \text{for all } g \in G$$

so $e \in Z(G)$

Suppose $a, b \in Z(G)$ let $g \in G$.

$$\text{then } (ab)g = a(bg) = a(gb) = (ag)b = (ga)b = g(ab)$$

therefore $ab \in Z(G)$

for $a \in Z(G)$ and $g \in G$.

then $ag = ga$.

$$a^{-1}ag = a^{-1}ga$$

$$g = a^{-1}ga$$

$$ga^{-1} = a^{-1}gaa^{-1}$$

$$ga^{-1} = a^{-1}g \quad \text{shows } a^{-1} \in Z(G)$$

By the subgroup test, $Z(G)$ is a subgroup of G .

Note: $Z(G) = G$ iff G is abelian.

9/19/2019

3 Subgroups

A subset H of a group G is a subgroup of G
 if H is a group under the operation of G .

Theorem (Subgroup Test)

A subset H of a group G is a subgroup of G

Iff 1) $e \in H$

2) if $a, b \in H$, then $a \cdot b \in H$

3) if $a \in H$, then $a^{-1} \in H$

Let G be a group

Suppose H & K are subgroup of G .

The product HK is $HK = \{hk \mid h \in H, k \in K\}$

Proposition: Suppose G is a abelian group and H & K are subgroup of G .

then the product HK is a subgroup of G .

Pf: Apply the subgroup test.

since $H, K \leq G$.

(1) then $e \in H, e \in K$.

so $e = e \cdot e \in HK$

(2) suppose $a, b \in HK$

then $a = h_1k_1, b = h_2k_2$, for some $h_1, h_2 \in H, k_1, k_2 \in K$

then $a \cdot b = (h_1k_1)(h_2k_2) = h_1h_2k_1k_2 \in HK$

(3) let $a = hk \in HK$

then $a^{-1} = (hk)^{-1} = k^{-1}h^{-1} = h^{-1}k^{-1} \in HK$

By the subgroup test, $HK \leq G$.

Theorem (Finite subgroup test)

If H is a finite nonempty subset of a group G .

then $H \leq G$. Iff H is closed.

Pf: Suppose H is closed, (if $a, b \in H$, then $a \cdot b \in H$)

Let $h \in H$, then each of $h, h^2, h^3, \dots \in H$.

Because it is finite, they are not all distinct.

so $h^n = h^{n+m}$ for some n, m .

Hence $h^n = h^n h^m$

$$e = h^m$$

so $e \in H$

Since $h^m = e$,

$$hh^{m-1} = h^{m-1}h = e$$

$$\text{so } h^{-1} = h^{m-1} \in H$$

by the subgroup test, $H \leq G$

Conversely if H is a subgroup, then H must be closed.

Ex: $\mathbb{Z}_4 = \{0, 1, 2, 3\}$ subset of \mathbb{Z}_4 : $\{0\}, \mathbb{Z}_4, \{0, 2\}$.

Theorem: Let G be a group and $a \in G$.

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

then $\langle a \rangle$ is a subgroup of G .

Pf: Apply subgroup test.

We have $e = a^0 \in \langle a \rangle$

then if $a^k \in \langle a \rangle$ and $a^m \in \langle a \rangle$

$$\text{then } a^k a^m = a^{k+m} \in \langle a \rangle$$

$$\text{if } a^k \in \langle a \rangle \text{ then } (a^k)^{-1} = a^{-k} \in \langle a \rangle$$

By the subgroup test $\langle a \rangle$ is a subgroup of G .

We call $\langle a \rangle = \{a^n \mid n \in \mathbb{Z}\}$ the cyclic subgroup of G generated by a .

and a is a generator of G .

Every cyclic group is abelian.

4. Cyclic groups

$$\mathbb{Z} = \langle 1 \rangle = \langle -1 \rangle \quad n \in \mathbb{Z}, \quad n = n \cdot 1 = (-n)(-1)$$

$$\langle 1 \rangle = \{k \cdot 1 \mid k \in \mathbb{Z}\}$$

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

$$\langle 1 \rangle = \mathbb{Z}_n \quad \langle -1 \rangle = \langle n-1 \rangle \subset \mathbb{Z}_n$$

1 and $n-1$ are generator.

9/11/2019

4 Cyclic Groups

Group G . Let $a \in G$

The subgroup

$\langle a^n \rangle = \{a^n \mid n \in \mathbb{Z}\}$ is the cyclic subgroup of G generated by a .

If $G = \langle a \rangle$ for some $a \in G$,

then G is a cyclic group and a is a generator.

$$\text{ex: } \mathbb{Z} = \langle 1 \rangle = \{1 \cdot k \mid k \in \mathbb{Z}\}$$

$$\langle -1 \rangle = \{-1 \cdot k \mid k \in \mathbb{Z}\}$$

$$\mathbb{Z}_n = \{0, 1, \dots, n-1\} = \langle 1 \rangle = \langle n-1 \rangle$$

Depending on n , there could be other.

Theorem: Let G be a group

Sps $a \in G$ with $|a| = n$

(1) $a^k = e$ iff n divides k

(2) $a^k = a^l$ iff $k \equiv l \pmod{n}$

(3) $\langle a \rangle = \{e, a, \dots, a^{n-1}\}$ and the elements e, a, \dots, a^{n-1} are distinct.

Hence $|\langle a \rangle| = n = |a|$

pf: (1) If $n \mid k$, then $k = qn, q \in \mathbb{Z}$

$$\text{Then } a^k = a^{qn} = (a^n)^q = e^q = e$$

• Conversely, if $a^k = e$

let $k = qn + r$ $0 \leq r < n$

$$\text{so } a^k = a^{qn+r} = a^q (a^n)^r = e \cdot e^r = e$$

Since $|a| = n$, $r = 0$

hence $a \mid k$

(2) $a^k = a^l$ means $a^{k-l} = e$

By (1), $n \mid k-l$

so $k \equiv l \pmod{n}$

(3) Let $x \in \langle a \rangle$, then $x = a^k$

using the division algorithm, $k = qn + r$, $0 \leq r < n$

$$\text{then } x = a^k = a^{qn+r} = (a^n)^q a^r = e^q a^r = e a^r = a^r$$

and $a^r \in \{e, a, \dots, a^{n-1}\}$

so $\langle a \rangle \subseteq \{e, a, \dots, a^{n-1}\}$

$\{e, a, \dots, a^{n-1}\} \subseteq \langle a \rangle$

hence $\langle a \rangle = \{e, a, \dots, a^{n-1}\}$

If $a^k = a^l$ for some $0 \leq k, l \leq n-1$

so $a^{k-l} = e$ where $0 \leq k-l < n$

but $|a| = n$, $k-l \geq 0$, $k = l$

thus e, a, \dots, a^{n-1} are distinct. $|\langle a \rangle| = n$

4 Cyclic Groups

group G , $a \in G$,

$$\langle a \rangle = \{a^n \mid n \in \mathbb{Z}\} = \{ \dots, a^2, a^{-1}, e, a, a^2, \dots \}$$

the cyclic subgroup generated by a .If $G = \langle a \rangle$ then G is cyclic a is a generator. \mathbb{Z} infinite cyclic Finite cyclic groups \mathbb{Z} .Theorem: Let G be a group. Let $a \in G$ with $|a| = n$.then 1) $a^k = e$ iff n divides k 2) $a^k = a^l$ iff $k \equiv l \pmod{n}$ 3) $\langle a \rangle = \{e, a, \dots, a^{n-1}\}$, e, a, \dots, a^{n-1} are distinct.So $|\langle a \rangle| = n = |a|$ Ex: $\mathbb{Z}_{19}^* = (\mathbb{Z}_{19} - \{0\}, \cdot)$ Let's show \mathbb{Z}_{19}^* is cyclic and 2 is a generator.

$$2^3 = 8, 2^6 = 2 \cdot 2^3 = 8 \cdot 8 = 64 = 7$$

$$2 \cdot 19 = 57$$

$$2^9 = 2^3 \cdot 2^6 = 8 \cdot 7 = 56 = 1$$

$$2^{18} = (-1)^2 = 1$$

if $|2| = n$, since $2^3 = 1 = e$, then n divides 18

$$n = 1, 2, 3, 6, 9, 18$$

$$2^1 = 2, 2^2 = 4, \text{ so } n = 18 \quad \text{since } 2^1, 2^2, 2^3, 2^6, 2^9 \neq 1.$$

$$\text{so since } 1 < 2 < 1 = |2| = 18$$

$$\text{and } 2^{18} = 1$$

then $\mathbb{Z}_{19}^* = \langle 2 \rangle$, therefore \mathbb{Z}_{19}^* is cyclic and 2 is a generator.Theorem: Let G be a group, and $a \in G$ with $|a| = \infty$ then 1) $a^k = e$ iff $k = 0$ 2) $a^k = a^l$ iff $k = l$ 3) $\langle a \rangle = \{ \dots, a^{-2}, a^{-1}, e, a, a^2, \dots \}$ and elements are distinct.Pf: 1) If $|a| = \infty$, then $a^k = e$ means $k = 0$.2) If $a^k = a^l$, then $a^{k-l} = e$ by 1) $k-l=0$ so $k=l$ 3) $\langle a \rangle = \{a^n \mid n \in \mathbb{Z}\} = \{ \dots, a^{-2}, a^{-1}, e, a, a^2, \dots \}$ so by 2) these elements are distinct.Theorem: Let $\langle a \rangle = \{e, a, \dots, a^{n-1}\} = G$ be a cyclic group of order n .then $G = \langle a^k \rangle$ iff $\gcd(k, n) = 1$ (k and n are relatively prime)Ex: \mathbb{Z}_6 has generators 1, 5Ex: \mathbb{Z}_9 has generators 1, 2, 4, 5, 7, 8

Theorem: (Fundamental theorem of cyclic group)

Let $G = \langle a \rangle = \{e, a, \dots, a^{n-1}\}$ be a cyclic group of order n 1) If $H \leq G$, then $|H|$ divides $|G| = n$ and $H = \langle a^d \rangle$ for some divisor d of n 2) If k divides n , then $|a^{n/k}| = k$ and $\langle a^{n/k} \rangle$ is the unique subgroup of G of order k .Def: Given $n \geq 1$, the cyclic group of order n written C_n , is the group $C_n = \{e, a, \dots, a^{n-1}\} = \langle a \rangle, a^n = 1$ we call a a generator of C_n .Since $|C_n| = n$, the elements are distinct.

Ex: Find all subgroups of C_{12}

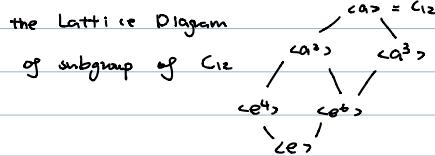
$$C_{12} = \langle a \rangle \quad |a| = 12$$

The divisors of 12 are 1, 2, 3, 4, 6, 12

The unique subgroup of each of these orders respectively,

$$\text{is } \langle e \rangle = \{e\}; \langle a^6 \rangle = \{e, a^6\}; \langle a^4 \rangle = \{e, a^4, a^8\}; \langle a^3 \rangle = \{e, a^3, a^6, a^9\};$$

$$\langle a^2 \rangle = \{e, a^2, a^4, a^6, a^8, a^{10}\}; \langle a \rangle = C_{12}$$



Corollary: Subgroups of \mathbb{Z}_n

for each positive divisor k of n

the set $\langle n/k \rangle$ is the unique subgroup of \mathbb{Z}_n of order k .

Moreover, these are the only subgroups of \mathbb{Z}_n .

Ex: \mathbb{Z}_{16} divisors of 16: 1, 2, 4, 8, 16

$$\langle 0 \rangle = \{0\}$$

$$\langle 8 \rangle = \{0, 8\}$$

$$\langle 4 \rangle = \{0, 4, 8, 12\}$$

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

$$\langle 1 \rangle = \mathbb{Z}_{16}$$

$$\langle 1 \rangle = \mathbb{Z}_{16}$$

$$\langle 2 \rangle$$

$$\langle 4 \rangle$$

$$\langle 8 \rangle$$

$$\langle 16 \rangle = \{0\}$$

9/16/2019

5. Permutation Groups

Let $n \geq 1$ be an integer

A map $\sigma: \{1, 2, \dots, n\} \rightarrow \{1, 2, \dots, n\}$ that is one to one and onto

is called a permutation

Set S $\text{perm}(S) = \{\sigma: S \rightarrow S \mid \sigma \text{ is a bijection}\}$

Notation: consider the permutation σ on $\{1, 2, 3, 4\}$ defined by $\sigma(1) = 3, \sigma(2) = 1,$

$$\sigma(3) = 4 \text{ and } \sigma(4) = 2 \text{ we write } \sigma \text{ as } \sigma = \begin{pmatrix} 1 & 2 & 3 & 4 \\ 3 & 1 & 4 & 2 \end{pmatrix}$$

A permutation is a bijection and so has an inverse

$$\sigma^{-1}(1) = 2 \quad \sigma^{-1}(2) = 4 \quad \sigma^{-1}(3) = 1 \quad \sigma^{-1}(4) = 3$$

σ^{-1} is obtained by reading the array for σ from down to up.

$$\sigma = \begin{pmatrix} 1 & 2 & 3 & 4 \\ 3 & 1 & 4 & 2 \end{pmatrix} \quad \sigma^{-1} = \begin{pmatrix} 1 & 2 & 3 & 4 \\ 2 & 4 & 1 & 3 \end{pmatrix}$$

A composition of bijections is a bijection, for permutations σ and τ on $\{1, 2, \dots, n\}$

we compute $(\sigma \tau)(k)$ ($k \in \{1, 2, \dots, n\}$ by function composition)

$$(\sigma \tau)(k) = \sigma(\tau(k)) \quad k \in \{1, 2, \dots, n\} \quad [\tau \text{ then } \sigma]$$

$$\text{ex: } \sigma = \begin{pmatrix} 1 & 2 & 3 & 4 \\ 3 & 1 & 4 & 2 \end{pmatrix} \quad \tau = \begin{pmatrix} 1 & 2 & 3 & 4 \\ 2 & 4 & 3 & 1 \end{pmatrix}$$

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

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

$$\neq \sigma \tau$$

$$\sigma = \begin{pmatrix} 1 & 2 & 3 & 4 \\ 3 & 1 & 4 & 2 \end{pmatrix} \quad \sigma^{-1} = \begin{pmatrix} 1 & 2 & 3 & 4 \\ 2 & 4 & 1 & 3 \end{pmatrix}$$

$$\sigma\sigma^{-1} = \begin{pmatrix} 1 & 2 & 3 & 4 \\ 1 & 2 & 3 & 4 \end{pmatrix} = \epsilon \text{ the identity permutation}$$

Let S_n denote the set of all permutations of $\{1, 2, \dots, n\}$

$$\text{we write } \sigma \in S_n \text{ as } \sigma = \begin{pmatrix} 1 & 2 & 3 & \dots & n \\ \sigma(1) & \sigma(2) & \sigma(3) & \dots & \sigma(n) \end{pmatrix}$$

For $\sigma \in S_n$, $\sigma(1), \sigma(2), \dots, \sigma(n)$ are all distinct

so there are n choices for $\sigma(1)$, $n-1$ choices for $\sigma(2)$...

Theorem: the set S_n of permutations of $\{1, 2, \dots, n\}$ has $n!$ elements.

ex: $S_3 \quad |S_3| = 3! = 6$

$$\epsilon = \begin{pmatrix} 1 & 2 & 3 \\ 1 & 2 & 3 \end{pmatrix} \quad \sigma = \begin{pmatrix} 1 & 2 & 3 \\ 2 & 3 & 1 \end{pmatrix} \quad \tau = \begin{pmatrix} 1 & 2 & 3 \\ 2 & 1 & 3 \end{pmatrix}$$

$$\sigma^2 = \begin{pmatrix} 1 & 2 & 3 \\ 3 & 1 & 2 \end{pmatrix} \quad \tau\sigma = \begin{pmatrix} 1 & 2 & 3 \\ 1 & 3 & 2 \end{pmatrix} \quad \tau\sigma^2 = \begin{pmatrix} 1 & 2 & 3 \\ 3 & 2 & 1 \end{pmatrix}$$

Theorem: S_n is a group, called the symmetric group of degree n .

pf: For $\sigma, \tau \in S_n$, the composition $\sigma\tau \in S_n$

for the identity permutation ϵ , $\sigma\epsilon = \epsilon\sigma = \sigma$.

function composition is associative: $(\sigma\tau)\mu = \sigma(\tau\mu)$

for the inverse permutation σ^{-1} , $\sigma^{-1}\sigma = \sigma\sigma^{-1} = \epsilon$

Cycle notation:

$$\tau = \begin{pmatrix} 1 & 2 & 3 & 4 & 5 & 6 & 7 \\ 4 & 7 & 1 & 6 & 5 & 2 & 3 \end{pmatrix} \quad \text{In cycle notation: } \tau = (1 4 6 2 7 3)(5)$$

Note: τ fixes 5, the length of τ is 6.

$$\tau^{-1} = \begin{pmatrix} 1 & 2 & 3 & 4 & 5 & 6 & 7 \\ 3 & 6 & 7 & 1 & 5 & 4 & 2 \end{pmatrix} \quad \tau^{-1} = (1 3 7 2 6 4) = (3 7 2 6 4 1)$$

Some permutations are products of several cycles.

$$\text{ex: } \sigma = \begin{pmatrix} 1 & 2 & 3 & 4 & 5 & 6 & 7 & 8 & 9 & 10 \\ 3 & 1 & 7 & 6 & 10 & 4 & 2 & 5 & 9 & 8 \end{pmatrix} \quad \sigma \in S_{10}$$

$$\sigma = (1 3 7 2)(4 6)(5 10 8)(9)$$

Note: we have expressed σ as a product of disjoint cycles.

$$\text{ex: } \sigma = \begin{pmatrix} 1 & 2 & 3 & 4 & 5 & 6 & 7 & 8 \\ 3 & 7 & 1 & 5 & 6 & 4 & 2 & 8 \end{pmatrix} \quad \tau = \begin{pmatrix} 1 & 2 & 3 & 4 & 5 & 6 & 7 & 8 \\ 2 & 3 & 7 & 8 & 5 & 4 & 1 & 6 \end{pmatrix}$$

$$\sigma\tau = \begin{pmatrix} 1 & 2 & 3 & 4 & 5 & 6 & 7 & 8 \\ 7 & 1 & 2 & 8 & 6 & 5 & 3 & 4 \end{pmatrix} \quad \sigma\tau = (1 7 3 2)(4 8)(5 6)$$

$$\sigma = (1 3)(2 7)(4 5 6)(8) \quad \tau = (1 2 3 7)(4 8 6)(5)$$

$$\sigma\tau =$$

9/18/19

Recall that a permutation σ is a one to one and onto function.

$$\sigma: \{1, 2, \dots, n\} \rightarrow \{1, 2, \dots, n\}$$

$$\sigma = \begin{pmatrix} 1 & 2 & \dots & n \\ \sigma(1) & \sigma(2) & & \sigma(n) \end{pmatrix}$$

Let S_n be the set of permutations $\sigma: \{1, 2, \dots, n\} \rightarrow \{1, 2, \dots, n\}$

then S_n is a group of order $n!$ called the symmetric group of degree n .

$$\text{ex: } \sigma = \begin{pmatrix} 1 & 2 & 3 & 4 & 5 & 6 & 7 & 8 \\ 3 & 7 & 1 & 5 & 6 & 4 & 2 & 8 \end{pmatrix} \quad \tau = \begin{pmatrix} 1 & 2 & 3 & 4 & 5 & 6 & 7 & 8 \\ 2 & 3 & 7 & 8 & 5 & 4 & 1 & 6 \end{pmatrix}$$

$$\sigma\tau = \begin{pmatrix} 1 & 2 & 3 & 4 & 5 & 6 & 7 & 8 \\ 7 & 1 & 2 & 8 & 6 & 5 & 3 & 4 \end{pmatrix} \quad \sigma\tau = (1 \ 7 \ 3 \ 2)(4 \ 8)(5 \ 6)$$

$$\sigma = (1 \ 3)(2 \ 7)(4 \ 5 \ 6)(8) \quad \tau = (1 \ 2 \ 3 \ 7)(4 \ 8 \ 6)(5)$$

$\sigma\tau$ is function composition (right to left)

$$\sigma\tau = (1 \ 3)(2 \ 7)(4 \ 5 \ 6)(1 \ 2 \ 3 \ 7)(4 \ 8) \quad \leftarrow \text{cycle notation.}$$

$$= (1 \ 7 \ 3 \ 2)(4 \ 8)(5 \ 6) \quad \leftarrow \text{product of disjoint cycles.}$$

Properties

Theorem: every permutation can be written as a cycle or as a product of disjoint cycles.

