8/26/2019

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

$\mathbb{Q} = \{ \frac{m}{n} \mid m, n \in \mathbb{Z}, n \neq 0 \}$ $(\mathbb{Q}, +)$ 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: $\{1\}$ $\{1, -1\}$ $\{1, -1, i, -i\}$

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

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

$(a+bi) \cdot (c+di) = ac + adi + bci + bdi^2$

$= (ac - bd) + (ad + bc)i$

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

Abelian groups:

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

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

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

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

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

Determinant:

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

General linear group

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

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

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

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

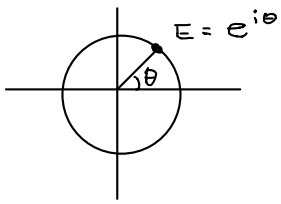
Identity $I = \begin{pmatrix} 1 & 0 \\ 0 & 1 \end{pmatrix}$

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

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

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

Example – Circle group



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

$E_1 \cdot E_2 = e^{i\theta_1} \cdot e^{i\theta_2} = e^{i(\theta_1+\theta_2)}$
$E = e^{i\theta}$, $E^{-1} = e^{-i\theta}$

Example – n^{th} roots of unity

for $n \geq 1$,
let $U_n = \{ E \in S^1 \mid E^n = 1 \}$

$= \left\{ E = e^{\frac{2k\pi i}{n}} \;\middle|\; k = 0, 1, \ldots, n-1 \right\}$

abelian group under complex multiplication.

subgroup of the circle group

$U_1 = \{1\}$
$U_2 = \{1, -1\}$
$\vdots$
$U_4 = \left\{ E = e^{\frac{2k\pi i}{4}} \mid k = 0, 1, 2, 3 \right\}$
$= \left\{ 1, e^{\frac{2\pi i}{4}}, e^{\frac{4\pi i}{4}}, e^{\frac{6\pi i}{4}} \right\}$
$= \{1, i, -1, -i\}$

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

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

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

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

$be = ce$ so $b = c$

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

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

$eb = ec$ 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 $ab = ac$ 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 $x = a^{-1}b$
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 $x = ba^{-1}$
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.

$U_4 = \{1, -1, i, -i\}$
$i^4 = 1$

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

proof: we have that $(ab)(ab)^{-1} = e$
also $(ab)b^{-1}a^{-1} = a(bb^{-1})a^{-1} = aea^{-1} = aa^{-1} = e$
so $(ab)(ab)^{-1} = (ab)(b^{-1}a^{-1})$
by left cancellation,
$(ab)^{-1} = b^{-1}a^{-1}$

Integers module 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

ex: $10 \equiv 4 \pmod 2$ → $10-4=6$

$11 \equiv 17 \pmod 2$

$12 \equiv 7 \pmod 5$ → $12-7=5$

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

proof: **reflextive**: let $a \in \mathbb{Z}$.

we show $a \equiv a \pmod n$

$a-a=0$ and n divides 0

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

so $a \equiv a \pmod n$

symmetry: suppose $a \equiv b \pmod n$,

then n divides $a-b$

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

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

So n divides $b-a$,

therefore $b \equiv a \pmod n$

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

and $b \equiv c \pmod n$

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

$[3] = [0] = [-6] = \cdots$

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

Let n be an equivalence relation on A.

$A/n = \{[a] \mid a \in A\}$ 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: $\mathbb{Z}_3 = \{[0], [1], [2]\} = \{0, 1, 2\}$

$\mathbb{Z}_2 = \{0, 1\}$ $\mathbb{Z}_4 = \{0, 1, 2, 3\}$.