Pf: Let $X = \{1, 2, \dots, n\}$ σ a permutation on X

Let $i \in X$. Consider $i, \sigma(i), \sigma^2(i), \dots$

because X is finite, eventually $\sigma^m(i) = i$ for some m

$$\sigma = (i \ \sigma(i) \ \dots \ \sigma^{m-1}(i))$$

Next, choose some $j \in X$ not appearing in the first cycle. (if there is no such j , we're done)

Look at $j \ \sigma(j) \ \sigma^2(j) \dots$

There is some r such that $\sigma^r(j) = j$

then $(j \ \sigma(j) \ \dots \ \sigma^{m-1}(j))$ which will be disjoint from the previous cycle. until the

elements of X are exhausted, we express σ as a product of disjoint cycles.

$$\sigma = (i_1, \sigma(i_1), \sigma^2(i_1) \dots \sigma^{m-1}(i_1))(j_1, \sigma(j_1), \dots, \sigma^{n-m}(j_1)) \dots (k_1, \dots, \sigma^{s-1}(k_1))$$

Theorem: Disjoint cycles commute.

If the cycles $\sigma = (a_1, a_2, \dots, a_m)$ $\tau = (b_1, b_2, \dots, b_n)$

have no entries in common, then $\sigma\tau = \tau\sigma$

$$\text{idea: } (\sigma\tau)(a_i) = \sigma(\tau(a_i)) = \sigma(a_i) = \begin{cases} a_{i+1} & i \neq m \\ a_1 & i = m \end{cases}$$

$$(\tau\sigma)(a_i) = \tau(\sigma(a_i)) = \begin{cases} \tau(a_{i+1}) = a_{i+1} & i \neq m \\ \tau(a_1) = a_1 & i = m \end{cases}$$

similarly for b_1, \dots, b_n and any a_i fixed by both τ & σ .

9/20/19

Thm: the order of a permutation written as a product of disjoint cycles is least common multiple of the lengths of the cycles.

$$\sigma = (a_1, a_2, \dots, a_m) \quad \text{length } m$$

$$\sigma\tau = (a_1, a_2, \dots, a_m)(b_1, b_2, \dots, b_n) \quad |\sigma| = m \quad |\tau| = n \quad \sigma, \tau \text{ disjoint}$$

$$\text{ex: } \sigma = \begin{pmatrix} 1 & 2 & 3 & 4 & 5 & 6 & 7 & 8 \\ 3 & 1 & 2 & 8 & 7 & 4 & 5 & 6 \end{pmatrix} \in S_8$$

$$\sigma = (1 \ 3 \ 2)(4 \ 8 \ 6)(5 \ 7) \quad |\sigma| = \text{lcm}(2, 3) = 6$$

A 2-cycle is a transposition

Thm: every cycle of length > 1 is a product of $k-1$ transpositions.

Hence every permutation is a product of transpositions.

$$(a_1, a_2, \dots, a_r) = (a_1, a_r)(a_1, a_{r-1}) \dots (a_1, a_3)(a_1, a_2)$$

$$\text{ex: } \sigma = (1 \ 2 \ 3 \ 4 \ 5) = (1 \ 5)(1 \ 4)(1 \ 3)(1 \ 2) \quad |\sigma| = 5$$

σ is expressed as an even number of transpositions. σ is an even permutation.

$$\text{ex: } \pi = \begin{pmatrix} 1 & 2 & 3 & 4 & 5 & 6 & 7 & 8 & 9 \\ 2 & 8 & 6 & 9 & 4 & 7 & 3 & 1 & 5 \end{pmatrix} = (1\ 2\ 8)(3\ 6\ 7)(4\ 9\ 5) \quad |A_3| = 3$$

$$= (1\ 8)(1\ 2)(3\ 7)(3\ 6)(4\ 5)(4\ 9)$$

$$= (4\ 5)(4\ 9)(3\ 7)(3\ 6)(1\ 8)(1\ 2)$$

even # of transp. $\Rightarrow \pi$ is even

parity: we say a transposition is even if it can be expressed as an even number of transpositions. It is odd if it can be expressed as an odd number of transpositions.

$$\text{ex: } S_5 \quad |S_5| = 5! = 120$$

let n denote a cycle of length n , possible disjoint cycle structures in S_n

(5) order 5

(4)(1) order 4

(3)(2) order $\text{lcm}(2, 3) = 6$

(2)(2)(1) order 2

(3)(1)(1) order 2

(1)(1)(1)(1)(1) order 1

An element of maximal order in S_5 is $(1\ 2\ 3)(4\ 5)$

9/20/2019

5. Permutation Groups.

A transposition is a 2-cycle $(1\ 4)$

Every permutation can be written as a product of transpositions

A permutation is even if it can be written as an even number of transpositions, otherwise, it is odd.

$$\text{Identity permutation. } \epsilon \in S_4. \quad \epsilon = \begin{pmatrix} 1 & 2 & 3 & 4 \end{pmatrix} = (1\ 2)(2\ 1)(3\ 2)(3\ 1)(4\ 1)(4\ 2)$$

$$= (1\ 2)(2\ 1)$$

Lemma: the identity permutation ϵ , can only be expressed as an even number of transpositions.

If $\epsilon = s_1 s_2 \dots s_r$ where s_1, s_2, \dots, s_r are transpositions, then r is even

The set of even permutations in S_n , is a subgroup denoted A_n , called the alternating group of degree n

Theorem. A_n is a subgroup of S_n of order $|A_n| = \frac{n!}{2}$

pf. ϵ is even, so $\epsilon \in A_n$

If $\sigma = s_1 \dots s_m$ and $\tau = r_1 \dots r_n$ where s_i and r_j are transpositions with m, n even,

then $\sigma\tau = s_1 \dots s_m r_1 \dots r_n$ with $m+n$ even. So $\sigma\tau \in A_n$

For any transposition, s , $s^{-1} = s$

$$\text{ex: } (1\ 3)^{-1} = (3\ 1) = (1\ 3)$$

So for $\sigma = s_1 \dots s_m \in A_n$, $\sigma^{-1} = s_m \dots s_1 \in A_n$.

By the subgroup test, $A_n \subseteq S_n$

For every odd permutation in S_n , there is an even permutation, and vice versa.

so since $|S_n| = n!$ we have $|A_n| = \frac{n!}{2}$.

6. Isomorphisms.

Fourth roots of unity.

$$\omega_4 = \epsilon_1, -1, i, -i^3 = \epsilon_1, i, i^2, i^3 = \langle i \rangle \text{ is cyclic generated by } i.$$

Group of units $\mathbb{Z}_5^* = \{1, 2, 3, 4\} = \{1, 2, 2^2, 2^3\} = \{1, 2, 4, 3\}$

Both \mathbb{U}_4 and \mathbb{Z}_5^* have the same Cayley table.

Both have the same structure as $\langle 4 : \langle a \rangle = \{e, a, a^2, a^3\}$

We say \mathbb{U}_4 and \mathbb{Z}_5^* are isomorphic.

Definition: Let G_1 and G_2 be groups. A map $\varphi: G_1 \rightarrow G_2$ is an isomorphism

if (1) φ is one to one [injective].

If $\varphi(a) = \varphi(b)$ then $a = b$.

(2) φ is onto

for every $y \in G_2$, there is some $x \in G_1$ such that $\varphi(x) = y$

(3) φ is operation preserving: $\varphi(a \cdot b) = \varphi(a) \varphi(b)$ for all $a, b \in G_1$.

Define: $\varphi: \mathbb{U}_4 \rightarrow \mathbb{Z}_5^*$ by $\varphi(i^k) = 2^k$

then if $\varphi(i^k) = \varphi(i^l)$ then $2^k = 2^l$ so $k = l$

hence $i^k = i^l$, so φ is one to one

let $2^k \in \mathbb{Z}_5^*$, then $\varphi(i^k) = 2^k$

so φ is onto

$\varphi(i^{k+l}) = \varphi(i^{k+1}) = 2^{k+1} = 2^k \cdot 2^1 = \varphi(i^k) \varphi(i^1)$

So $\varphi: \mathbb{U}_4 \rightarrow \mathbb{Z}_5^*$ is an isomorphism.

Proposition: Sps $G = \langle a \rangle$ is a cyclic group

(1) If $|G| = n$, then $G \cong \mathbb{Z}_n$

(2) If $|G| = \infty$, then $G \cong \mathbb{Z}$

Pf: For (1) sps $|a| = |a| = n$

define $\varphi: \mathbb{Z}_n \rightarrow G$ by $\varphi([k]) = a^k$

φ is one to one.

If $\varphi([k]) = \varphi([l])$, then $a^k = a^l$. so $k \equiv l \pmod{n}$

therefore $[k] = [l]$

φ is onto let $a^k = \langle a \rangle$

let $k \equiv l \pmod{n}$ then $\varphi([k]) + [l] = a^k + a^l = a^{k+l} = a^k a^l = \varphi([k]) \varphi([l])$

φ is operation preserving: $\varphi([k]) + [l] = \varphi([k+l]) = a^{k+l} = a^k a^l = \varphi([k]) \varphi([l])$

thus $\varphi: \mathbb{Z}_n \rightarrow G$ is an isomorphism. ■

Note: $\varphi: G \rightarrow G_1$ is operation preserving if $\varphi(a \cdot b) = \varphi(a) \varphi(b)$ $\forall a, b \in G$

A structure property of a group is a property depending only on the Cayley table

An isomorphism between two groups preserving all structural properties.

Properties of Isomorphisms:

Theorem: Sps $\varphi: G_1 \xrightarrow{\cong} G_2$,

then (1) $\varphi(e_{G_1}) = e_{G_2}$

(2) $\varphi(a^n) = [\varphi(a)]^n \quad \forall a \in G_1 \neq \{e\}$

(3) $ab = ba$ iff $\varphi(a)\varphi(b) = \varphi(b)\varphi(a)$

(4) $G = \langle a \rangle$ iff $G_1 = \langle \varphi(a) \rangle$

(5) $|a| = |\varphi(a)|$

(6) $x^k = b$ has the same number of solutions in G_1

as $x^k = \varphi(b)$ in G_2 .

(7) If G is finite, G_1 and G_2 have exactly the same number of elements of every order.

6 Isomorphisms

Let G and G_1 be groups. A map $\varphi: G \rightarrow G_1$ is an isomorphism if

- (1) φ is one to one: $\forall a, b \in G$, if $\varphi(a) = \varphi(b)$ then $a = b$
- (2) φ is onto: $\forall y \in G_1$, there is some $x \in G$ st $\varphi(x) = y$
- (3) φ is operation preserving: $\varphi(a \cdot b) = \varphi(a) \varphi(b)$ OR $\varphi(a+b) = \varphi(a) + \varphi(b)$ OR $\varphi(a \cdot b) = \varphi(a) + \varphi(b) \quad \forall a, b \in G$

If $\varphi: G \rightarrow G_1$ is isomorphism, we say G and G_1 are isomorphic write $G \cong G_1$.

proposition: Let G be a group. If G is infinite cyclic, then $G \cong \mathbb{Z}$

pf: G is infinite cyclic. so $G = \langle a \rangle = \{a^n \mid n \in \mathbb{Z}\}$ for some $a \in G$

define $\varphi: G \rightarrow \mathbb{Z}$ by $\varphi(a^n) = n$

- φ is one to one: sps $\varphi(a^n) = \varphi(a^m)$ then $n = m$ so $a^n = a^m$ φ is injective.
- φ is onto: let $n \in \mathbb{Z}$ then $\varphi(a^n) = n$, so φ is surjective.
- φ is operation preserving: let $a^n, a^m \in G$, then $\varphi(a^n a^m) = \varphi(a^{n+m}) = n+m = \varphi(a^n) + \varphi(a^m)$
hence φ is isomorphism.

Isomorphic groups share all the same structural properties.

ex: Consider \mathbb{Z}_{12} and A_4 (Alternating group of degree 4)

$$|\mathbb{Z}_{12}| = 12, |A_4| = 4! / 2 = 12$$

\mathbb{Z}_{12} contains elements of order 12. (any generator of order 12, e.g. 1)

$A_4 \leq S_4$ (symmetric group) The maximum order of an element in S_4 is 4.

S_4 contains no elements of order 12. A_4 has no ele of order 12.

Therefore $\mathbb{Z}_{12} \not\cong A_4$, or A_4 is nonabelian but \mathbb{Z}_{12} is abelian.

Theorem: sps $\varphi: G \xrightarrow{\cong} G_1$

then (1) $\varphi^{-1}: G_1 \xrightarrow{\cong} G$

(2) G is abelian iff G_1 is abelian.

(3) G is cyclic iff G_1 is cyclic

(4) If $K \subseteq G$, then $\varphi(K) = \{\varphi(g) \mid g \in K\}$ is a subgroup of G_1 .

(5) If $H \subseteq G_1$, then $\varphi^{-1}(H) = \{g \in G \mid \varphi(g) \in H\}$ is a subgroup of G .

(6) $\varphi(\text{Z}(G)) = \text{Z}(G_1)$

Theorem: Let G, G_1, G_2 be groups.

(1) the identity map $\text{id}_G: G \rightarrow G$ is an isomorphism.

(2) If $\varphi: G \xrightarrow{\cong} G_1$, then $\varphi^{-1}: G_1 \xrightarrow{\cong} G$

(3) If $\varphi: G \xrightarrow{\cong} G_1$, and $\psi: G_1 \xrightarrow{\cong} G_2$, then $(\psi \circ \varphi): G \rightarrow G_2$ is an isomorphism.

Corollary: \cong is an equivalence relation on groups.

10/4/19.

Exam 1

$$(1) \text{ a) } \mathbb{Z}_{10} = \langle 1, 3, 7, 9 \rangle$$

$$1+3 = 1+7 = 4 \quad 1+9 = 2$$

$$\text{b) yes, } 3 \text{ & } 7 \text{ are generators. } \mathbb{Z}_{10} = \langle 3 \rangle = \langle 7 \rangle$$

$$\text{c) } \mathbb{Z}_{10} = \langle 3 \rangle = \langle 7 \rangle \quad \mathbb{Z}_{10} = \langle 3 \rangle \\ \langle 9 \rangle = \langle 1, 9 \rangle \quad \langle 7 \rangle \\ \langle 1 \rangle$$

$$(2) H = \left\{ \begin{pmatrix} a & b \\ 0 & c \end{pmatrix} : a, b, c \in \mathbb{R}, a \neq 0, c \neq 0 \right\}$$

$$\left(\begin{pmatrix} a & b \\ 0 & c \end{pmatrix} \right)^{-1} = \frac{1}{c} \begin{pmatrix} c & -b \\ 0 & a \end{pmatrix} = \left(\frac{1}{a} \begin{pmatrix} 0 & -b \\ 0 & 1 \end{pmatrix} \right)$$

$$(\alpha \ 0) \cdot (\bar{\alpha} \ 0) = (0 \ 1)$$

$$Z(H) = \{ z \in H \mid zh = hz \quad \forall h \in H\}$$

$$Z(H) = \left\{ \begin{pmatrix} a & b \\ 0 & c \end{pmatrix} \mid a \neq 0 \right\}$$

$$\begin{pmatrix} a & b \\ 0 & c \end{pmatrix} \begin{pmatrix} 1 & 1 \\ 0 & 1 \end{pmatrix} = \begin{pmatrix} 1 & 1 \\ 0 & 1 \end{pmatrix} \begin{pmatrix} a & b \\ 0 & c \end{pmatrix}$$

$$\begin{pmatrix} a & a+b \\ 0 & c \end{pmatrix} = \begin{pmatrix} a & b+c \\ 0 & c \end{pmatrix} \quad \begin{array}{l} a+b=b+c \\ a=c \end{array}$$

$$\begin{pmatrix} a & b \\ 0 & a \end{pmatrix} \quad a \neq 0$$

$$\begin{pmatrix} a & b \\ 0 & c \end{pmatrix} \begin{pmatrix} x & y \\ 0 & z \end{pmatrix} = \begin{pmatrix} x & y \\ 0 & z \end{pmatrix} \begin{pmatrix} a & b \\ 0 & c \end{pmatrix}$$

$$\begin{pmatrix} ax & ay+bz \\ 0 & az \end{pmatrix} = \begin{pmatrix} ax & bx+ay \\ 0 & az \end{pmatrix} \quad \begin{array}{l} bz = bx \\ \text{if } x \neq 0 \\ b = 0 \end{array}$$

$$Z(H) = \left\{ \begin{pmatrix} a & 0 \\ 0 & a \end{pmatrix} \mid a \neq 0 \right\}$$

3)

$$4) |S_3| = 3 \quad \sigma^3 = e$$

$$|I_2| = 2 \quad \tau^2 = e \quad (12)(12) = (1)(2)$$

$$5) S_3 = \{e, \sigma, \sigma^2, \tau, \tau\sigma, \tau\sigma^2\} \quad |S_3| = 6$$

$$\sigma = (123) \quad \sigma^2 = (231) \quad \tau = (12) \quad \tau^2 = \dots$$

these are the all six distinct element in S_3 .

$$c) S_3 \in \sigma \sigma^2 \tau \tau\sigma \tau\sigma^2$$

$$e \quad e \quad \sigma \quad \sigma^2 \quad \tau \quad \tau\sigma \quad \tau\sigma^2 \quad \sigma\tau = \tau\sigma^2$$

$$\sigma \quad \sigma \quad \sigma^2 \quad e \quad \tau^2 \quad \tau^2\sigma \quad \tau^2\sigma^2 \quad \sigma\sigma = \tau\sigma^3$$

$$\sigma^2 \quad \sigma^2 \quad e \quad \sigma \quad \tau \quad \tau^2\sigma \quad \tau^2\sigma^2 \quad \tau = \sigma\tau\sigma$$

$$\tau\sigma \quad \tau\sigma^2$$

$$\tau\sigma^2 \quad \tau\sigma$$

$$d) \text{ No. } \sigma\tau \neq \tau\sigma \quad \sigma\tau = \tau\sigma^2$$

$$5) a) 12$$

$$b) (1234)(567)$$

$$= \left[\frac{7 \times 6 \times 5 \times 4}{4} \right] \cdot \left[\frac{3 \times 2 \times 1}{3} \right] = 7 \times 6 \times 5 \times 2 = 420$$

$$c) \delta = (123456)$$

length 6. written as 5 transpositions.

$\Rightarrow \delta$ is odd

3 cycle (1 2 3) length 3 \Rightarrow it is even. 2 transpositions.

any product of 3 cycles are even. but δ is odd, so δ is not a product of 3 cycles.

Isomorphism.

$\varphi: G \xrightarrow{\cong} G$, φ is bijective $\varphi(g_1g_2) = \varphi(g_1)\varphi(g_2)$ $\forall g_1, g_2 \in G$

An automorphism of a group G is an isomorphism $\varphi: G \rightarrow G$

$\text{Aut}(G) = \{ \varphi: G \rightarrow G \mid \varphi \text{ is an isomorphism} \}$

$\text{Aut}(G)$ is a group. identity $\text{id}_G: G \xrightarrow{\cong} G$

$\varphi \circ \text{id}_G = \text{id}_G \circ \varphi = \varphi$ for any $\varphi \in \text{Aut}(G)$

$\varphi, \psi, \gamma \in \text{Aut}(G)$

$\varphi \circ (\gamma \circ \psi) = (\varphi \circ \gamma) \circ \psi$

$\text{Aut}(G)$ is a group under function composition.

proposition: let G be a group, and $a \in G$

then $\varphi_a: G \rightarrow G$ by $\varphi_a(x) = axa^{-1}$ is an $\text{Aut}(G)$

and $\{\varphi_a \mid a \in G\}$ is a subgroup of $\text{Aut}(G)$

pf: φ_a is an isomorphism

• $\varphi_a(x) = \varphi_a(y)$ then $axa^{-1} = ay a^{-1}$

$$a^2a \times a^{-1}a = a^{-1}a \times y \times a^{-1}a$$

$$x = y \quad \varphi_a \text{ is 1-1}$$

• let $y \in G$. then $\varphi_a(a^{-1}ya) = a^{-1}ya \times a^{-1} = y$ φ_a is onto.

$$\varphi_a(xy) = axya^{-1} = axa^{-1}aya^{-1} = \varphi_a(x)\varphi_a(y)$$

\Rightarrow So φ_a is an isomorphism.

$$\{\varphi_a \mid a \in G\} \subseteq \text{Aut}(G)$$

$$\varphi_a(x) = aea^{-1} = x = \text{id}(x)$$

$$\therefore \text{id } G \subseteq \{\varphi_a \mid a \in G\}$$

• closed. if $\varphi_a, \varphi_b \in \{\varphi_a \mid a \in G\}$

$$\varphi_a \varphi_b(x) = a[\varphi_b(x)]a^{-1} = a[b \times b]a^{-1} = ab \times (ab)^{-1} = \varphi_{ab}(x)$$

$$(\varphi_a)^{-1} = \varphi_{a^{-1}}$$

$$\varphi_a \varphi_{a^{-1}}(x) = a[\varphi_{a^{-1}}(x)]a^{-1} = a a^{-1} \times a a^{-1} = x = \text{id}(x)$$

10/7/2019

Isomorphism $\varphi: G \rightarrow G$, one to one, onto, and $\varphi(ab) = \varphi(a)\varphi(b)$ $\forall a, b \in G$

An isomorphism $\varphi: G \rightarrow G$ is an antiautomorphism of G .

$\text{Aut}(G) = \{ \varphi: G \rightarrow G \mid \varphi \text{ is an isomorphism} \}$

is a group under function composition, called automorphism group of G .

Group G let $a \in G$. Define $\varphi_a: G \rightarrow G$ by $\varphi_a(x) = axa^{-1}$

φ_a is an automorphism of G called the inner automorphism of G induced by a .

$$\text{Inn}(G) = \{ \varphi_a: G \rightarrow G \mid a \in G \}$$

Theorem: $\text{Aut}(G)$ is a group and $\text{Inn}(G)$ is a subgroup

Theorem: If $G \cong G'$, then $\text{Aut}(G) \cong \text{Aut}(G')$

pf: Suppose $\varphi: G \xrightarrow{\cong} G'$, Define a map $\theta: \text{Aut}(G) \rightarrow \text{Aut}(G')$ by $\theta(\varphi) = \varphi^{-1}\varphi$

$$(G \xrightarrow{\cong} G') \rightarrow (G, \xrightarrow{\cong} G, \xrightarrow{\cong} G, \xrightarrow{\cong} G')$$

$$\text{if } \theta(\varphi_1) = \theta(\varphi_2) \text{ then } \varphi_1^{-1}\varphi_1 = \varphi_2^{-1}\varphi_2$$

$$\varphi_1 = \varphi_2 \quad \bullet \text{ 1-1}$$

Given $\gamma \in \text{Aut}(G)$, then $\varphi^{-1}\gamma\varphi \in \text{Aut}(G)$

$$\theta(\varphi^{-1}\gamma\varphi) = \varphi\varphi^{-1}\gamma\varphi\varphi^{-1} = \gamma$$

$$\text{and } \theta(\varphi_1\varphi_2) = \varphi_1\varphi_1^{-1}\varphi_2\varphi_2^{-1} = \theta(\varphi_1)\theta(\varphi_2)$$

ex: $\text{Aut}(\mathbb{Z}_8)$, $\mathbb{Z}_8 \cong \mathbb{C}_1$

If $\alpha: \mathbb{Z}_8 \rightarrow \mathbb{Z}_8$ is an isomorphism.

then $\langle \alpha(1) \rangle = \mathbb{Z}_8$, $\alpha(1)$ must be a generator of \mathbb{Z}_8 .

Generators of \mathbb{Z}_8 are 1, 3, 5, 7, $\mathbb{Z}_8^* \subset \{1, 3, 5, 7\}$, there are 4 automorphisms.

$$\alpha_1(1) = 1 \quad \alpha_3(1) = 3 \quad \alpha_5(1) = 5 \quad \alpha_7(1) = 7$$

Define $\Theta: \mathbb{Z}_8^* \rightarrow \text{Aut}(\mathbb{Z}_8)$ by $\Theta(m) = \alpha_m$

then Θ is an isomorphism, therefore $\text{Aut}(\mathbb{Z}_8) \cong \mathbb{Z}_8^*$

Theorem: $\text{Aut}(\mathbb{Z}_n) = \mathbb{Z}_n^*$

ex: $G = \langle a \rangle$, $|G| = 10$

then $G \cong \mathbb{Z}_{10}$, therefore $\text{Aut}(G) \cong \text{Aut}(\mathbb{Z}_{10}) \cong \mathbb{Z}_{10}^*$

Theorem: (Cayley's Theorem): every group of order n is isomorphic to a subgroup of S_n .

b/c $|G| = n$. S_n = permutations of G

S_n = permutations of $\{1, 2, \dots, n\}$

Given a G $\tau_a: G \rightarrow S_n$ by $\tau_a(g) = ag$

τ_a is an element of S_n

let $G_1 = \{\tau_a \mid a \in G\}$ then $G_1 \cong G$,

and G_1 is a subgroup of $S_n \cong S_n$

7. Cosets and Lagrange's theorem

$a, b \in \mathbb{Z}$ $a \equiv b \pmod{n}$ iff $n|(a-b)$ equivalence relationship on \mathbb{Z} .

let $n\mathbb{Z} = \{nk \mid k \in \mathbb{Z}\}$ is a subgroup of \mathbb{Z} .

$a \equiv b \pmod{n}$ iff $a-b \in n\mathbb{Z}$.

Lemma: let H be a subgroup of G , for $a, b \in G$, define $a \equiv b$ iff $ab^{-1} \in H$

(1) This is an equivalence relationship.

(2) the equivalence class of a in G is $Ha = \{fha \mid f \in H\}$

$$\begin{aligned} \text{for } 2) [a] &= \{g \in G \mid g \equiv a\} = \{g \in G \mid g^{-1} \in Ha = \{f \in H \mid fa^{-1} = f\} \text{ for some } f \in H\} \\ &= \{g \in G \mid g = ha, h \in H\} = Ha \end{aligned}$$

Definition: Let H be a subgroup of G

$Ha = \{ha \mid h \in H\}$ is the right coset of H in G generated by a .

$aH = \{ah \mid h \in H\}$ is the left coset of H in G generated by a .

$$(1) He = H = eH$$

$$(2) a \in Ha \text{ and } a \in aH$$

(3) if G is abelian then $aH = Ha$ \forall subgroups H and $a \in G$.

10/9/2019

7. Cosets and Lagrange's theorem

Group G, H a subgroup of G

say for $a, b \in G$

$$a \equiv b \iff ab^{-1} \in H$$

this is an equivalence relationship on G .

for $a \in G$, the equivalence class of a

$$[a] = \{g \in G \mid g \equiv a\}$$

$$= Ha = \{ha \mid h \in H\}$$

$H_a = \{ha \mid h \in H\}$ right coset

$aH = \{ah \mid h \in H\}$ left coset

In an abelian group $Ha = aH$

ex: \mathbb{Z}_{10} divisors of 10: 1, 2, 5, 10

$$\begin{array}{l} \text{2} \rightarrow \text{2+2} \rightarrow \text{2+2+2} \rightarrow \text{2+2+2+2} \\ \text{2+2+2+2+2} \end{array} \quad \bullet \text{ Let } H = \langle 2 \rangle = \{0, 2, 4, 6, 8\} \quad |H| = 5 \quad 2 \text{ cosets.} \quad |G:H| = 2$$

$$\begin{aligned} \text{cosets: } H &= 2+H = 4+H \\ 1+H &= \{1, 3, 5, 7, 9\} = H+1 \\ &= 3+H = 5+H \end{aligned}$$

Distinct cosets: $H, 1+H, 3+H$.

$$\bullet \text{ Let } K = \langle 5 \rangle = \{0, 5\}$$

$$1+K = K+1 = \{1, 6\} \quad 3+K = K+3 = \{3, 8\}$$

$$2+K = K+2 = \{2, 7\} \quad 4+K = K+4 = \{4, 9\}$$

Cosets of K in \mathbb{Z}_{10} are $K, 1+K, 2+K, 3+K, 4+K$.

Index: If $H \leq G$, the number of distinct cosets is called the index.

written $|G:H|$

Klein Group $K_4 = \{e, a, b, c\}$

$$a^2 = b^2 = c^2 = e \quad ab = ba = c, ac = ca = b, bc = cb = a$$

Fact: Every group of order 4, is either cyclic or isomorphic to K_4 .

Lemma: Let $H \leq G$. Then $|H| = |Ha| = |aH| \quad \forall a \in G$.

Pf: Define $\sigma: H \rightarrow Ha$ by $\sigma(h) = ha$ or is bijection.

so $|H| = |Ha|$

Similarly $|H| = |aH|$

Fact: Group G , $H \leq G$, the distinct cosets of H are a partition of G .

Lagrange's theorem: Let H be a subgroup of G . then $|H|$ divides $|G|$

Pf: let $H_{a_1}, H_{a_2}, \dots, H_{a_k}$ be distinct cosets of H .

G is the disjoint union $G = H_{a_1} \cup H_{a_2} \cup \dots \cup H_{a_k}$

then $|G| = |H_{a_1}| + |H_{a_2}| + \dots + |H_{a_k}|$

$$|G| = \underbrace{|H| + |H| + \dots + |H|}_k = k|H| \quad \text{so } |H| \mid |G|$$

Corollary: $|G| = |G:H| |H|$

10/11/2019

Lagrange's theorem:

Let G be a finite group. If $H \leq G$, then the order of H divides the order of G .

index $|G:H| = \text{number of cosets of } H$

corollary $|G| = |H| |G:H|$

Corollary: Let G be a finite group, and $g \in G$.

then $|g|$ divides $|G|$

Pf: $\langle g \rangle = \{e, g, g^2, \dots\}$ is a subgroup of G

by Lagrange's theorem $|\langle g \rangle|$ divides $|G|$

since $|\langle g \rangle| = |\langle g^2 \rangle|$, then $|g|$ divides $|G|$

corollary: let $|G| = n$

then $g^n = e$ for all $g \in G$.

pf: let $|g| = k$

since $|g| | |G| \Rightarrow |g| | n$

we have $n = kl$ for some $l \in \mathbb{Z}$.

then $g^n = (g^k)^l = e^l = e$

corollary: if p is prime, then every group G of order p is cyclic.

so $G = \langle g \rangle$ for every $g \neq e$ in G .

so only subgroups of G are G and $\{e\}$

pf: let $g \in G$, $g \neq e$

then $|\langle g \rangle| \mid p$ by the lagrange's theorem.

so $|\langle g \rangle| = p$ hence $G = \langle g \rangle$

corollary: let H and K be finite subgroup of G .

If $|H|$ and $|K|$ are relatively prime.

then $H \cap K = \{e\}$

b/c $H \cap K \leq H \nsubseteq H \cap K \leq K$.

If $|H|$ & $|K|$ are relatively prime. then $|H \cap K| = 1$

8 Direct products.

Set G_1, G_2, \dots, G_n .

Cartesian product $G_1 \times G_2 \times \dots \times G_n = \{(g_1, g_2, \dots, g_n) \mid g_i \in G_i \text{ for } i=1, \dots, n\}$

$X \times Y = \{(x, y) \mid x \in X, y \in Y\}$

Defn: If G_1, G_2, \dots, G_n are groups.

their direct product is the set $G_1 \times G_2 \times \dots \times G_n$

with componentwise operation:

$$(g_1, g_2, \dots, g_n) \cdot (g'_1, g'_2, \dots, g'_n)$$

$$= (g_1 g'_1, g_2 g'_2, \dots, g_n g'_n)$$

Theorem: $G_1 \times G_2 \times \dots \times G_n$ is a group. with identity (e, e, \dots, e)

$$\text{inverse } (g_1, g_2, \dots, g_n)^{-1} = (g_1^{-1}, g_2^{-1}, \dots, g_n^{-1})$$

Write the direct product $G_1 \times G_2 \times \dots \times G_n$ as $G_1 \oplus G_2 \oplus G_3 \oplus \dots \oplus G_n$

ex: $\mathbb{Z}_2 \oplus \mathbb{Z}_2 = \{(0,0), (1,0), (0,1), (1,1)\}$

Note $\mathbb{Z}_2 \oplus \mathbb{Z}_2 \cong K_4$ the klein group.

ex: $\mathbb{Z}_2 \oplus \mathbb{Z}_3 = \{(0,0), (0,1), (0,2), (1,0), (1,1), (1,2)\}$

$$(1,1) \cdot 2(1,1) = (0,2) \quad , \quad 3(1,1) = (1,0) \quad 4(1,1) = (0,1) \quad 5(1,1) = (1,1) \quad 6(1,1) = (0,0)$$

$\mathbb{Z}_2 \oplus \mathbb{Z}_3$ is cyclic with generator $(1,1)$

$$\mathbb{Z}_2 \oplus \mathbb{Z}_3 = \langle (1,1) \rangle$$

10/16/19

Quiz on cosets & lagrange's theorem.

Groups G_1, G_2, \dots, G_n

Direct product $G_1 \times G_2 \times \dots \times G_n$

$$(g_1, g_2, \dots, g_n) \cdot (g_1', g_2', \dots, g_n')$$

$$= g_1 g_1' + g_2 g_2' + \dots + g_n g_n'$$

Sometimes use \oplus instead of \times

$$\mathbb{Z}_2 \oplus \mathbb{Z}_3 = \{(0,0), (1,3), (0,2), \dots\}$$

$$(1,3) + (0,2) = (1,1)$$

$$|\mathbb{Z}_2 \oplus \mathbb{Z}_3| = 2 \cdot 3 = 6$$

Theorem: If G_1, G_2, \dots, G_n are finite,

$$\text{then } |G_1 \times G_2 \times \dots \times G_n| = |G_1||G_2| \dots |G_n|$$

and for $(g_1, g_2, \dots, g_n) \in G_1 \times G_2 \times \dots \times G_n$

$$|(g_1, g_2, \dots, g_n)| = \text{lcm}(|g_1|, |g_2|, \dots, |g_n|)$$

$$\mathbb{Z}_2 \oplus \mathbb{Z}_3 = \langle (1,1) \rangle \quad \text{cyclic with generator } (1,1) \quad |\mathbb{Z}_2 \oplus \mathbb{Z}_3| = 2 \cdot 3 = 6$$

$$60 \cong \mathbb{Z}_6$$

Theorem: Criterion for $G \oplus H$ to be cyclic.

Let G and H be finite cyclic groups.

Then $G \oplus H$ is cyclic.

Iff: (1) $|G_1|$ and $|H_1|$ are relatively prime.

(Corollary): Let G_1, G_2, \dots, G_n be finite cyclic groups.

Then $G_1 \oplus G_2 \oplus \dots \oplus G_n$ is cyclic.

Iff $|G_i|$ and $|G_j|$ are relatively prime $\forall i \neq j$

Corollary: $m = n_1 n_2 \dots n_k$

Then $\mathbb{Z}_m \cong \mathbb{Z}_{n_1} \oplus \mathbb{Z}_{n_2} \oplus \dots \oplus \mathbb{Z}_{n_k}$.

Iff n_i and n_j are relatively prime $\forall i \neq j$

Ex: $\mathbb{Z}_2 \oplus \mathbb{Z}_3 \oplus \mathbb{Z}_{11} \cong \mathbb{Z}_{110}$.