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

Modular Arithmetic

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

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

9/4/2018

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

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

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

cayley table

$(\mathbb{Z}_4, +)$	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 $[a] \cdot [b] \in \mathbb{Z}_n = \{[0], [1] \dots [n-1]\}$

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

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

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

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

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

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

cayley table

$\mathbb{Z}_8^\times$	1	3	5	7
1	1	3	5	7
3	3	1	7	5
5	5	7	1	3
7	7	5	3	1

$2^2 = 4 \quad 2^3 = 8 \quad 2^4 = 16 = 6 \quad 2^5 = 32 = 2$

$\mathbb{Z}_{10}: \quad 4^2 = 16 = 6 \quad 4^3 = 64 = 4 \quad 4^4 = 256 = 6$

$6^2 = 36 = 6 \quad 6^3 = 216 = 6$

$7^2 = 49 \quad 7^3 = 343 = 3 \quad 2401 = 1$

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

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

$\mathbb{Z}_5^\times$	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: $\mathbb{Z}_{10}^\times = \{1, 3, 7, 9\} \quad |\mathbb{Z}_{10}^\times| = 4$

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

the order of element g in a group is the smallest positive integer n st $g^n = e$ (or $ng = 0$ inditive notation) and denoted $|g| = n$. if no such n exists, then g is infinite order. and $|g| = \infty$

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

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

ex: group of units

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

① $8 = -5 \pmod{13}$

② $8^2 = 25 = 12 = -1$

③ $8^4 = (-1)^2 = 1$

④ $|8| = 4$

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.

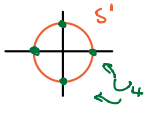
then $\{e\}$ is a subgroup of G called the trivial subgroup.

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 $H \leq G$, then 1, 2 and 3 hold.

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

pf: the identity of $\mathbb{Z}$ is 0,
and $0 = n \cdot 0$ so $0 \in n\mathbb{Z}$.
suppose $a, b \in n\mathbb{Z}$.
$a = nk$, $b = n\ell$, for some $n, \ell \in \mathbb{Z}$.
$a+b = nk + n\ell = n(k+\ell)$, $k+\ell \in \mathbb{Z}$.
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, $n\mathbb{Z} \leq \mathbb{Z}$. ∎

Definition: Let G be a group, the center of G is define by
$Z(G) = \{z \in G \mid zg = gz$ 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:
$eg = ge = g$ for all $g \in G$
So $e \in Z(G)$
Suppose $a, b \in Z(G)$ let $g \in G$.
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 $ag = ga$.
$a^{-1}ag = a^{-1}ga$.
$g = a^{-1}ga$
$ga^{-1} = a^{-1}gaa^{-1}$
$ga^{-1} = a^{-1}g$ 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.

9/9/2019

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 $ab \in H$

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.

the 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 $ab = (h_1k_1)(h_2k_2) = h_1h_2k_1k_2 \in HK$

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: $\Rightarrow$ pos H is closed, (if $a, b \in H$, then $a, b \in H$)

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

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 $h^m = e$.

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

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 $a^\ell \in \langle a \rangle$ and $a^m \in \langle a \rangle$

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

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

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

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

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

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

$\langle 1 \rangle = \mathbb{Z}_n \qquad \langle -1 \rangle = \langle n-1 \rangle \leq \mathbb{Z}_n$

1 and $n-1$ are generator.

9111 | 2019

4 Cyclic Groups

Group G Let $a \in G$

The subgroup

$\langle a \rangle = \{a^n \mid n \in \mathbb{Z}\}$ is the cyclic subgroup of G generated by 4.

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

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

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

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

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

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

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

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

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

- Conversely, if $a^k = e$

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

So $a^r = a^{k-qn} = a^k (a^n)^{-q} = e \cdot e^{-q} = e$

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

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

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

So $\langle a \rangle \leq \{e, a, \ldots a^{n-1}\}$

$\{e, a \ldots a^{n-1}\} \leq \langle a \rangle$

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

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

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

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

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

9/13/2019

4 Cyclic Groups

group G, $a \in G$.

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

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 $\mathbb{Z}_n$.

Theorem: Let G be a group. Let $a \in G$ with $|a| = n$.

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

2) $a^k = a^\ell$ iff $k \equiv \ell \pmod n$

3) $\langle a \rangle = \{e, a, \ldots a^{n-1}\}$, $e, a \ldots a^{n-1}$ are distinct.

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

ex: $\mathbb{Z}_{19}^\times = (\mathbb{Z}_{19} - \{0\}, \cdot)$

Let's show $\mathbb{Z}_{19}^\times$ is cyclic and 2 is a generator

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

$3 \cdot 19 = 57$

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

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

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

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

$2^1 = 2$, $2^2 = 4$. So $n = 18$ since $2^1, 2^2, 2^3, 2^6, 2^9 \neq 1$.