9. Normal subgroups and Factor Groups

$$S_3 = \{\epsilon, (1 2 3), (1 3 2), (1 2), (2 3), (1 3)\}$$

$$\text{let } \sigma = (1 2 3), \tau = (1 2)$$

$$\text{then } \sigma^2 = (1 3 2) \quad \sigma^3 = \epsilon$$

$$\tau \sigma = (2 3) \quad \tau \sigma^2 = (1 3)$$

$$S_3 = \{\epsilon, \sigma, \sigma^2, \tau, \tau \sigma, \tau \sigma^2\}$$

$$\sigma^2 = \epsilon = \tau^2 \quad \sigma \tau \sigma = \tau$$

$$\sigma \tau = \tau \sigma$$

$$\text{let } H = \{\epsilon, \tau\}, H \leq S_3$$

$$H\sigma = \{\sigma, \tau \sigma\} \quad \sigma H = \{\epsilon \sigma, \sigma \tau\} = \{\epsilon, \tau\} = H\sigma$$

$$\text{So } H\sigma \neq \sigma H \quad \text{Non abelian}$$

Defn: A subgroup H of a group G is normal

$$\text{if } gH = Hg \quad \forall g \in G$$

We write $H \trianglelefteq G$

$$\text{Ex: } S_3 = \{\epsilon, \sigma, \sigma^2, \tau, \tau \sigma, \tau \sigma^2\}$$

$$\text{let } K = \{\epsilon, \sigma, \sigma^2\}$$

$$\sigma \tau \sigma = \tau$$

$$\tau K = K \tau \quad \& \quad \sigma^2 K = K \sigma^2$$

$$\sigma \tau = \tau \sigma^2$$

$$\tau \sigma = \sigma^2 \tau \quad \& \quad \sigma \tau \sigma = \tau \sigma^2$$

$$\tau K = \langle \tau, \tau\sigma, \tau\sigma^2 \rangle = \tau K = \tau\sigma^2 K$$

$$\Rightarrow \tau K = K\tau \quad \text{so } K \in S_3.$$

Theorem: If G is abelian, then every subgroup of G is normal.

Normality test: let H be a subgroup of a group G .

then equivalent: ① $H \trianglelefteq G$

$$② gHg^{-1} = H \quad \forall g \in G$$

$$③ gHg^{-1} \subseteq H \quad \forall g \in G$$

Ex: General linear group $GL(2, \mathbb{R}) = \left\{ \begin{pmatrix} a & b \\ c & d \end{pmatrix} \mid ad - bc \neq 0 \right\}$

$$SL(2, \mathbb{R}) = \left\{ \begin{pmatrix} a & b \\ c & d \end{pmatrix} \mid ad - bc = 1 \right\}$$

$$\text{let } A = GL(2, \mathbb{R}) \quad B = SL(2, \mathbb{R})$$

$$\text{then } \det(ABA^{-1}) = \det A \det B \det A^{-1}$$

$$= \det A \det B \frac{1}{\det A}$$

$$= \det A (1) \frac{1}{\det A} = 1$$

$$\text{so } ABA^{-1} \in SL(2, \mathbb{R})$$

$$\text{consequently } SL(2, \mathbb{R}) \trianglelefteq GL(2, \mathbb{R})$$

Ex: The alternating group A_n of even permutations is normal in S_n .

let $\tau \in A_n$ and consider $\sigma \in S_n$

τ can be written as a product of an even number of transpositions.

Suppose σ can be written as a product of m transpositions

$$\text{then } \sigma\tau\sigma^{-1} = m + k + m = 2m + k, \quad k \text{ even. } 2m + k \text{ is even.}$$

$$\text{so } \sigma\tau\sigma^{-1} \in A_n$$

$$\text{consequently } A_n \trianglelefteq S_n$$

10/18/19 Exam 2 Friday 10/25

Isomorphisms, cosets, Lagrange's theorem, Direct products, normal subgroups, factor (quotient groups)

Quotient Groups (Factor Groups)

let G be a group and H a subgroup.

let $G/H = \text{set of cosets.}$

$$= \{ Ha \mid a \in G \}$$

Define a product in G/H by $HaHb = Hab$

Question: When is G/H a group? When is this product well defined?

Lemma: let G be a group and K a subgroup.

then equivalent: ① $K \trianglelefteq G$

Recall for $K \leq G$, $k \in G$ if $kg = gk \quad \forall g \in G$

② The product of cosets $ka_kb = kab$ is well defined

if ① implies ② Suppose $K \trianglelefteq G$, if $ka_1a_2 = kb_1b_2$,

then $kab = ka_1b_1$,

$$kab = ka_1b_1$$

$$kab = ka_1b_1 = a_1kb_1 = a_1k b_1 = ka_1b_1,$$

Theorem. Let $K \trianglelefteq G$. Then the set of right or left cosets $G/K = \{Ka\mid a \in G\}$ is a group (Factor, quotient group) such that $Kak^{-1} = Kab$

Proof: $KeKa = Kea = Ka = Kae = kak^{-1}$

so $Ke = K$, so K is the identity in G/K

Inverse of ka is $k^{-1}a^{-1}$

$$Kak^{-1} = Kaa^{-1} = K = ka^{-1}a = K^{-1}Ka$$

Associative:

$$Ka(KkbKc) = Ka(Kbc) = K(aKb) = kab = (kaKb)Kc$$

10/21/19

Factor / Quotient groups

$$H \trianglelefteq G, H \trianglelefteq G.$$

$$\text{if } H \trianglelefteq G \quad \forall g \in G$$

$$\text{Set of cosets } G/H = \{Ha \mid a \in G\}$$

when H is a normal subgroup, $G/H = \{Ha \mid a \in G\}$ is a group.

$$HaHb = Hab. \quad G/H \text{ is a quotient, factor group.}$$

$$\text{ex: } G = \langle a \rangle, |a| = 12, \text{ let } K = \langle a^4 \rangle = \{e, a^4, a^8\}$$

$K \trianglelefteq G$, since G is abelian.

$$\text{Cosets of } K \text{ in } G. \quad K = \{e, a^4, a^8\} \quad Ka = \{a^4, a^8, a^{10}\}$$

$$ka = \{a, a^5, a^9\} \quad ka^2 = \{a^3, a^7, a^{11}\}$$

Quotient group.

$$G/K = \{K, Ka, Ka^2, Ka^3\} \text{ is cyclic of order 4, } G/K = \langle Ka \rangle$$

G/K	K	ka	ka^2	ka^3
K	K	ka	ka^2	ka^3
ka	ka	ka^2	ka^3	K
ka^2	ka^2	ka^3	K	ka
ka^3	ka^3	K	ka	ka^2

Theorem: (Properties of quotient groups)

Let G be a group and $K \trianglelefteq G$.

① If G is abelian, then G/K is abelian.

② If $G = \langle a \rangle$ is cyclic, then G/K is cyclic with $G/K = \langle Ka \rangle$.

③ If G is finite, then $|G/K| = |G|/|K| = |G|/|eK|$

If: ① If G is abelian, then $Kak^{-1} = Kab = Kba = KbkK$

② If G is cyclic, then $G = \langle a \rangle = \{a^n \mid n \in \mathbb{Z}\}$

$$G/K = \{ke \mid a^n \in K\} = \{(ka^n) \mid n \in \mathbb{Z}\} = \langle Ka \rangle$$

③ $|G/K| = \text{number of distinct cosets of } K \text{ in } G. = |G|/|K|$

by Lagrange's theorem ($|G| = |G| : |K| \cdot |K|$)

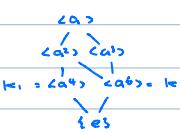
$$\text{so } |G| : |K| = |G| / |K|$$

$$\text{so } |G| : |K| = |G| : |eK| = |G| / |eK|$$

$$\text{ex: let } G = \langle a \rangle = \{e, a^2\}, |a| = 12$$

let $K = \langle a^6 \rangle = \{e, a^6\}$ lattice of subgroups of G .

$$\text{and } K_1 = \langle a^4 \rangle = \{e, a^4, a^8\}$$



$$\text{for } G/K, |G| : |K| = 12 : 2 = 6$$

Since G is cyclic, G/K is cyclic with $G/K = \langle Ka \rangle = \{K, Ka, Ka^2, Ka^3, Ka^4, Ka^5\}$

proper subgroups of $\langle ka \rangle$ are $\langle ka^2 \rangle = \{K, ka^2, ka^4\}$ ← divisors of 6 are 2, 3.
 $\langle ka^3 \rangle = \{K, ka^3\}$

lattice of subgroups of $\langle ka \rangle$
 $\langle ka \rangle = \langle ka^3 \rangle$
 $\langle ka^2 \rangle$
 $\langle ka \rangle$
 $\langle ka^3 \rangle$
 $\{K\}$

$$\text{For } G/\langle K \rangle, |G/\langle K \rangle| = |G|/|\langle K \rangle| = 12/3 = 4.$$

since $G = \langle a \rangle$ is cyclic, $G/\langle K \rangle$ is cyclic with $\langle ka \rangle$

$$G/\langle K \rangle = \langle \langle ka \rangle \rangle = \{K, \langle ka \rangle, \langle ka^2 \rangle, \langle ka^3 \rangle\}$$

trivial proper subgroup $\langle \langle ka^3 \rangle \rangle = \{K, \langle ka^3 \rangle\}$

lattice of subgroups of $G/\langle K \rangle$,

$\langle ka \rangle = \langle \langle ka^3 \rangle \rangle$
 $\langle ka^2 \rangle$
 $\langle ka \rangle$
 $\{K\}$

Note: There is a one-to-one correspondence between the subgroup of G with contain K , ($\{K\}, \langle a^2 \rangle, \langle a^3 \rangle, \langle a \rangle$) and the subgroup of $G/\langle K \rangle$ ($G/\langle K \rangle, \langle \langle ka^2 \rangle \rangle, \langle \langle ka^3 \rangle \rangle, \{K\}$)

Theorem: (Correspondence theorem)

Let $K \trianglelefteq G$, then the correspondence between $H \leftrightarrow H/\langle K \rangle$

is a bijection between the subgroups H of G that contain K and the subgroups of $G/\langle K \rangle$

$$\text{ex: } G = \langle a \rangle, |a| = 18 \quad \text{let } K = \langle a^6 \rangle$$

Determine the order of $\langle ka^5 \rangle$ in $G/\langle K \rangle$.

$$K = \langle a^6 \rangle = \{K, a^6, a^{12}\}$$

$$|G/\langle K \rangle| = 18/3 = 6$$

$$G/\langle K \rangle = \{K, \langle ka \rangle, \langle ka^2 \rangle, \langle ka^3 \rangle, \langle ka^4 \rangle, \langle ka^5 \rangle\} = \langle \langle ka \rangle \rangle$$

Since $|G/\langle K \rangle| = 6$. by Langrange theorem $|\langle ka^5 \rangle| = 1, 2, 3, \text{ or } 6$.

Since $\langle ka^5 \rangle \neq K$, $|\langle ka^5 \rangle| \neq 1$

$$(ka^5)^2 = ka^{10} \neq K \quad \text{since } a^{10} \notin K \quad |\langle ka^5 \rangle| \neq 2$$

$$(ka^5)^3 = ka^{15} \neq K \quad a^{15} \notin K \quad |\langle ka^5 \rangle| \neq 3.$$

$$(ka^5)^6 = ka^{30} = ka^{12} \quad \text{therefore } |\langle ka^5 \rangle| = 6$$

OR: since $G/\langle K \rangle = \langle \langle ka \rangle \rangle$ is cyclic of order 6

we know $\langle \langle ka \rangle \rangle^5 = \langle \langle ka^5 \rangle \rangle$ is also a generator, so $|\langle \langle ka^5 \rangle \rangle| = 6$

OR: $\gcd(6, 18) = 1$

$$G = \langle a^6 \rangle \quad \text{so } G/\langle K \rangle = \langle \langle ka^5 \rangle \rangle \quad |\langle \langle ka^5 \rangle \rangle| = 6$$

10/28/19

10. Group Homomorphisms

Let G_1 and G_2 be groups.

We say a map $\varphi: G_1 \rightarrow G_2$ is a homomorphism

$$\text{if } \varphi(ab) = \varphi(a)\varphi(b) \quad \forall a, b \in G_1$$

Ex: 1) An isomorphism is a homomorphism that is one to one and onto

2) Trivial homomorphism $\varphi: G \rightarrow G_1$, $\varphi(a) = e$ $\forall a \in G$

3) Id: $G \rightarrow G$ $\text{Id}(a) = a$

4) The determinant map $GL(2, \mathbb{R}) \xrightarrow{\det} \mathbb{R}^\times$

$$\det(AB) = \det A \det B$$

\mathbb{R}^\times : group of units of \mathbb{R} = $(\mathbb{R} - \{0\}, \times)$

5) Suppose $K \leq G$, the coset map or canonical map

$$\varphi: G \rightarrow G/K, \quad \varphi(a) = Ka = [a]$$

is a homomorphism

$$\text{Op: } \varphi(ab) = Kab = KAK^{-1} = \varphi(a)\varphi(b)$$

6) Special case of 5: $\mathbb{Z} \rightarrow \mathbb{Z}_n \cong \mathbb{Z}/n\mathbb{Z}$

$$m \mapsto [m]$$

Theorem: $\varphi: G \rightarrow G_1$, a homomorphism

then 1) $\varphi(e) = e$

2) $\varphi(a^{-1}) = \varphi(a)^{-1}$

3) $\varphi(a^k) = \varphi(a)^k \quad k \in \mathbb{Z}$

$$\text{pf: 1) } \varphi(e) = \varphi(e \cdot e) = \varphi(e)\varphi(e)$$

$$\varphi(e) \cdot e = \varphi(e)\varphi(e)$$

$$\varphi(e) = e$$

$$\Rightarrow \varphi(a^{-1})\varphi(a) = \varphi(a^{-1}a) = \varphi(e) = e$$

$$\text{so } \varphi(a^{-1}) = \varphi(a)^{-1}$$

$$\text{3) } \varphi(a^k) = \varphi(a \cdots a) = \varphi(a) \cdots \varphi(a) = \varphi(a)^k$$

let $\varphi: G \rightarrow G_1$, a homomorphism.

Image of φ $\text{Im } \varphi: \varphi(G) = \{ \varphi(a) \mid a \in G \}$

kernel of φ $\ker \varphi: \{ a \in G \mid \varphi(a) = e \}$

Theorem: let $\varphi: G \rightarrow G_1$, be a homomorphism.

then 1) $\text{Im } \varphi \leq G_1$

2) $\ker \varphi \trianglelefteq G$

pf: 1) Apply the subgroup test.

$$\therefore \varphi(e) = e, \text{ so } e \in \text{Im } \varphi$$

Closed - let $b_1, b_2 \in \text{Im } \varphi$

$$\text{then } b_1 = \varphi(a_1), b_2 = \varphi(a_2) \text{ for some } a_1, a_2 \in G,$$

$$\text{then } \varphi(a_1 a_2) = \varphi(a_1) \varphi(a_2) = b_1 b_2$$

$$\text{so } b_1 b_2 \in \text{Im } \varphi.$$

$$\bullet \text{ If } b \in \text{Im } \varphi, \text{ then } b = \varphi(a) \text{ for some } a \in G$$

$$\text{then } \varphi(a^{-1}) = \varphi(a)^{-1} = b^{-1}$$

$$\text{so } b^{-1} \in \text{Im } \varphi$$

By the subgroup test $\text{Im } \varphi \trianglelefteq G_1$.

2) Apply the subgroup test.

① to show $\ker \varphi \trianglelefteq G$...

Apply the test for normality to show $\ker \varphi \trianglelefteq G$

$$\text{let } g \in G, \quad g(\ker \varphi)g^{-1} \subseteq \ker \varphi$$

$$\text{let } a \in \ker \varphi \text{ then } \varphi(gag^{-1}) = \varphi(g)\varphi(a)\varphi(g^{-1})$$

$$= \varphi(g)\varphi(g^{-1}) = e$$

$$\text{hence } gag^{-1} \in \ker \varphi$$

$$\text{Consequently } g(\ker \varphi)g^{-1} \subseteq \ker \varphi \quad \forall g \in G$$

ex: 1) multiplication by n map

$$\mathbb{Z} \xrightarrow{\times n} \mathbb{Z}, \quad k \mapsto nk.$$

$$\varphi: \mathbb{Z} \rightarrow \mathbb{Z}, \quad \varphi(k) = nk$$

$$\varphi(k+l) = nk+nl = \varphi(k)+\varphi(l)$$

$$\ker \varphi: \quad \varphi(k) = nk = 0 \quad k=0$$

$$\ker \varphi = \{0\} \quad \text{trivial Kernel} = \varphi \text{ is 1-1}$$

$$\text{Im } \varphi = n\mathbb{Z}$$

2) G abelian, let $m \in \mathbb{Z}$, $\varphi: G \rightarrow G$

m^{th} power map: $\varphi(a) = a^m$ is a homomorphism

$$\varphi(ab) = (ab)^m = a^m b^m = \varphi(a)\varphi(b)$$

3) let $K \trianglelefteq G$ kanonical map $g: G \rightarrow G/K$ $g(a) = ka$

$$\ker g = K \quad \text{because} \quad g(a) = ka = 1_K \iff a \in K$$

the kanonical map $G \rightarrow G/K$ is always onto

$$\text{Given } ka \in G/K, \quad g(a) = ka \quad \text{Im } g = G/K$$

Every normal subgroup is a kernel of an onto homomorphism

4) determinant mapping

$$\det: GL(2, \mathbb{R}) \rightarrow \mathbb{R}^\times$$

$$\ker \det = \{ A \in GL(2, \mathbb{R}) \mid \det A = 1 \}$$

$$\ker \det = SL(2, \mathbb{R})$$

$$SL(2, \mathbb{R}) \trianglelefteq GL(2, \mathbb{R})$$

5) sign mapping

$$\text{sgn}: S_n \rightarrow \{1, -1\}$$

$$\text{sgn } \sigma = \begin{cases} 1 & \text{if } \sigma \text{ is even} \\ -1 & \text{if } \sigma \text{ is odd} \end{cases}$$

$$\text{sgn } (\sigma\tau) = \text{sgn } \sigma \text{sgn } \tau \quad \forall \sigma, \tau \in S_n.$$

homomorphism

$$\text{sgn}: S_n \rightarrow \{1, -1\}$$

$$\ker \text{sgn} = \{ \sigma \in S_n \mid \sigma \text{ is even} \} = A_n$$

$$\text{therefore } A_n \trianglelefteq S_n$$

10/30/19

II Fundamental theorem of finite abelian groups

$$\mathbb{Z}_8 \cong \mathbb{Z}_2 \oplus \mathbb{Z}_2$$

only one abelian group of order 15

isomorphism classes of abelian group of order 12

$$12 = 2^2 \cdot 3 \quad \mathbb{Z}_{12} \cong \mathbb{Z}_2 \oplus \mathbb{Z}_6$$

$$\mathbb{Z}_{12} \cong \mathbb{Z}_2 \oplus \mathbb{Z}_2 \oplus \mathbb{Z}_3 \quad \mathbb{Z}_2 \oplus \mathbb{Z}_2 \not\cong \mathbb{Z}_4$$

up to isomorphism, there are two abelian groups of order 12

Fundamental theorem of finite abelian groups.

every finite abelian group is isomorphic to a direct product of cyclic groups of prime power order.

The number of terms in the product and the order of the cyclic groups are uniquely determined by the group.