So since $|\langle 2 \rangle| = |2| = 18$

and $\mathbb{Z}_{19}^\times = 18$

then $\mathbb{Z}_{19}^\times = \langle 2 \rangle$, therefore $\mathbb{Z}_{19}^\times$ is cyclic and 2 is a generator.

theorem. Let G be a group, and $a \in G$. with $|a| = \infty$

than 1) $a^k = e$ iff $k = 0$

2) $a^k = a^\ell$ iff $k = \ell$

3) $\langle a \rangle = \{\ldots a^{-2}, a^{-1}, e, a, a^2 \ldots\}$ and elements are distinct.

pf: 1) If $|a| = \infty$, then $a^k = e$ means $k = 0$.

2) If $a^k = a^\ell$. then $a^{k-\ell} = e$ by (1) $k - \ell = 0$ so $k = \ell$

3) $\langle a \rangle = \{a^n \mid n \in \mathbb{Z}\} = \{\ldots a^{-2}, a^{-1}, e, a, a^2 \ldots\}$ so by (2) these elements are distinct.

theorem: Let $\langle a \rangle = \{e, a \ldots a^{n-1}\} = G$ 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 $1, 5$

ex: $\mathbb{Z}_9$ has generators $1, 2, 4, 5, 7, 8$

theorem: (Fundamental theorem of cyclic group)

Let $G = \langle a \rangle = \{e, a, \ldots a^{n-1}\}$ 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 divide 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 $C_n = \{e, a, \ldots a^{n-1}\} = \langle a \rangle$, $a^n = 1$

we call a a generator of C_n.

since $|C_n| = n$, the elements are distinct.

ex: Find all subgroups of C_{12}

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

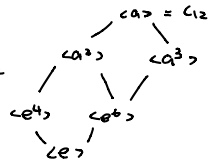
The divisors of 12 are 1, 2, 3, 4, 6, 12

the unique subgroup of each of these orders respectively,

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

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

the Lattice Diagram of subgroup of 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

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

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

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

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

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

$\langle 1 \rangle = \mathbb{Z}_{16}$
|
$\langle 2 \rangle$
|
$\langle 4 \rangle$
|
$\langle 8 \rangle$
|
$\langle 0 \rangle = \{0\}$

9/16/2019

5. Permutation Groups

Let $n \geq 1$ be an integer

A map $\sigma : \{1, 2, \dots n\} \to \{1, 2, \dots n\}$ that is one to one and on to is called a permutation

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

Notation : consider the permutation σ on $\{1, 2, 3, 4\}$ defined by $\sigma(1) = 3$, $\sigma(2) = 1$, $\sigma(3) = 4$ and $\sigma(4) = 2$ we write σ 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 $(\sigma\tau)(k)$ by function composition)

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

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

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

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

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

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

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

we write $\sigma \in S_n$ 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 $\quad |S_3| = 3! = 6$

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

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

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, $\sigma\varepsilon = \varepsilon\sigma = \sigma$.

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

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

Cycle notation:

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

note: τ fixes 5, the layth 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.

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.

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.

$\sigma = \{1, 2 \dots n\} \to \{1, 2 \dots n\}$

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

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

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

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

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

$\sigma = (13)(27)(456)(8)$ $\tau = (1237)(486)(5)$

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

$\sigma\tau = (13)(27)(456)(1237)(486)$ ← cycle notation.

$= (1732)(48)(56)$ ← 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

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

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

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

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

then $(j \quad \sigma(j) \dots \sigma^{r-1}(j))$ which will be disjoint for the previous cycle. until the elements of X are exhausted, we express σ as a product of disjoint cycles.

$\sigma = (i, \sigma(i), \sigma^2(i) \dots \sigma^{m-1}(i))(j \; \sigma(j) \dots \sigma^{r-1}(j)) \dots (k \dots \sigma^{s-1}(k))$

theorem: Disjoint cycles commute.

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

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

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

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

similary for $b_1 \dots b_n$ and any c_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.

$\sigma = (a_1 \; a_2 \dots a_m)$ length m

$\sigma\tau = (a_1 \; a_2 \dots a_m)(b_1 \; b_2 \dots b_n)$ $|\sigma| = m$ $|\tau| = n$ σ, τ disjoint

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

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

A 2-cycle is a transposition

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

Hence every permutation is a product of transpositions.