That is, if G is a finite abelian group, then G is isomorphic $\mathbb{Z}_{p_1^{n_1}} \oplus \mathbb{Z}_{p_2^{n_2}} \oplus \dots \oplus \mathbb{Z}_{p_k^{n_k}}$

where $p_1 \dots p_k$ are prime, not necessarily distinct primes. and the prime powers $p_1^{n_1}, p_2^{n_2} \dots p_k^{n_k}$ are uniquely determined by G .

ex: $|G| = p^k$ $p \in \text{prime}$ $k \in \mathbb{Z}^+$

A partition of k is a set of positive integers $n_1 \dots n_k$, whose sum is k .
 $n_1 + n_2 + \dots + n_k = k$.

there is an abelian group of order p^k for each partition of k .

ex: $p = 2$, $k = 4$, $|G| = 2^4 = 16$

Isomorphism classes of abelian group of order 16.

partition of 4. Group.

4	\rightarrow	\mathbb{Z}_{16}
1+3	\rightarrow	$\mathbb{Z}_2 \oplus \mathbb{Z}_8$
2+2	\rightarrow	$\mathbb{Z}_4 \oplus \mathbb{Z}_4$
1+1+2	\rightarrow	$\mathbb{Z}_2 \oplus \mathbb{Z}_2 \oplus \mathbb{Z}_4$
1+1+1+1	\rightarrow	$\mathbb{Z}_2 \oplus \mathbb{Z}_2 \oplus \mathbb{Z}_2 \oplus \mathbb{Z}_2$

Ex: G is abelian $|G| = 72 = 8 \cdot 9 = 2^3 \cdot 3^2$

partition of 3	/ 2	Group
3	2	$\mathbb{Z}_2 \trianglelefteq \mathbb{Z}_2 \oplus \mathbb{Z}_9$
1+2	2	$\mathbb{Z}_2 \oplus \mathbb{Z}_3 \oplus \mathbb{Z}_9$
1+1+1	2	$\mathbb{Z}_2 \oplus \mathbb{Z}_2 \oplus \mathbb{Z}_2 \oplus \mathbb{Z}_9$
3	1+1	$\mathbb{Z}_8 \oplus \mathbb{Z}_3 \oplus \mathbb{Z}_3$
1+2	1+1	$\mathbb{Z}_2 \oplus \mathbb{Z}_4 \oplus \mathbb{Z}_3 \oplus \mathbb{Z}_3$
1+1+1	1+1	$\mathbb{Z}_2 \oplus \mathbb{Z}_2 \oplus \mathbb{Z}_2 \oplus \mathbb{Z}_3 \oplus \mathbb{Z}_3$

Ex: Find all abelian groups up to isomorphism of order $2 \cdot 3^2 \cdot 5^2 \cdot 7 = 3150$

partition of 2	Groups.
2	$\mathbb{Z}_2 \oplus \mathbb{Z}_9 \oplus \mathbb{Z}_{25} \oplus \mathbb{Z}_7 \cong \mathbb{Z}_{3150}$
1+1	$\mathbb{Z}_2 \oplus \mathbb{Z}_3 \oplus \mathbb{Z}_3 \oplus \mathbb{Z}_{25} \oplus \mathbb{Z}_7 \cong \mathbb{Z}_3 \oplus \mathbb{Z}_{1050}$
	$\mathbb{Z}_2 \oplus \mathbb{Z}_9 \oplus \mathbb{Z}_5 \oplus \mathbb{Z}_5 \oplus \mathbb{Z}_7 \cong \mathbb{Z}_5 \oplus \mathbb{Z}_{630}$
	$\mathbb{Z}_2 \oplus \mathbb{Z}_3 \oplus \mathbb{Z}_3 \oplus \mathbb{Z}_5 \oplus \mathbb{Z}_5 \oplus \mathbb{Z}_7 \cong \mathbb{Z}_3 \oplus \mathbb{Z}_5 \oplus \mathbb{Z}_{210}$
	$\underbrace{\mathbb{Z}_5 \oplus \mathbb{Z}_{210}}_{\substack{\text{prime power decomposition.} \\ \text{Invariant factor decomposition}}}$

11/1/19

Fundamental Theorem of Finite Abelian Groups

G a finite abelian group.

$$G \cong \mathbb{Z}_{p_1^{n_1}} \oplus \mathbb{Z}_{p_2^{n_2}} \oplus \dots \oplus \mathbb{Z}_{p_k^{n_k}}$$

$p_1 \dots p_k$ not necessarily distinct prime
 $p_1^{n_1} \dots p_k^{n_k}$ are uniquely determined by G

All abelian groups (up to isomorphism) of order 36

$$|G| = 36 = 4 \cdot 9 = 2^2 \cdot 3^2$$

$$\mathbb{Z}_4 \oplus \mathbb{Z}_9 \cong \mathbb{Z}_{36}$$

$$\mathbb{Z}_4 \oplus \mathbb{Z}_2 \oplus \mathbb{Z}_3 \cong \mathbb{Z}_3 \oplus \mathbb{Z}_{12}$$

$$\mathbb{Z}_2 \oplus \mathbb{Z}_2 \oplus \mathbb{Z}_9 \cong \mathbb{Z}_2 \oplus \mathbb{Z}_{18}$$

$$\mathbb{Z}_2 \oplus \mathbb{Z}_2 \oplus \mathbb{Z}_7 \oplus \mathbb{Z}_3 \cong \mathbb{Z}_6 \oplus \mathbb{Z}_6$$

prime power
decomposition

invariant factor
decomposition

Suppose

$$G \cong \mathbb{Z}_{p_1^{n_1}} \oplus \mathbb{Z}_{p_2^{n_2}} \oplus \cdots \oplus \mathbb{Z}_{p_k^{n_k}}$$

Using that $\mathbb{Z}_r \cong \mathbb{Z}_s \oplus \mathbb{Z}_t \iff \gcd(r, s) = 1$

we write $G \cong \mathbb{Z}_{m_1} \oplus \mathbb{Z}_{m_2} \oplus \cdots \oplus \mathbb{Z}_{m_s}$

$m_1 | m_2, m_2 | m_3, \dots$ this is the invariant factor decomposition of G .

Corollary: If m divides the order of a finite abelian group G ,

then G has a subgroup of order m .

ex: isomorphism classes of abelian groups of order 108

$$108 = 2 \cdot 54 = 2 \cdot 9 \cdot 6 = 2^2 \cdot 3^3$$

$$\mathbb{Z}_4 \oplus \mathbb{Z}_{27} \cong \mathbb{Z}_{108}$$

$$\mathbb{Z}_2 \oplus \mathbb{Z}_2 \oplus \mathbb{Z}_{27} \cong \mathbb{Z}_2 \oplus \mathbb{Z}_{54}$$

$$\mathbb{Z}_4 \oplus \mathbb{Z}_3 \oplus \mathbb{Z}_9 \cong \mathbb{Z}_3 \oplus \mathbb{Z}_{36}$$

$$\mathbb{Z}_4 \oplus \mathbb{Z}_3 \oplus \mathbb{Z}_3 \oplus \mathbb{Z}_3 \cong \mathbb{Z}_3 \oplus \mathbb{Z}_3 \oplus \mathbb{Z}_{12}$$

$$\mathbb{Z}_2 \oplus \mathbb{Z}_3 \oplus \mathbb{Z}_3 \oplus \mathbb{Z}_9 \cong \mathbb{Z}_6 \oplus \mathbb{Z}_6$$

$$\mathbb{Z}_2 \oplus \mathbb{Z}_2 \oplus \mathbb{Z}_3 \oplus \mathbb{Z}_3 \oplus \mathbb{Z}_3 \cong \mathbb{Z}_3 \oplus \mathbb{Z}_6 \oplus \mathbb{Z}_6$$

First Isomorphism Theorem

$\varphi: G \rightarrow G'$ homomorphism: $\varphi(a+b) = \varphi(a) + \varphi(b) \quad \forall a, b \in G$

$\text{Ker } \varphi = \{a \in G \mid \varphi(a) = e\}$

Theorem: If $\varphi: G \rightarrow G'$ is a homomorphism,

then $\text{Ker } \varphi = \{e\}$ iff φ is one-to-one

pf: suppose φ is one to one

then since $\varphi(e) = e$, $\text{Ker } \varphi = \{e\}$

conversely, let $\text{Ker } \varphi = \{e\}$, $\varphi(a) = \varphi(b)$

$$\text{then } \varphi(a b^{-1}) = \varphi(a) \varphi(b^{-1}) = \varphi(a) \varphi(b)^{-1} = \varphi(a) \varphi(a)^{-1} = e$$

$$\text{since } \text{Ker } \varphi = \{e\} \quad a b^{-1} = e \quad a = b$$

Theorem (First Isomorphism Theorem)

Suppose $\varphi: G \rightarrow G'$ is a homomorphism, and let $K = \text{Ker } \varphi$

then φ induces an isomorphism $\bar{\varphi}: G/K \rightarrow \text{Im } \varphi$

$$\bar{\varphi}(ka) = \varphi(a)$$

that is $G/K \cong \text{Im } \varphi$

thus φ factors as $\bar{\varphi} = \varphi q$

$$\begin{array}{ccc} a & \xrightarrow{\varphi} & G' \\ \downarrow q & \nearrow \bar{\varphi} & \downarrow \varphi(a) \\ ka & \xrightarrow{q} & G'/K \end{array}$$

where $q: G \rightarrow G/K$ is the canonical map $q(a) = ka$

Suppose we have an onto homomorphism $\varphi: G \rightarrow G'$ with $K = \text{Ker } \varphi$.

then by the isomorphism theorem, $G/K \cong G'$.

11/4/19

a) $n \in m\mathbb{Z}$

Define $\varphi: n\mathbb{Z} \rightarrow m\mathbb{Z}$ by $\varphi(nk) = mk$

$$\varphi(nk) = \varphi(nk)$$

$$mk = ml \quad k = l \Rightarrow nk = nl$$

$$\text{if } mk \in m\mathbb{Z}$$

then $\varphi(nk) = nk$

$$\varphi(nk+n\ell) = \varphi(n(k+\ell)) = n(k+\ell) = nk+n\ell = \varphi(nk) + \varphi(n\ell)$$

(1) $\text{Aut } \mathbb{Z} \quad \mathbb{Z} \xrightarrow{\varphi} \mathbb{Z} \quad \varphi(1)$ must be a generator of \mathbb{Z} .

$$\varphi(1) = 1 \quad \text{or} \quad \varphi(1) = -1$$

$$\varphi: \mathbb{Z} \rightarrow \mathbb{Z} \quad \varphi(x) = x$$

$$\varphi: \mathbb{Z} \rightarrow \mathbb{Z} \quad \varphi(x) = -x$$

$$\text{Aut } \mathbb{Z} \cong \{1, -1\} \cong \mathbb{Z}_2$$

4) $\varphi: G_1 \rightarrow G_1, \quad H \trianglelefteq G_1$

Claim $\varphi(H) \trianglelefteq G_1$,

Let $g_1 \in G_1$, we show

$$g_1 \varphi(H) g_1^{-1} \subseteq \varphi(H)$$

Since φ is onto, there is some $g \in G_1$ so that $\varphi(g) = g_1$.

$$\text{Let } \varphi(h) \in \varphi(H)$$

$$\text{then } g_1 \varphi(h) g_1^{-1} = \varphi(g_1) \varphi(h) \varphi(g_1^{-1}) = \varphi(g h g^{-1})$$

$$\text{and } g h g^{-1} \in H, \text{ since } H \trianglelefteq G_1.$$

$$\text{So } \varphi(g h g^{-1}) \in \varphi(H)$$

$$\text{Therefore } \varphi(H) \trianglelefteq G_1.$$

The Isomorphism theorem

Theorem : Let $\varphi: G \rightarrow G_1$ be an onto homomorphism, with $\ker \varphi = K$

$$\text{then } G/K \cong G_1.$$

ex: The homomorphism $\mathbb{Z} \xrightarrow{\varphi} \mathbb{Z}_n$

by $\varphi(k) = [k]$ is onto with $\ker \varphi = n\mathbb{Z}$

By the Isomorphism theorem,

$$\mathbb{Z}/n\mathbb{Z} \cong \mathbb{Z}_n$$

ex: $\mathbb{Z} \xrightarrow{\varphi} \mathbb{Z}_5$

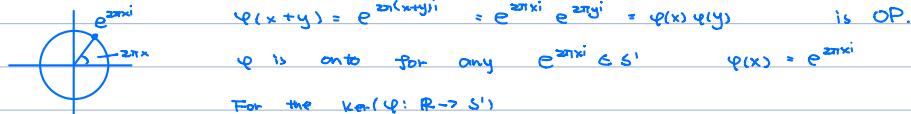
$$7 \mapsto 2$$

$$5 \mapsto 0 \quad 10 \mapsto 0$$

ex: $\mathbb{R}/\mathbb{Z} \cong S^1$ S^1 is the circle group

$$S^1 = \{z \in \mathbb{C} \mid |z|=1\}$$

Define $\varphi: \mathbb{R} \rightarrow S^1$ by $\varphi(x) = e^{2\pi xi}$



$$\varphi(x+y) = e^{2\pi i(x+y)} = e^{2\pi ix} e^{2\pi iy} = \varphi(x)\varphi(y) \quad \text{is OP.}$$

$$\varphi \text{ is onto for any } e^{2\pi xi} \in S^1 \quad \varphi(x) = e^{2\pi xi}$$

$$\text{For the } \ker(\varphi: \mathbb{R} \rightarrow S^1)$$

$$e^{2\pi xi} = 1 \text{ iff } x \in \mathbb{Z}$$

By the Isomorphism Theorem, $\mathbb{R}/\mathbb{Z} \cong S^1$

12. Introduction to Rings

Definition : A set R is a ring if it has two binary operations,

$a+b$ and ab such that

$$(R, +) \quad \left\{ \begin{array}{l} 1) a+b=b+a \\ 2) a+(b+c)=(a+b)+c \end{array} \right.$$

$$\text{is abelian} \quad \left\{ \begin{array}{l} 3) \exists 0 \in R \text{ such that } a+0=a \quad \forall a \in R \\ 4) \forall a \in R \exists -a \in R \text{ such that } a+(-a)=0 \end{array} \right.$$

$$\text{group} \quad \left\{ \begin{array}{l} 5) a(b+c) = (a b)c \end{array} \right.$$

$$5) a(b+c) = (a b)c$$

$$6) a(b+c) = ab+ac$$

$$(b+c)a = ba+ca \quad \forall a, b, c \in R$$

In addition, most rings also satisfy

$$7) \exists 1 \in R \text{ s.t. } 1 \cdot a = a = a \cdot 1 \quad \forall a \in R$$

We call 1 the unity of R.

R is commutative if $ab = ba \quad \forall a, b \in R$

ex: If multiplicative inverses are missing

\mathbb{Z} ring with no unity

$\mathbb{Q}, \mathbb{R}, \mathbb{C}$ all commutative. $\exists a^{-1} \forall a \neq 0$ there are fields.

$$\text{In } [\alpha] + [\beta] = [\alpha+\beta], \quad [\alpha][\beta] = [\alpha\beta].$$

$[\alpha]^{-1}$ is missing in general (units \mathbb{Z}^\times)

special case:

\mathbb{Z}_p . $p \in \text{prime}$. Then $[\alpha]^{-1}$ exists for all $a \neq 0$

\mathbb{Z}_p is a field.

ex: $R = \mathbb{Z}, \mathbb{Q}, \mathbb{R}, \mathbb{C}$

$M(2, R) \approx 2 \times 2$ matrices over R

Is a noncommutative ring.

ex: Let $R = \mathbb{Z}, \mathbb{Q}, \mathbb{R}, \mathbb{C}$.

Ring of polynomials over R.

$$R[x] = \{a_0 + a_1x + a_2x^2 + \dots + a_nx^n \mid a_i \in R\}$$

Polynomials of indeterminate x coefficients in R.

Add / multiply polynomials like usual

Direct product of Rings:

Let R_1, R_2, \dots, R_n be rings

$$R_1 \times R_2 \times \dots \times R_n = R_1 \oplus R_2 \oplus \dots \oplus R_n \approx \{(r_1, r_2, \dots, r_n) \mid r_i \in R_i, i=1, \dots, n\}$$

$$(r_1, r_2, \dots, r_n) + (s_1, s_2, \dots, s_n) = (r_1+s_1, r_2+s_2, \dots, r_n+s_n)$$

$$(r_1, r_2, \dots, r_n)(s_1, s_2, \dots, s_n) = (r_1s_1, r_2s_2, \dots, r_ns_n)$$

11/6/19

Intro to Rings

A Ring R has operations $a+b$, ab so that $(R, +)$ is an abelian group

$$- a(b+c) = (ab)c$$

$$- a(b+c) = ab+ac$$

$$(b+c)a = ba+ca$$

Properties of Rings.

Familiar rules for multiplication

ex: In \mathbb{Z} (theorem 12.1) $a \cdot 0 = 0, (-1)a = -a$

The unity of a ring is unique.

If $a \in R$ has a multiplicative inverse a^{-1} , it is unique.

Subrings

A subset S of a ring R is a subring if S is itself a ring under the operations in R.

Subring test:

A subset S of a ring R is a subring

iff ① $a \in S$ and $1 \in S$

② If $s \in S$ and $t \in S$, then $s+t$, st , $-s$ are in S

Ex. The ring of Gaussian integers:

$$\mathbb{Z}[i] = \{n + mi \mid n, m \in \mathbb{Z}\}$$

This is a subring of \mathbb{C} .

Ex: Let R be a ring, the ring of upper triangular matrices over R

$$\left\{ \begin{pmatrix} a & b \\ 0 & c \end{pmatrix} \mid a, b, c \in R \right\} \text{ is a subring of } M(2, R)$$

13. Integral Domains

Definition: we say $a \in R$, R a ring,

a is a zero divisor in R if $a \neq 0$ and either $ab=0$ for some $b \neq 0$ in R .

or $ca=0$ for some $c \neq 0$ in R .

Ex: In the ring \mathbb{Z}_6 , $2, 3, 4$ are zero divisors.

$$2 \cdot 3 = 0, \quad 3 \cdot 4 = 0$$

Note: If a is not a zero divisor, then $ab=0$ or $ba=0$ implies that $b=0$.

Ex: \mathbb{Z} has no zero divisors.

Definition: A ring R is a domain if it has no zero divisors.

A commutative domain is an integral domain.

Ex: Integral domains: 1) \mathbb{Z}

2) $\mathbb{Z}[i]$ gaussian integers.

3) $\mathbb{Z}[x]$ polynomials over \mathbb{Z}

4) \mathbb{Z}_p , p prime, every non-zero element is a unit,
so not a zero divisor.

11/18/19

13 Integral Domains

R a ring

$a \in R, a \neq 0$ is a zero divisor

if $ab=0$ for some $b \neq 0$ or $ca=0$ for some $c \neq 0$.

$$\text{Ex } M(2, \mathbb{Z}) \quad \begin{pmatrix} 1 & 0 \\ 0 & 0 \end{pmatrix} \begin{pmatrix} 0 & 1 \\ 0 & 0 \end{pmatrix} = \begin{pmatrix} 0 & 0 \\ 0 & 0 \end{pmatrix}$$

An integral domain is a commutative ring with no zero divisors.