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

ex: $\sigma = (1 \; 2 \; 3 \; 4 \; 5) = (1 \; 5)(1 \; 4)(1 \; 3)(1 \; 2)$ $|\sigma| = 5$

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

ex: $\tau = \begin{pmatrix} 1 & 2 & 3 & 4 & 5 & 6 & 7 & 8 & 9 \\ 2 & 8 & 6 & 9 & 4 & 7 & 3 & 1 & 5 \end{pmatrix} = (1\,2\,8)(3\,6\,7)(4\,9\,5)$ $|\tau| = 3$

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

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

even # of transp. → τ is even

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

ex: S_5 $|S_5| = 5! = 120$

let n denote a cycle of length n, possible disjoint cycle structures in S_5

(5) order 5

(4)(1) order 4

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

(2)(2)(1) order 2

(3)(1)(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 transportations

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

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

$= (1\,3)(2\,1)$

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

If $\varepsilon = \delta_1 \delta_2 \cdots \delta_r$ where $\delta_1 \delta_2 \cdots \delta_r$ are transportations, 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 $\varepsilon \in A_n$

If $\sigma = \delta_1 \cdots \delta_m$ and $\tau = \gamma_1 \cdots \gamma_n$ where δ_i and γ_j are transportations with m, n even, then $\sigma\tau = \delta_1 \cdots \delta_m \gamma_1 \cdots \gamma_n$ with $m+n$ even. So $\sigma\tau \in A_n$

For any transportation, δ, $\delta^{-1} = \delta$

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

So for $\sigma = \delta_1 \cdots \delta_m \in A_n$, $\sigma^{-1} = \delta_m \cdots \delta_1 \in A_n$.

By the subgroup test, $A_n \leq S_n$

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

So since $|S_n| = n!$ we have $|A_n| = n!/2$.

6. Isomorphisms.

Fourth roots of unity.

$U_4 = \{1, -1, i, -i\} = \{1, i, i^2, i^3\} = \langle i \rangle$ is cyclic generated by i.

Group of units $Z_5^\times = \{1, 2, 3, 4\} = \{1, 2, 2^2, 2^3\} = \langle 2 \rangle$

Both U_4 and $Z_5^\times$ have the same cayley table.

Both have the same structure as $C_4 = \langle a \rangle = \{e, a, a^2, a^3\}$

We say U_4 and $Z_5^\times$ are isomorphic.

Definition: Let G and G_1 be groups A map $\varphi: G \to G_1$ 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 $y \in G_1$ there is some $x \in G$ such that $\varphi(x) = y$

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

Define: $\varphi: U_4 \to Z_5^\times$ by $\varphi(i^k) = 2^k$

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

have $i^k = i^l$, so φ is one to one

let $2^k \in Z_5^\times$, then $\varphi(i^k) = 2^k$

So φ is onto

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

So $\varphi: U_4 \to Z_5^\times$ is an isomorphism

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

(1) If $|G| = n$, then $G \cong Z_n$

(2) if $|G| = \infty$, then $G \cong Z$

pf: For (1) Sps $|\langle a \rangle| = |a| = n$

define $\varphi: Z_n \to G$ 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 $k([l]) = a^l = a^k$

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

thus φ $Z_n \to G$ is an isomorphism. ∎

note: $\varphi: G \to G_1$ is operation preserving if $\varphi(ab) = \varphi(a)\varphi(b)$ $\forall a, b \in G$

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 $\varphi: G \xrightarrow{\sim} G_1$

then ① $\varphi(e_G) = e_{G_1}$

② $\varphi(a^n) = [\varphi(a)]^n$ $\forall a \in G$ & $n \in Z$

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

as $x^k = \varphi(b)$ in G_1

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

10/2/2019

6 Isomorphisms

Let G and G_1 be groups. A map $\varphi: G \to G_1$ 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: $\varphi(ab) = \varphi(a)\varphi(b)$ OR $\varphi(a+b) = \varphi(a)\varphi(b)$ OR $\varphi(ab) = \varphi(a) + \varphi(b)$ $\forall a, b \in G$

If $\varphi: G \to G_1$ 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 $\varphi: G \to \mathbb{Z}$ 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 surjurtive.
- 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 $K \leq G$, then $\varphi(K) = \{\varphi(g) \mid g \in G\}$ is a subgroup of G_1.