\mathbb{Z} is an integral domain

$\mathbb{Z}[x] = \{a_0 + a_1 x + a_2 x^2 + \dots + a_n x^n \mid a_0, a_1, \dots, a_n \in \mathbb{Z}\}$ is an integral domain.

Not integral domains:

1) \mathbb{Z}_n , n not prime

2) $\mathbb{Z} \oplus \mathbb{Z}$ $(1, 0)(0, 1) = (0, 0)$

3) $M(2, \mathbb{Z})$ 2×2 matrices with \mathbb{Z} entries. $\begin{pmatrix} 1 & 0 \\ 0 & 0 \end{pmatrix} \begin{pmatrix} 0 & 1 \\ 0 & 0 \end{pmatrix} = \begin{pmatrix} 0 & 0 \\ 0 & 0 \end{pmatrix}$

Theorem: Let R be an integral domain.

If $ab = ac$ and $a \neq 0$, then $b = c$

Pf: $ab = ac \Rightarrow ab - ac = 0 \Rightarrow a(b - c) = 0$

Since R is an integral domain and $a \neq 0$,

then $b - c = 0 \Rightarrow b = c$

Fields: Ring R , we say $u \in R$ is a unit if it has a multiplicative inverse $u^{-1} \in R$

Group of units $R^\times = \{u \in R \mid u \text{ is a unit}\}$

A ring R is a division ring if every nonzero element is a unit.

$$R^\times = R - \{0\}$$

A commutative division ring is a field.

Proposition: If $u \in R$ is a unit, then u is not a zero divisor.

Pf: $a \cdot u = 0$

$$a \cdot u \cdot u^{-1} = 0 \cdot u^{-1}$$

$$a = 0$$

Theorem: Every finite integral domain is a field

Pf: Let $a \in D$, $a \neq 0$, D is a finite integral domain,

since D is finite, so a, a^2, a^3, \dots can't all be distinct.

So $a^i = a^j$ for some $i > j$

$$a^{i-j} = 1$$

$$a \cdot a^{i-j-1} = 1$$

$$\text{so } a^{-1} = a^{i-j-1}$$

every nonzero a in D is a unit, so D is a field.

Corollary: \mathbb{Z}_p , p prime is a field

Characteristic of a ring

Defn: R a ring, characteristic of R written as $\text{char } R$.

is the smallest positive integer n such that $na = 0 \quad \forall a \in R$

$\text{char } R = 0$, if no such integer exists.

Ex: 1) $\text{char } \mathbb{Z} = 0$

2) $\text{char } \mathbb{Z}_n = n$.

3) $\mathbb{Z}_2[x] = \{a_0 + a_1x + \dots + a_nx^n \mid a_i \in \mathbb{Z}_2\}$ infinite ring with finite characteristic.

$$\text{char } \mathbb{Z}_2[x] = 2$$

11/11/19

13 Integral Domains

R a ring, $a \in R$ is a zero divisor if $a \neq 0$ and $ab = 0$ for some $b \neq 0$ in R

An Integral Domain is a commutative ring with no zero divisors

Characteristic of a ring

$\text{char } R = n$ means n is the smallest positive integer

such that $na = 0 \quad \forall a \in R$

If no such n exists, then $\text{char } R = 0$

Ex: $\text{char } \mathbb{Z}_n = n \quad \text{char } \mathbb{Z} = 0$

Theorem: Let R be a ring with 1.

If 1 has infinite order under addition, then char $R = 0$.

If 1 has order n under addition, then char $R = n$.

because $0 \times 1R = n \times 1R$

$$\text{ex: } M(2, \mathbb{Z}_2) = \left\{ \begin{pmatrix} ab \\ cd \end{pmatrix} \mid a,b,c,d \in \mathbb{Z}_2 \right\}$$

$$n \left(\begin{pmatrix} 1 & 0 \\ 0 & 1 \end{pmatrix} \right) = \left(\begin{pmatrix} 0 & 0 \\ 0 & 0 \end{pmatrix} \right) = \left(\begin{pmatrix} 0 & 0 \\ 0 & 0 \end{pmatrix} \right)$$

$$\text{char } M(2, \mathbb{Z}_2) = 2$$

Theorem: The characteristic of every domain D is either 0 or a prime.

pf: suppose $\text{char } D = n \neq 0$

$$\text{suppose } n = st \quad 0 = n \cdot 1 = (s \cdot 1)(t \cdot 1)$$

because D is a domain, $s \cdot 1 = 0$ OR $t \cdot 1 = 0$

because n is the smallest positive integer with this property,

$$s = n \text{ OR } t = n \quad \text{so } n \text{ is prime.}$$

Field: A field is a commutative ring with unity where every nonzero element is a unit.

example of fields: 1) $\mathbb{Q}(\sqrt{2}) = \{r+s\sqrt{2} \mid r,s \in \mathbb{Q}\}$

$$\text{inverse: } \frac{1}{r+s\sqrt{2}} = \frac{r-s\sqrt{2}}{r^2-2s^2} = \frac{r}{r^2-2s^2} - \frac{s}{r^2-2s^2}\sqrt{2}$$

Note $r+s\sqrt{2} \neq 0$, $r,s \neq 0$, $r-s\sqrt{2} \neq 0$ since $\sqrt{2} \notin \mathbb{Q}$, $r^2-2s^2 \neq 0$

$$2) \mathbb{Z}_3[i] = \{a+bi \mid a,b \in \mathbb{Z}_3\} \quad \text{field of 8 elements}$$

$$= \{0, 1, 2, i, 2i, 1+i, 1+2i, 2+2i\}$$

$$\text{inverse: } \frac{1}{a+bi} = \frac{a-bi}{a^2+b^2} = \frac{a}{a^2+b^2} - \frac{b}{a^2+b^2}i;$$

since \mathbb{Z}_3 is a field we can divide by a^2+b^2 in \mathbb{Z}_3

14. Ideals and Quotient Rings.

R a commutative ring with 1, we say I is an ideal of R .

if 1) $(I, +)$ is a subgroup of $(R, +)$

2) If $a \in R$, $b \in I$ then $ab \in I$

ex: 1) {0} and R are ideals of \mathbb{Z} , the trivial ideal

$$2) R = \mathbb{Z}, \quad I = 5\mathbb{Z}, \dots, I = n\mathbb{Z}, n \in \mathbb{Z}^+$$

$$3) I[x] = \{a_0 + a_1x + a_2x^2 + \dots \mid a_i \in \mathbb{Z}\}$$

$$I = \{a_0 + a_2x^2 \mid a_i \in \mathbb{Z}\}$$

Note that if I is an ideal and $1 \in I$, then $I = R$

because $a \in R$, $1 \in I$, implies $a \cdot 1 = a \in I$, therefore $I = R$

Principal Ideal: Let $a \in R$, then $\langle a \rangle = Ra = \{ra \mid r \in R\}$ is an principal ideal of R generated by a .

pf: to show $(\langle a \rangle, +) \subseteq (R, +)$

$$0 = 0 \cdot a \in \langle a \rangle$$

Given $ra, sa \in \langle a \rangle$

$$ra + sa = (r+s)a \in \langle a \rangle$$

$$-ra = (-r)a \in \langle a \rangle$$

Let $s \in R$, and $ra \in \langle a \rangle$

$$\text{then } sra = (sr)a \in \langle a \rangle \text{ since } sr \in R$$

Quotient Rings.

Suppose $(A, +)$ is a subgroup of $(R, +)$

then $R/A = \{r+A \mid r \in R\}$ is an additive abelian group.

$$(r+A)+(s+A) = (r+s)+A$$

Theorem : Let I be an ideal of $\text{Hng } R$.

$R/I = \{r+I \mid r \in R\}$ is a Hng under the operations $(r+I) + (s+I) = (r+s)+I$

the unity of R/I is $1+I$

$$(r+I)(s+I) = rs+I$$

Proof : We show if I is an ideal, then the product is well defined.

$$\text{If } r+I = r'+I \quad \text{and} \quad s+I = s'+I \quad \text{then} \quad rs+I = r's'+I$$

since $s+I = s'+I$ we have $s-s' \in I$

then $s-s' = a, a \in I$ then $s = s'+a$

similarly : $r = r'+b, b \in I$

$$\text{therefore } rs+I = (r'+b)(s'+a)+I$$

$$= r's' + \underbrace{ra}_{\in I} + \underbrace{s'b}_{\in I} + ba + I = rs'+I$$

since $a, b \in I$

11/13/19

14. Ideals and Quotient Rings

Let R be a commutative ring with 1.

we say I is an ideal of R if

$$1) (I, +) \subseteq (R, +)$$

2) If $r \in R$ and $a \in I$, then $ra \in I$.

Principal Ideal

Let $a \in R$.

then $\langle a \rangle = Ra = \{ra \mid r \in R\}$ is an ideal of R ,

the principal ideal generated by a

Theorem :

Let I be an ideal of R . then $R/I = \{r+I \mid r \in R\}$ is a Hng.

$$(r+I) + (s+I) = (r+s)+I$$

$$(r+I)(s+I) = rs+I$$

ex: Gaussian integers

$$\mathbb{Z}(i) = \{m+ni \mid m, n \in \mathbb{Z}\} = R$$

$$\text{principal ideal } \langle z+i \rangle = R(z+i) = \{(m+ni)(z+i) \mid m+ni \in \mathbb{Z}(i)\}$$

Quotient Ring

$$\mathbb{Z}(i)/\langle z+i \rangle = \{(m+ni) + \langle z+i \rangle \mid m+ni \in \mathbb{Z}(i)\}$$

In the quotient ring, $z+i=0$ $(z+i)+I=0+I$

so $i=-z$ hence $-1=4$ so $5=0$ in the quotient ring.

We can write cosets in $\mathbb{Z}(i)/\langle z+i \rangle$ in the form

$$m+ni + \langle z+i \rangle = m-2n + \langle z+i \rangle \quad \text{using } i=-z$$

where $m-2n \in \mathbb{Z}$ and $5=0$

$$\text{therefore } \mathbb{Z}(i)/\langle z+i \rangle = \{k + \langle z+i \rangle \mid k \in \mathbb{Z}_5\}$$

$$= \{ \langle z+i \rangle, 1 + \langle z+i \rangle, 2 + \langle z+i \rangle, 3 + \langle z+i \rangle, 4 + \langle z+i \rangle \}$$

$\mathbb{Z}(i)/\langle z+i \rangle$ is a field of 5 elements isomorphic to \mathbb{Z}_5

ex: Ring of polynomials over R :

$$R[x] = \{a_0 + a_1x + a_2x^2 + \dots + a_nx^n \mid a_i \in R\} = R$$

Principal ideal generated x^2+1 :

$$\langle x^2+1 \rangle = R(x^2+1) = \{f(x)(x^2+1) \mid f(x) \in R[x]\}$$

In the quotient Hng,

$$R[x]/\langle x^2+1 \rangle = \{g(x) + \langle x^2+1 \rangle \mid g(x) \in R[x]\}$$

$$x^2 + 1 = 0 \text{ so } x^2 = -1$$

Also, using the division algorithm, $g(x) = q(x)(x^2 + 1) + r(x)$

where $r \in \text{deg } R[x] \leq 1$

$$\text{so } R[x]/\langle x^2 + 1 \rangle = \{(ax+b) + \langle x^2 + 1 \rangle \mid a, b \in R\} \text{ with } x^2 = -1$$

thus $R[x]/\langle x^2 + 1 \rangle$ is a field isomorphic to \mathbb{C}

$$\begin{aligned} \text{ex: } & (2x-1) + \langle x^2 + 1 \rangle \cdot ((4x+2) + \langle x^2 + 1 \rangle) \\ &= (2x-1)(4x+2) + \langle x^2 + 1 \rangle \\ &= 12x^2 + 6x - 2 + \langle x^2 + 1 \rangle \\ &= 2x - 14 + \langle x^2 + 1 \rangle \end{aligned}$$

11/15/19

Prime and maximal ideals

commutative ring R with 1 , I is an ideal if:

- 1) $(I, +) \leq (R, +)$
- 2) For every $a \in I$ and $r \in R$, $ra \in I$.

when I is an ideal, $R/I = \{a+I \mid a \in R\}$ is a ring

$$(a+I) + (b+I) = (a+b) + I$$

$$(a+I)(b+I) = ab + I$$

Defn: An ideal P of R is a prime ideal if $P \neq R$

and if $rs \in P$, then $r \in P$ or $s \in P$

Defn: An ideal M is maximal ideal if $M \neq R$

and for any ideal I , such that $M \subseteq I \subseteq R$

either $I = M$ or $I = R$

ex: $R = \mathbb{Z}$, then $n\mathbb{Z}$ is an ideal of \mathbb{Z}

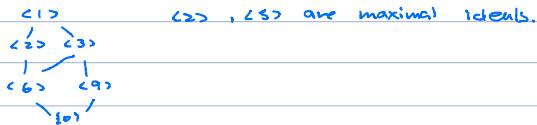
$n\mathbb{Z}$ is a prime ideal when n is prime

If $k \in \mathbb{Z}$ either $k \in p\mathbb{Z}$ or $\mathbb{Z} \in p\mathbb{Z}$

$p\mathbb{Z}$, p prime is a maximal ideal in \mathbb{Z}

If $3\mathbb{Z} \subseteq k\mathbb{Z}$, $k=3$ or $k=1$

Ex: Lattice of ideals of $\mathbb{Z}/18$



Theorem: Let R be a commutative ring with 1 ,

Suppose I an ideal of R . then I is a prime ideal iff R/I is an integral domain.

pf: Suppose I is a prime ideal

$$\text{suppose } (a+I)(b+I) = I \Rightarrow (ab+I) = I \Rightarrow ab \in I$$

Since I is a prime ideal, $a \in I$ or $b \in I$.

$$\text{so } a+I = I \text{ or } b+I = I$$

therefore R/I has no zero divisors. So its a integral domain.

Conversely: Suppose R/I is an integral domain

$$\text{suppose } ab \in I, \text{ then } (a+I)(b+I) = ab+I = I$$

since R/I is an integral domain,

$$a+I = I \text{ or } b+I = I, \text{ so } a \in I \text{ or } b \in I$$

therefore I is a prime ideal.

Theorem: Let M be an ideal of a commutative ring R .

then M is maximal iff R/M is a field.

ex: $\mathbb{R}[x]/\langle x^2 + 1 \rangle \cong \mathbb{C}$ a field.

so $\langle x^2 + 1 \rangle$ is a maximal ideal in $\mathbb{R}[x]$

11.18.19

15 Ring Homomorphisms

Let R and R_1 be rings, $\varphi: R \rightarrow R_1$ is a ring homomorphism

$$\text{if } a, b \in R \quad 1) \quad \varphi(a+b) = \varphi(a) + \varphi(b)$$

$$2) \quad \varphi(ab) = \varphi(a)\varphi(b)$$

$$3) \quad \varphi(1_R) = 1_{R_1}$$

ex: 1) canonical map $R \rightarrow R/I$, $r \mapsto r+I$, I an ideal of R .

2) natural homomorphism $\mathbb{Z} \rightarrow \mathbb{Z}_n$, $k \mapsto [k]$

3) R a ring $\varphi: R[x] \rightarrow R$, $\varphi(a_0 + a_1x + \dots + a_nx^n) = a_0$

Properties of Ring homomorphisms

Theorem: Let $\varphi: R \rightarrow R_1$ be a ring homomorphism and $r \in R$.

$$\text{then } 1) \quad \varphi(0) = 0$$

$$2) \quad \varphi(-r) = -\varphi(r)$$

$$3) \quad \varphi(kr) = kr \quad k \in \mathbb{Z}$$

$$4) \quad \varphi(r^n) = (\varphi(r))^n, \quad n \geq 0 \quad n \in \mathbb{Z}$$

$$5) \quad \text{If } u \in R^\times, \quad \varphi(u^{-1}) = \varphi(u)^{-1} \quad u \in R$$

Theorem: Let $\varphi: R \rightarrow R_1$ be a ring homomorphism.

1) If S is a subring of R , then $\varphi(S)$ is a subring of R_1 .

2) If I is an ideal of R and φ is onto then $\varphi(I)$ is an ideal of R_1 .

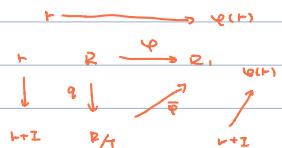
3) $\ker \varphi = \{r \in R \mid \varphi(r) = 0\}$ is an ideal of R .

Corollary: Let I be an ideal of R , then I is the kernel of the

canonical map $R \rightarrow R/I$, $r \mapsto r+I$

Isomorphism Theorem for Rings

Let $\varphi: R \rightarrow R_1$ be a ring homomorphism with $I = \ker \varphi$, then φ induces the isomorphism of rings $\bar{\varphi}: R/I \rightarrow \varphi(R)$ where $\bar{\varphi}(r+I) = \varphi(r)$



Corollary: If $\varphi: R \rightarrow S$ is an onto ring homomorphism with $\ker \varphi = I$,

then I is an ideal of R and $R/I \cong S$

ex: R a ring, $R[x] = \{a_0 + a_1x + \dots + a_nx^n \mid a_i \in R\}$

$$\langle x \rangle = R[x]x = \{x \cdot f(x) \mid f(x) \in R\}$$

Define $\varphi: R[x] \rightarrow R$ by $\varphi(a_0 + a_1x + \dots + a_nx^n) = a_0$

then φ is an onto ring homomorphism with kernel.

$$\ker \varphi = \{a_0 + a_1x + \dots + a_nx^n \mid a_0 = 0\} = \langle x \rangle$$

By the isomorphism theorem of ring

$$R/I \cong R$$

taking $R = \mathbb{Z}$, we get $\mathbb{Z}[x] / \langle x \rangle \cong \mathbb{Z}$
↳ prime, not maximal bc, \mathbb{Z} not a field.

• R/I is an integral domain $\Leftrightarrow I$ is a prime ideal $ab \in I \Rightarrow a \in I$ or $b \in I$

• R/I is an field $\Leftrightarrow I$ maximal ideal $I \subseteq J \subseteq R$, $J = I$ or $J = R$

every field is an integral domain, every maximal ideal is a prime ideal.

Theorem: Let R be a ring with \mathbb{Z} , then

$\mathbb{Z} \cdot 1_R = \{k \cdot 1_R \mid k \in \mathbb{Z}\}$ is a subring of R .