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

⑥ $\varphi(Z(G)) = Z(G_1)$

theorem: Let G, G_1, G_2 be groups.

① the identity map $id_G: G \to G$ 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 $(\psi \circ \varphi): G \to G_2$ is an isomorphism.

Corollary: $\cong$ is an equivalence relation on groups.

10/4/19.

Exam 1

(1) a) $\mathbb{Z}_{10}^\times = \{1, 3, 7, 9\}$

$|3| = |7| = 4$ $|9| = 2$

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

c) $\mathbb{Z}_{10}^\times = \langle 7 \rangle = \langle 7 \rangle$ $\mathbb{Z}_{10}^\times = \langle 3 \rangle$

$\langle 9 \rangle = \{1, 9\}$ $\langle 9 \rangle$

$\langle 1 \rangle$

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

$\begin{pmatrix} a & b \\ 0 & c \end{pmatrix}^{-1} = \frac{1}{ac} \begin{pmatrix} c & -b \\ 0 & a \end{pmatrix} = \begin{pmatrix} 1/a & -b/ac \\ 0 & 1/c \end{pmatrix}$

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

$$\begin{pmatrix} a & a+b \\ 0 & c \end{pmatrix} = \begin{pmatrix} a & b+c \\ 0 & c \end{pmatrix} \qquad a+b = b+c,\ a = c$$

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

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

$$\begin{pmatrix} ax & ay+bz \\ 0 & az \end{pmatrix} = \begin{pmatrix} ax & bx+ay \\ 0 & az \end{pmatrix} \qquad bz = bx \text{ if } x \neq z,\ b = 0$$

$$Z(H) = \begin{pmatrix} a & 0 \\ 0 & a \end{pmatrix}$$

3)

4) $|\sigma| = 3 \qquad \sigma^3 = \varepsilon$

$|\tau| = 2 \qquad \tau^2 = \varepsilon \qquad (12)(12) = (1)(2)$

b) $S_3 = \{\varepsilon, \sigma, \sigma^2, \tau, \tau\sigma, \tau\sigma^2\} \qquad |S_3| = 6$

$\tau\sigma = (23) \qquad \sigma = \qquad \tau\sigma^2 = \ldots$

these are the all six distinct element in S_3.

c)

S_3	ε	σ	σ^2	τ	$\tau\sigma$	$\tau\sigma^2$
ε	ε	σ	σ^2	τ	$\tau\sigma$	$\tau\sigma^2$
σ	σ	σ^2	ε	$\tau\sigma^2$	τ	$\tau\sigma$
σ^2	σ^2	ε	σ	$\tau\sigma$	$\tau\sigma^2$	τ
τ	τ	$\tau\sigma$	$\tau\sigma^2$	ε	σ	σ^2
$\tau\sigma$	$\tau\sigma$	$\tau\sigma^2$	τ	σ^2	ε	σ
$\tau\sigma^2$	$\tau\sigma^2$	τ	$\tau\sigma$	σ	σ^2	ε

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

$\sigma\tau\sigma = \tau \qquad \sigma^3\tau = \tau$

d) No. $\sigma\tau \neq \tau\sigma \qquad \sigma\tau = \tau\sigma^2$

5 a) 12

b) $(1\,2\,3\,4)(5\,6\,7)$

$= \left[\frac{7\times6\times5\times4}{4}\right]\cdot\left[\frac{3\times2\times1}{3}\right] = 7\times6\times5\times2 = 420$

c) $\sigma = (1\,2\,7\,4\,5\,6)$

length 6. written as 5 transpositions.

$\Rightarrow \sigma$ is odd

3 cycle $(1\,2\,3)$ length 3 $\Rightarrow$ it is even. 2 transposition.

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

Isomorphism.

$\varphi: G \xrightarrow{\cong} G_1$, φ is bijective $\varphi(g_1 g_2) = \varphi(g_1)\varphi(g_2)$ $\forall g_1, g_2 \in G$

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

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

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

$\varphi \circ id_G = id_G \circ \varphi = \varphi$ for any $\varphi \in Aut(G)$

$\varphi, \psi, \gamma \in Aut(G)$

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

$Aut(G)$ is a group under function composition.