1) If $\text{char } R = n > 0$, then $\mathbb{Z} \cdot 1_R \cong \mathbb{Z}_n$

2) If $\text{char } R = 0$, then $\mathbb{Z} \cdot 1_R \cong \mathbb{Z}$

every ring contains \mathbb{Z}_n or \mathbb{Z} as a subring

Proof: Define $\varphi: \mathbb{Z} \rightarrow R$ by $\varphi(k) = k \cdot 1_R$

φ is an ring homomorphism with its $\text{Im } \varphi: \varphi(\mathbb{Z}) = \mathbb{Z} \cdot 1_R$

$\ker \varphi: \{k \in \mathbb{Z} \mid k \cdot 1_R = 0\}$

If $\text{char } R = n$, then $\ker \varphi = n\mathbb{Z}$, so $\mathbb{Z}_n \subseteq \mathbb{Z}/n\mathbb{Z} \cong \mathbb{Z} \cdot 1_R$

If $\text{char } R = 0$, then $\ker \varphi = 0$, so $\mathbb{Z} \cong \mathbb{Z}/0\mathbb{Z} \cong \mathbb{Z} \cdot 1_R$

Corollary: Let F be a field, If $\text{char } F = p$, prime.

then F contains a subfield isomorphic to \mathbb{Z}_p .

If $\text{char } F = 0$, then F contains a subfield isomorphic to \mathbb{Q} , rational numbers.

$$\mathbb{Q} \subseteq R \subseteq \mathbb{C} \quad R = \left\{ \frac{m}{n} \mid m, n \in \mathbb{Z}, n \neq 0 \right\}$$

Exam: give how the domain of finite order

big, ideals, homomorphism

11/20/19

1) a) $\varphi(7) = 7 \varphi(1) = 7 = 21$

$$\varphi(1) = 3$$

$$\varphi(x) = 3x$$

b) $\text{im } \varphi = \{0, 3, 6, 9, 12\}$

c) $\ker \varphi: \{x \in \mathbb{Z}_{20} \mid \varphi(x) = 0\}$

$$\ker \varphi = \{0, 5, 10, 15, 20, 25, 30, 35, 40, 45\}$$

d) $\varphi^{-1}(3)$

$$\varphi(x) = 3x = 3 \text{ in } \mathbb{Z}_{15} \quad x \in \{1, 6, 11, 16, 21, 26, 31, 36, 41, 46\} = \varphi^{-1}(3)$$

2) a) $108 = 2^2 \cdot 3^4$

$$\mathbb{Z}_4 \oplus \mathbb{Z}_{27} \cong \mathbb{Z}_{108} \leftarrow$$

$$\mathbb{Z}_2 \oplus \mathbb{Z}_2 \oplus \mathbb{Z}_{27} \cong \mathbb{Z}_2 \oplus \mathbb{Z}_{54} \leftarrow$$

$$\mathbb{Z}_4 \oplus \mathbb{Z}_3 \oplus \mathbb{Z}_3 \oplus \mathbb{Z}_2 \cong \mathbb{Z}_3 \oplus \mathbb{Z}_3 \oplus \mathbb{Z}_{12}$$

$$\mathbb{Z}_2 \oplus \mathbb{Z}_2 \oplus \mathbb{Z}_3 \oplus \mathbb{Z}_9 \cong \mathbb{Z}_6 \oplus \mathbb{Z}_{18}$$

$$\mathbb{Z}_2 \oplus \mathbb{Z}_2 \oplus \mathbb{Z}_3 \oplus \mathbb{Z}_3 \oplus \mathbb{Z}_3 \cong \mathbb{Z}_3 \oplus \mathbb{Z}_6 \oplus \mathbb{Z}_6$$

b) \mathbb{Z}_{108} has $\{0, 36, 72\}$

$$\mathbb{Z}_2 \oplus \mathbb{Z}_{54} \text{ has } \{(0, 0), (0, 18), (0, 36)\}$$

3) $S = \{a + a\sqrt{-1} \mid a \in \mathbb{R}\}$ is a subring.

Subring test $0 = a \cdot 0 \cdot a \in S$

$$1 = a \cdot 1 \cdot a = a^2 = 1 \in S$$

Suppose $a + a\sqrt{-1}, b + b\sqrt{-1} \in S$

$$(a + a\sqrt{-1})(b + b\sqrt{-1}) = ab + (a + b)\sqrt{-1} \in S$$

$$(a+r)(a+ra) = a + ra^2 + r^2a \in S$$

$$-ra = a(-r) \in S$$

by the subring test S is a subring of R

4) a) In \mathbb{Z}_7 , $7 \cdot 1 = 0$ and 7 is the smallest such positive integer

$$\text{char } \mathbb{Z}_7(\mathbb{Z}) = 7$$

b) take $a+b\sqrt{3} \neq 0$ in $\mathbb{Z}_7(\mathbb{Z})$

$$1^2 = 1, \quad 2^2 = 4, \quad 3^2 = 2, \quad 4^2 = 2, \quad 5^2 = 4, \quad 6^2 = 1.$$

$$16 \notin \mathbb{Z}_7$$

so if $a+b\sqrt{3} \neq 0$ then $a+b\sqrt{3} \neq 0$

$$\frac{1}{a+b\sqrt{3}} \cdot \frac{a+b\bar{3}}{a+b\bar{3}} = \frac{a-b\bar{3}}{a^2 - 3b^2} = \frac{a}{a^2 - 3b^2} - \frac{b}{a^2 - 3b^2}\bar{3}$$

$$a^2 - 3b^2 \neq 0 \text{ since } \bar{3} \in \mathbb{Z}_7$$

5) a) $(IJ, +) \subseteq (R, +)$

$$(a_1b_1 + a_2b_2 + \dots + a_nb_n) + (c_1b_1' + c_2b_2' + \dots + c_nb_n') = a_1b_1 + a_2b_2 + \dots + a_nb_n + \dots + a_nb_n' \in IJ$$

$$0 \in I, \quad 0 \in J, \quad 0 \in IJ$$

$$-(a_1b_1 + a_2b_2 + \dots + a_nb_n) = -a_1b_1 + (-a_2)b_2 + \dots + (-a_n)b_n \in IJ$$

Now let $r \in R$. Since I an ideal.

$$r(a_1b_1 + a_2b_2 + \dots + a_nb_n) = (ra_1)b_1 + (ra_2)b_2 + \dots + (ra_n)b_n \in IJ$$

therefore IJ an ideal of R .

$$b) IJ \subseteq I \cap J$$

$$\text{let } a_1b_1 + \dots + a_nb_n \in IJ \text{ since } I \text{ ideal } a_ib_i \in I$$

$$\text{since } J \text{ ideal, } a_ib_i \in J$$

$$(I \cap J, +) \subseteq (R, +), \text{ so } a_1b_1 + \dots + a_nb_n \in I \cap J$$

$$6) R = \mathbb{Z}(i) = \{m+n; m, n \in \mathbb{Z}\}$$

$$I = \langle 1+2i \rangle$$

$$R/I = \mathbb{Z}(i)/\langle 1+2i \rangle = \{m+ni + \langle 1+2i \rangle \mid m, n \in \mathbb{Z}\}$$

$$3+1 = (1+2i)(1-i) \in \langle 1+2i \rangle = I$$

$$\text{so in } R/I, 3+1 = 0 \text{ hence } i = -3$$

$$R/I = \{(m-3n) + \langle 1+2i \rangle \mid m, n \in \mathbb{Z}\}$$

$$= \{k + \langle 1+2i \rangle \mid k \in \mathbb{Z}\}$$

$$\text{Also in } R/I, 1+2i = 0$$

$$2i = -1$$

$$-4 = 1 \quad \text{so} \quad 5 = 0$$

$$R/I = 2\mathbb{Z}, 1+\mathbb{Z}, 2+\mathbb{Z}, 3+\mathbb{Z}, 4+\mathbb{Z} \quad (\text{since } 5 = 0)$$

$$\cong \mathbb{Z}_5$$

8) Define map $\varphi: \mathbb{Z}(i) \rightarrow \mathbb{Z}_3(i)$

by $\varphi(m+ni) = \bar{m} + \bar{n}i$, m, n reduce mod 3

then φ is an onto ring homomorphism

$\mathbb{Z}(i) \rightarrow \mathbb{Z}_3$ is a ring homomorphism with kernel $\ker \varphi = 3\mathbb{Z}(i) = \{3m+3ni \mid m, n \in \mathbb{Z}\}$

so $\ker \varphi = 3\mathbb{Z}(i)$ is an ideal

Since $\varphi: \mathbb{Z}(i) \rightarrow \mathbb{Z}_3(i)$ is an onto ring homomorphism with $\ker \varphi = 3\mathbb{Z}(i)$

by the isomorphism theorem $\mathbb{Z}(i)/3\mathbb{Z}(i) \cong \mathbb{Z}_3(i)$

Ring of Polynomials over R $R[x] = \{a_0 + a_1x + a_2x^2 + \dots + a_nx^n \mid a_i \in R\}$

in the indeterminate x . $f(x) = a_0 + a_1x + a_2x^2 + \dots$

$$g(x) = b_0 + b_1x + b_2x^2 + \dots$$

$$f(x) + g(x) = a_0 + b_0 + (a_1 + b_1)x + (a_2 + b_2)x^2 + \dots$$

$$fg(x) = (a_0 + a_1x + \dots)(b_0 + b_1x + \dots) = a_0b_0 + (a_0b_1 + a_1b_0)x + (a_0b_2 + a_1b_1 + a_2b_0)x^2 + \dots$$

In general, the coefficient of x^k in $fg(x)$ is $a_0b_0 + a_1b_{k-1} + \dots + a_{k-1}b_1 + a_kb_0 = \sum_{i+j=k} a_i b_j$

Theorem: Let R be an integral domain

1) Then $R[x]$ is an integral domain

2) If $f(x) \neq 0$ and $g(x) \neq 0$ in $R[x]$, then $\deg(fg(x)) = \deg(f(x)) + \deg(g(x))$

3) The units in $R[x]$ are the units in R

Proof: Let $f(x) = a_0 + a_1x + a_2x^2 + \dots$ $g(x) = b_0 + b_1x + b_2x^2 + \dots$ where $a_0 \neq 0, b_0 \neq 0$

$$fg(x) = a_0b_0 + (a_0b_1 + a_1b_0)x + \dots + a_nb_0x^{n+m}$$

Since R is a domain and $a_0 \neq 0, b_0 \neq 0$ then $a_0b_0 \neq 0$, $fg(x) \neq 0$

Hence $R[x]$ is an integral domain. Furthermore $\deg(fg(x)) = n+m = \deg(f(x)) + \deg(g(x))$

For 3), suppose $f(x) \in R[x]^*$, then $f(x)g(x) = 1$ for some $g(x) \in R[x]$

$$\text{so } \deg(fg(x)) = \deg(f(x)) + \deg(g(x))$$

$$\deg 1 = \deg f + \deg g$$

$$0 = \deg f + \deg g$$

Hence $f(x) \in R$, so $R[x]^* \subseteq R^*$, clearly $R^* \subseteq R[x]^*$

Ex: $R = \mathbb{Z}_4$ not an integral domain b/c has zero divisor. $2 \cdot 2 = 4$,

$$f(x) = 1 + 2x \in \mathbb{Z}_4[x] \quad f(x)^2 = (1+2x)^2 = 1 + 4x + 4x^2 = 1$$

$(1+2x)$ is a unit in $\mathbb{Z}_4[x]$ selfinverse,

then is not a unit in \mathbb{Z}_4 , $\mathbb{Z}_4 = \{0, 1, 2, 3\}$

$$\deg(f(x)f(x)) = \deg 1 = 0 \neq \deg f + \deg f = 2$$

And $(2x)^2 = 0$ in $\mathbb{Z}_4[x]$, so $2x$ is a zero divisor in $\mathbb{Z}_4[x]$, so not integral domain.

Theorem: Division Algorithm. Let R be a commutative ring and suppose $f(x), g(x) \in R[x]$

Suppose $f(x) \neq 0$, and the leading coefficient of $f(x)$ is a unit in R , then there exists polynomials $q(x)$ and $r(x)$ such that

$$1) g(x) = q(x)f(x) + r(x)$$

$$2) \text{either } r(x) = 0 \text{ or } \deg(r(x)) < \deg(f(x))$$

$$\text{Ex: } f(x) = x^2 + x + 2 \quad g(x) = x^5 + 2x^4 + x^3 + x + 4 \quad \text{in } \mathbb{Z}_7[x]$$

$$\begin{array}{r} x^3 + x^2 + 4x + 2 \\ x^2 + x + 2 \quad | \quad x^5 + 2x^4 + x^3 + x + 4 \\ \underline{x^5 + x^4 + 2x^3} \\ x^4 + 5x^3 + x^2 + x + 4 \\ \underline{x^4 + x^3 + 2x^2} \\ 4x^3 + 6x^2 + x + 4 \\ \underline{4x^3 + 4x^2 + x} \\ 2x^2 + 4 \\ \underline{2x^2 + 2x + 4} \\ 5x \end{array}$$

$$g(x) = q(x)f(x) + r(x)$$

$$x^5 + 2x^4 + x^3 + x + 4 = (x^3 + x^2 + 4x + 2)(x^2 + x + 2) + 5x$$

12/21/9

Exam Three

$$1. a) \varphi((a_1, b_1) + (a_2, b_2)) = \varphi(a_1, b_1) + \varphi(a_2, b_2)$$

$$\text{we have } \varphi(a_1 + a_2, b_1 + b_2) = (a_1 + a_2) - (b_1 + b_2) = (a_1 - b_1) + (a_2 - b_2) = \varphi(a_1, b_1) + \varphi(a_2, b_2)$$

$$b) \text{Im } \varphi = ?$$

Let $a \in \mathbb{Z}$, then $\varphi(a, 0) = a - 0 = a$ φ is onto.

$$\text{so } \text{Im } \varphi = \mathbb{Z}$$

$$c) \ker \varphi = ?$$

$$\varphi(a, b) = a - b = 0 \quad a = b$$

$$\ker \varphi = \{(a, b) \in \mathbb{Z} \oplus \mathbb{Z} \mid a = b\}$$
$$= \{(a, a) \mid a \in \mathbb{Z}\}$$

$$d) \varphi(a, b) = a - b = 3 \quad b = a - 3$$

$$\varphi^{-1}(3) = \{(a, a-3) \mid a \in \mathbb{Z}\}$$

$$2. a) 3300 = 2^2 \cdot 3 \cdot 5^2 \cdot 11$$

$$\mathbb{Z}_4 \oplus \mathbb{Z}_3 \oplus \mathbb{Z}_{25} \oplus \mathbb{Z}_{11} \cong \mathbb{Z}_{3300}$$

$$\mathbb{Z}_2 \oplus \mathbb{Z}_2 \oplus \mathbb{Z}_3 \oplus \mathbb{Z}_{25} \oplus \mathbb{Z}_{11} \cong \mathbb{Z}_2 \oplus \mathbb{Z}_{1650}$$

$$\mathbb{Z}_4 \oplus \mathbb{Z}_3 \oplus \mathbb{Z}_5 \oplus \mathbb{Z}_5 \oplus \mathbb{Z}_{11} \cong \mathbb{Z}_5 \oplus \mathbb{Z}_{660}$$

$$\mathbb{Z}_2 \oplus \mathbb{Z}_2 \oplus \mathbb{Z}_3 \oplus \mathbb{Z}_5 \oplus \mathbb{Z}_5 \oplus \mathbb{Z}_{11} \cong \mathbb{Z}_6 \oplus \mathbb{Z}_{330}$$

$$b) \ln \mathbb{Z}_{3300}, \langle 10 \rangle$$

$$\ln \mathbb{Z}_2 \oplus \mathbb{Z}_{1650}, \langle (0, 5) \rangle$$

$$\ln \mathbb{Z}_5 \oplus \mathbb{Z}_{660}, \langle (0, 2) \rangle$$

$$\ln \mathbb{Z}_{10} \oplus \mathbb{Z}_{330}, \langle (0, 1) \rangle$$

3. a)

$$b) \text{char } \mathbb{Z}_m \oplus \mathbb{Z}_n = \text{lcm}(m, n)$$

$$\text{char} \left(\begin{smallmatrix} p & q \\ r & s \end{smallmatrix} \right) = \text{lcm}(m, n)$$

$$4. a) \mathbb{Z} \oplus \mathbb{Q} = \{(k, q) \mid k \in \mathbb{Z}, q \in \mathbb{Q}\}$$

$$(k, 0) \cdot (0, q) = (0, 0)$$

zero divisors in $\mathbb{Z} \oplus \mathbb{Q}$ are $\{(k, 0) \text{ or } (0, q) \mid k \in \mathbb{Z}, k \neq 0, q \in \mathbb{Q}, q \neq 0\}$

$$b) \text{units } \mathbb{Z}^\times = \{\pm 1\}$$

$$\text{units in } \mathbb{Z} \oplus \mathbb{Q} = \{(\pm 1, q) \mid q \neq 0, q \in \mathbb{Q}\}$$

$$(\pm 1, q) \cdot (\pm 1, q^{-1}) = (1, 1)$$

$$5. a) \mathbb{Z}_{2i} = \{m + ni \in \mathbb{C} \mid m, n \in \mathbb{Z}\}$$

$$I = \langle 1 + 2i \rangle$$

$$(1+2i)(1-2i) = 10, \text{ so } 10 \in \langle 1+2i \rangle$$

$$\ln R/I, 10 = 0$$

$$(1+2i)(1-2i) = 7+i \quad \text{so} \quad 7+i = 0 \quad i = -7$$

$$R/I = \{m + ni + \langle 1+2i \rangle \mid m + ni \in \mathbb{Z}_{2i}\}$$

$$= \{m - 7n + \langle 1+2i \rangle \mid m, n \in \mathbb{Z}\}$$

$$= \{k + \langle 1+2i \rangle \mid k \in \mathbb{Z}\} \text{ and } 0 = 0$$

$$= \{1, 1+I, 2+I, \dots, 9+I\} \cong \mathbb{Z}_{10}$$

$$b) \text{a)} \varphi: \mathbb{R} \rightarrow \mathbb{Z}$$

$$R = \left\{ \begin{pmatrix} a & b \\ b & a \end{pmatrix} \mid a, b \in \mathbb{Z} \right\}$$

$$\varphi \left(\begin{pmatrix} 1 & 0 \\ 0 & 1 \end{pmatrix} \right) = 1 - 0 = 1$$

$$\varphi \left(\begin{pmatrix} a_1 & b_1 \\ b_1 & a_1 \end{pmatrix} + \begin{pmatrix} a_2 & b_2 \\ b_2 & a_2 \end{pmatrix} \right) = \varphi \left(\begin{pmatrix} a_1+a_2 & b_1+b_2 \\ b_1+b_2 & a_1+a_2 \end{pmatrix} \right) = (a_1+a_2) - (b_1+b_2) = (a_1 - b_1) + (a_2 - b_2) = \varphi \left(\begin{pmatrix} a_1 & b_1 \\ b_1 & a_1 \end{pmatrix} \right) + \varphi \left(\begin{pmatrix} a_2 & b_2 \\ b_2 & a_2 \end{pmatrix} \right)$$

$$\varphi \left(\begin{pmatrix} a_1 & b_1 \\ b_1 & a_1 \end{pmatrix} \begin{pmatrix} a_2 & b_2 \\ b_2 & a_2 \end{pmatrix} \right) = \varphi \left(\begin{pmatrix} a_1a_2 + b_1b_2 & a_1b_2 + b_1a_2 \\ b_1a_2 + a_1b_2 & b_1b_2 + a_1a_2 \end{pmatrix} \right) = a_1a_2 + b_1b_2 - a_1b_2 + b_1a_2 = (a_1 - b_1)(a_2 - b_2)$$

$$= \varphi \left(\begin{pmatrix} a_1 & b_1 \\ b_1 & a_1 \end{pmatrix} \right) \cdot \varphi \left(\begin{pmatrix} a_2 & b_2 \\ b_2 & a_2 \end{pmatrix} \right)$$

$$b) \ker \varphi = \left\{ \begin{pmatrix} a & 0 \\ 0 & a \end{pmatrix} \mid a \in \mathbb{Z} \right\}$$

$$c) \text{Given } a \in \mathbb{Z}, \varphi \left(\begin{pmatrix} a & 0 \\ 0 & a \end{pmatrix} \right) = a - 0 = a$$

φ is an onto ring homomorphism with $\ker \varphi$.

so by the isomorphism theorem.

$$R/\ker \varphi \cong \mathbb{Z}$$

d) $R/\ker \varphi \cong \mathbb{Z}$, and the integral domain, so $\ker \varphi$ is prime.

$R/\ker \varphi \cong \mathbb{Z}$, \mathbb{Z} is not a field, so $\ker \varphi$ is not maximal.

16. Polynomial Rings.

R commutative ring with 1. $R[x] = \{a_0 + a_1x + a_2x^2 + \dots + a_nx^n \mid a_i \in R\}$

$$1+x+x^3, x+x^2 \in \mathbb{Z}_2[x]$$

$$(1+x+x^5) + (x+x^4) = 1+2x+x^2+x^3 = 1+x^2+x^3$$

The division algorithm theorem:

Let $f(x), g(x) \in R[x]$

Suppose $f(x) \neq 0$, and the leading coefficient of $f(x)$ is a unit in R .

then there exists $q(x), r(x) \in R[x]$

such that 1) $g(x) = q(x)f(x) + r(x)$

2) either $r(x)=0$ or $\deg r(x) < \deg f(x)$

Terminology: We say $g(x)$ divides $f(x)$ if $f(x) = g(x)h(x)$

We call $g(x)$ a factor of $f(x)$

For $f(x) = b_0 + b_1x + b_2x^2 + \dots + b_nx^n \in R[x]$

if $a \in R$, $f(a) = b_0 + b_1a + b_2a^2 + \dots + b_na^n$ is evaluation of f at a

We say $a \in R$ is a zero or root of $f(x)$ if $f(a)=0$

A root a has multiplicity $m \geq 1$ if $f(x) = (x-a)^m h(x)$ where $h(a) \neq 0$

Remainder Theorem: If $f(x)$ is divided by $x-a$, then the remainder is $f(a)$.

by the division algorithm, $f(x) = (x-a)q(x) + r(x)$, $\deg r(x)=0$, $r(x) = r$ constant.

$$f(a) = r(a) = r$$

12/4/19

The division algorithm and its consequences

R commutative ring with 1

Division algorithm: Let $f(x), g(x)$ with $f(x) \neq 0$ and suppose the leading coefficient of $f(x)$ is a unit. Then there exists unique $q(x), r(x) \in R[x]$

so that: 1) $g(x) = f(x)q(x) + r(x)$

2) either $r(x)=0$ or $\deg r(x) < \deg f(x)$

Theorem (Factor theorem)

Let $f(x) \in R[x]$ and $a \in R$

then $f(a)=0$ (a is a root of $f(x)$)

iff $f(x) = (x-a)h(x)$ for some $h(x) \in R[x]$ (that is $x-a$ is a factor of $f(x)$)

pf: esp. $f(a)=0$ by the division algorithm, $f(x) = (x-a)h(x) + r(x)$

where $\deg r(x)=0$ so $r(x)=c$ so $f(x) = (x-a)h(x) + c$ with $c = f(a) = 0$

hence $f(x) = (x-a)h(x)$

conversely, if $f(x) = (x-a)h(x)$, then $f(a)=0$.

Theorem: Let R be an integral domain and sps $f(x) \in R[x]$ with $\deg f(x)=n$.

then $f(x)$ has at most n roots in R

Pf: by induction on $n = \deg f(x)$

For $n=1$, $f(x) = a_0 + a_1x$, $a_1 \neq 0$

$$\text{Sps } f(b) = a_0 + a_1b = 0 = a_0 + a_1c = f(c)$$

$$a_1b = a_1c \Rightarrow a_1(b-c) = 0$$

since $a_1 \neq 0$. R an integral domain, so $b=c$

For the inductive step. sps $\deg f(x) = n$ & $f(a) = 0$

By the factor theorem, $f(x) = (x-a)f(x)$

so since R an integral domain, $\deg f(x) = n-1$

By induction, $f(x)$ has at most $n-1$ roots,

therefore $f(x)$ has at most n roots.

17 Factorization of Polynomials.

F a field.

Definition: sps $p(x) \in F[x]$, $\deg p(x) \geq 1$, we say $p(x)$ is irreducible if $p(x) \neq f(x)g(x)$

where $\deg f(x), \deg g(x) < \deg p(x)$

Equivalently, we say $p(x)$ is irreducible if $p(x) = f(x)g(x)$

implies $\deg f(x) = 0$ OR $\deg g(x) = 0$

Ex: (1) $f(x) = 2x^2 + 4$ is irreducible over R .

$$f(x) = 2(x^2 + 2) = 2(x + i\sqrt{2})(x - i\sqrt{2}) \text{ reducible over } C$$

(2) $f(x) = x^2 - 2$ irreducible over Q

$$= (x - \sqrt{2})(x + \sqrt{2}) \text{ reducible over } R.$$

(3) $f(x) = x^2 + 1$ irreducible over Z_3

$$= x^2 + 1 = (x-2)(x-3) \text{ reducible over } Z_5$$

$$x^2 - 3x - 2x + 6 = x^2 - 5x + 6$$

Proposition: If F is a field, then every linear polynomials is irreducible over F .

Pf: sps $\deg p(x) = 1$, if $p(x) = f(x)g(x)$ then $\deg p(x) = 1 = \deg f(x) + \deg g(x)$

so $\deg f(x) = 0$ or $\deg g(x) = 0$, hence $p(x)$ irreducible.

Theorem: sps $p(x) \in F[x]$ with $\deg p(x) \geq 2$.

(1) If $p(x)$ irreducible over F , then $p(x)$ has no root in F .

(2) If $\deg p(x) = 2$ or 3 , then $p(x)$ is irreducible iff it has no root in F .

Pf. (1) If $p(x) \neq 0$, then $p(x) = (x-a)f(x)$ by the factor theorem.

so $p(x)$ is not irreducible.

(2) sps $p(x)$ has no root in F

If $p(x) = f(x)g(x)$. then $f(x), g(x)$ have no roots in F .

so $\deg f(x)$ and $\deg g(x) \neq 1$

since $\deg p(x) = \deg f(x) + \deg g(x) = 2$ or 3

either $\deg f(x) = 0$ or $\deg g(x) = 0$.

Ex. (1) $p(x) = x^3 + 3x^2 + x + 2 \in Z_5[x]$

$p(0) = 2$, $p(1) = 2$, $p(2) = 4$, $p(3) = 4$, $p(4) = 3$ $p(x)$ has no root, so irreducible over Z_5 .

(2) $p(x) = x^4 + 3x^2 + 2$

$$= (x^2 + 1)(x^2 + 2) \text{ reducible in } R[x] \text{ but has no root in } R.$$

Theorem: If $f(x) \in Z[x]$, if $f(x)$ is reducible over Q , then it is reducible over Z

$$\text{Ex: } f(x) = (3x - \frac{9}{2})(4x + \frac{8}{3})$$

$= 12x^2 - 10x - 12 \in \mathbb{Z}[x]$ is reducible over \mathbb{Q}

$$12x^2 - 10x - 12 = (2x-3)(6x+4) \quad f(x) \text{ is reducible over } \mathbb{Z}$$

12/6/19

Theorem (Rational Roots Theorem)

Let $f(x) = a_n x^n + a_{n-1} x^{n-1} + \dots + a_1 x + a_0 \in \mathbb{Z}[x]$ where $a_n, a_0 \neq 0$,

let c/d be a root of $f(x)$ expressed in lowest terms ($\Rightarrow \gcd(c, d) = 1$)

then $c | a_0$ and $d | a_n$.

$$\text{Ex: } f(x) = 4x^4 + x^3 - 3x^2 + 4x - 3 \in \mathbb{Z}[x]$$

$\pm 1, \pm 3$ divides 3 and $\pm 1, \pm 2, \pm 4$ divides 4

By the rational roots theorem, the possible rational roots of $f(x)$ are

$$\pm 1, \pm \frac{1}{2}, \pm \frac{1}{4}, \pm 3, \pm \frac{3}{2}, \pm \frac{3}{4}$$

$$f\left(\frac{3}{4}\right) = 81/64 + 27/16 - 27/4 + 3 - 3 = 108/64 - 108/64 = 0 \quad \text{thus } (x - \frac{3}{4}) \text{ is a factor of } f(x).$$

$$x - \frac{3}{4} \mid 4x^4 + x^3 - 3x^2 + 4x - 3 \quad \text{so } f(x) = (x - \frac{3}{4})(4x^3 + 4x^2 + 4)$$

$$4x^3 + 4x^2 + 4 \quad = (4x - 3)(x^2 + x^2 + 1)$$

$$4x^4 - 3x^3$$

$$4x^3 - 3x^2$$

$$4x^2 - 3x$$

$$4x - 3$$

$$0$$

$$x^2 + x^2 + 1 : \text{possible rational roots } \pm 1$$

Hence, irreducible over \mathbb{Q} .

$f(x)$ reducible over $\mathbb{Z}[x]$

Theorem (Modular irreducibility test)

Let $f(x) \in \mathbb{Z}[x]$, s.t. prime p exists

such that (1) p does not divide the leading coefficient of $f(x)$

(2) the reduction $\bar{f}(x)$ modulo p is irreducible in $\mathbb{Z}_p[x]$

then $f(x)$ is irreducible in $\mathbb{Q}[x]$

$$\text{Ex: } f(x) = x^3 + 4x^2 + 6x + 2 \quad \text{we show } f(x) \text{ is irreducible in } \mathbb{Q}[x]$$

Reduce mod 3 to obtain $\bar{f}(x) = x^3 + x^2 + 2 \in \mathbb{Z}_3[x]$

$$\bar{f}(0) = 2, \quad \bar{f}(1) = 1, \quad \bar{f}(2) = 2$$

Eisenstein Criterion,

Let $f(x) = a_n x^n + a_{n-1} x^{n-1} + \dots + a_1 x + a_0 \in \mathbb{Z}[x]$

s.t. \exists a prime p such that (1) p divides each of a_0, a_1, \dots, a_{n-1}

(2) $p \nmid a_n$ and $p^2 \nmid a_0$

then $f(x)$ is irreducible over \mathbb{Q} .

$$\text{Ex: } f(x) = 2x^5 + 27x^3 - 18x + 12$$

$$\text{let } p = 3, \quad 3 \mid 27, \quad 3 \mid -18, \quad 3 \mid 12, \quad 3 \nmid 2 \quad 3^2 = 9 \nmid 12$$

By the Eisenstein criterion, $f(x)$ is irreducible over \mathbb{Q}

12/9/19

Final Exam Review

1) a) Divisors of 15 are 1, 3, 5, 15

$$\begin{array}{c} \mathbb{Z}_{15} \\ \swarrow \quad \searrow \\ \langle 3 \rangle \quad \langle 5 \rangle \\ \downarrow \quad \downarrow \\ \langle 15 \rangle \end{array}$$

b) $\mathbb{Z}_{15}^* = \{1, 2, 4, 7, 8, 11, 13, 14\}$ is an abelian group of order 8.

therefore it is isomorphic to \mathbb{Z}_8 . $\mathbb{Z}_2 \oplus \mathbb{Z}_4$, $\mathbb{Z}_2 \oplus \mathbb{Z}_2 \oplus \mathbb{Z}_2$

We look at the order of the elements

$$2^2 = 4, 2^3 = 8, 2^4 = 16 = 1 \quad \text{so } 12 \nmid 4$$

$\therefore \mathbb{Z}_8 \not\cong \mathbb{Z}_2 \oplus \mathbb{Z}_2 \oplus \mathbb{Z}_2$

Note $\mathbb{Z}_8 = \langle 1 \rangle = \langle 3 \rangle = \langle 5 \rangle = \langle 7 \rangle$

$$4^2 = 16 = 1 \quad |4| = 2$$

$$7^2 = 49 = 4 \quad |7| = 4$$

$$8^2 = 64 = 4 \quad |8| = 4 \quad \text{that leaves } 11, 13, 14 \in \mathbb{Z}_8^2$$

\mathbb{Z}_8 must contain 4 elements of order 8. $\therefore \mathbb{Z}_8 \not\cong \mathbb{Z}_2 \oplus \mathbb{Z}_4$

We conclude that $\mathbb{Z}_{15} \not\cong \mathbb{Z}_2 \oplus \mathbb{Z}_4$

c) $H = \langle 5 \rangle = \langle 10, 5, 10 \rangle$

$$1+H = \{1, 6, 11\} \quad 2+H = \{2, 7, 12\}$$

$$3+H = \{3, 8, 13\} \quad 4+H = \{4, 9, 14\}$$

$$\text{Index } |\mathbb{G}/H| = 5 = |\mathbb{G}|/|H| = 15/3$$

d) $\mathbb{G}/H = \{H, 1+H, 2+H, 3+H, 4+H\} \cong \mathbb{Z}_5$

$$\mathbb{G}/H = \langle 1+H \rangle \cong \mathbb{Z}_5$$

e) Any homomorphism $\varphi: \mathbb{Z}_9 \rightarrow \mathbb{Z}_{15}$ is determined by $\varphi(1)$

$1\varphi(1)$ will divide 15, so φ is a homomorphism,

$$9\varphi(1) = \varphi(9) = \varphi(0) = 0 \quad \text{therefore } 1\varphi(1) \text{ also divide 9}$$

$$1\varphi(1) \text{ divide 9 and 15, so } |\varphi(1)| = 1 \text{ or } 3$$

The homomorphisms $\varphi: \mathbb{Z}_9 \rightarrow \mathbb{Z}_{15}$ are

$$\varphi(1) = 0 \quad \text{or } \varphi(1) = 0$$

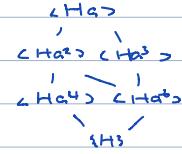
$$\varphi(1) = 5 \quad \varphi(1) = 5k$$

$$\varphi(1) = 10 \quad \varphi(1) = 10k$$

since 5, 10 in \mathbb{Z}_{15} are the only elements of order 3.

$$\mathbb{G}/H = \langle H, Ha \rangle = \{H, Ha, Ha^2, Ha^3, Ha^4\} \cong \mathbb{Z}_{12}$$

proper subgroup of \mathbb{G}/H are $\langle Ha^2 \rangle, \langle Ha^3 \rangle, \langle Ha^4 \rangle, \langle Ha^6 \rangle$



$24 \rightarrow \mathbb{Z}_{10}$ is determined by $\varphi(1)$

1, 2 divided 4 & 10, so $|\varphi(1)| = 1, 2$

$$\varphi(1) = 0 \quad \varphi(1) = 2$$

$$\varphi(1) = 5 \quad \varphi(1) = 5k$$

2. a) Determine all abelian groups up to isomorphism

a) $72 = 8 \cdot 9 = 2^3 \cdot 3^2$

$$\mathbb{Z}_8 \oplus \mathbb{Z}_9 \cong \mathbb{Z}_{72}$$

$$\mathbb{Z}_2 \oplus \mathbb{Z}_4 \oplus \mathbb{Z}_9 \cong \mathbb{Z}_2 \oplus \mathbb{Z}_{36}$$

$$\mathbb{Z}_2 \oplus \mathbb{Z}_2 \oplus \mathbb{Z}_2 \oplus \mathbb{Z}_9 \cong \mathbb{Z}_2 \oplus \mathbb{Z}_2 \oplus \mathbb{Z}_{18}$$

$$\mathbb{Z}_3 \oplus \mathbb{Z}_3 \oplus \mathbb{Z}_3 \cong \mathbb{Z}_3 \oplus \mathbb{Z}_{24}$$

$$\mathbb{Z}_2 \oplus \mathbb{Z}_4 \oplus \mathbb{Z}_3 \oplus \mathbb{Z}_3 \cong \mathbb{Z}_6 \oplus \mathbb{Z}_2$$

$$\mathbb{Z}_2 \oplus \mathbb{Z}_2 \oplus \mathbb{Z}_2 \oplus \mathbb{Z}_3 \oplus \mathbb{Z}_3 \cong \mathbb{Z}_2 \oplus \mathbb{Z}_6 \oplus \mathbb{Z}_6$$

b) How many have exactly three subgroups of order 2?

In \mathbb{Z}_2 , $\langle 3 \rangle$

In $\mathbb{Z}_2 \oplus \mathbb{Z}_{36}$, $\langle 1, 0 \rangle, \langle 1, 18 \rangle, \langle 0, 18 \rangle$ ✓

In $\mathbb{Z}_2 \oplus \mathbb{Z}_2 \oplus \mathbb{Z}_8$, $\langle 1, 0, 0 \rangle, \langle 1, 1, 0 \rangle, \langle 0, 0, 1 \rangle, \langle 0, 1, 0 \rangle$ more than 3

In $\mathbb{Z}_3 \oplus \mathbb{Z}_{24}$, $\langle 0, 12 \rangle$

In $\mathbb{Z}_6 \oplus \mathbb{Z}_{12}$, $\langle 3, 0 \rangle, \langle 0, 6 \rangle, \langle 3, 6 \rangle$ ✓

In $\mathbb{Z}_2 \oplus \mathbb{Z}_6 \oplus \mathbb{Z}_6$, $\langle 1, 0, 0 \rangle, \langle 1, 3, 0 \rangle, \langle 1, 0, 3 \rangle, \dots$ more than 3

4. Consider the ring $R = \mathbb{Z}_2[x]$ and $I = \langle x^2 + 1 \rangle$

a) Describe the cosets in the quotient ring R/I .

$$R/I = \mathbb{Z}_2[x]/\langle x^2 + 1 \rangle = \{ f(x) + \langle x^2 + 1 \rangle \mid f(x) \in \mathbb{Z}_2[x] \}$$

By the division algorithm, $f(x) = g(x)(x^2 + 1) + r(x)$

where $\deg r(x) < 2$, so $r(x) = a_0 + a_1x$

$$r(x) \langle x^2 + 1 \rangle \subseteq \langle x^2 + 1 \rangle = I$$

$$R/I = \{a_0 + a_1x + I \mid a_0, a_1 \in \mathbb{Z}_2\}$$
$$= \{I, 1+I, x+I, 1+x+I\}$$