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

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

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

pf: φ_a is an isomorphism

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

$a^{-1}axa^{-1}a = a^{-1}aya^{-1}a$

$x = y$ φ_a is 1-1

- Let $y \in G$. then $\varphi_a(a^{-1}ya) = aa^{-1}yaa^{-1} = y$ φ_a is onto.
- $\varphi_a(xy) = axya^{-1} = axa^{-1}aya^{-1} = \varphi_a(x)\varphi_a(y)$

→ So φ_a is an isomorphism.

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

$\varphi_e(x) = exe^{-1} = x = id(x)$

- So $id \in \{\varphi_a \mid a \in G\}$
- closed. if $\varphi_a, \varphi_b \in \{\varphi_a \mid a \in G\}$

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

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

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

10/7/2019

Isomorphism $\varphi: G \to G_1$ one to one, onto, and $\varphi(ab) = \varphi(a)\varphi(b)$ $\forall a, b \in G$

An isomorphism $\varphi: G_1 \to G$ is an antoisomorphism of G.

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

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

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

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

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

Theorem: $Aut(G)$ is a group and $Inn(G)$ is a subgroup

theorem: If $G \cong G_1$, then $Aut(G) \cong Aut(G_1)$

pf: Suppose $\varphi: G \xrightarrow{\cong} G_1$, Define a map $\Theta: Aut(G) \to Aut(G_1)$ by $\Theta(\psi) = \varphi\psi\varphi^{-1}$

$(G \xrightarrow{\psi} G) \longrightarrow (G_1 \xrightarrow{\varphi^{-1}} G \xrightarrow{\psi} G \xrightarrow{\varphi} G_1)$

if $\Theta(\psi_1) = \Theta(\psi_2)$ then $\varphi\psi_1\varphi^{-1} = \varphi\psi_2\varphi^{-1}$

$\psi_1 = \psi_2$ • 1-1

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

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

and $\Theta(\psi_1\psi_2) = \varphi\psi_1\varphi^{-1}\varphi\psi_2\varphi^{-1} = \Theta(\psi_1)\Theta(\psi_2)$

ex: $\mathrm{Aut}(\mathbb{Z}_8)$, $\mathbb{Z}_8 = \langle 1 \rangle$

If $\alpha : \mathbb{Z}_8 \to \mathbb{Z}_8$ 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 $1, 3, 5, 7$, $\mathbb{Z}_8^\times = \{1, 3, 5, 7\}$, there are 4 automorphisms.

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

Define $\theta : \mathbb{Z}_8^\times \to \mathrm{Aut}\,\mathbb{Z}_8$ by $\theta(m) = \alpha_m$

then θ is an isomorphism, therefore $\mathrm{Aut}(\mathbb{Z}_8) \cong \mathbb{Z}_8^\times$

theorem: $\mathrm{Aut}(\mathbb{Z}_n) = \mathbb{Z}_n^\times$

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

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

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

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

S_n permutations of $\{1, 2, \ldots n\}$

Given $a \in G$ $\tau_a : G \to G$ by $\tau_a(g) = ag$

τ_a is a element of S_G

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

and G_1 is a subgroup of $S_{G_1} \cong S_n$

7. Cosets and Lagranges theorem

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

let $n\mathbb{Z} = \{n k \mid k \in \mathbb{Z}\}$ 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 a equivalence relationship.

2) the equivalence class of a in G is $Ha = \{ha \mid h \in H\}$

for 2) $[a] = \{g \in G \mid g \equiv a\} = \{g \in G \mid ga^{-1} \in H\} = \{g \in G \mid ga^{-1} = h$ for some $h \in H\}$

$= \{g \in G \mid g = ha, h \in H\} = Ha$

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) $a \in Ha$ 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

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

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

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

- Let $H = \langle 2 \rangle = \{0, 2, 4, 6, 8\}$ $|\langle 2 \rangle| = 5$ 2 cosets. $|G : H| = 2$

  $5 \times 2 = 10$

  cosets : $H = 2 + H = 4 + H$

  $1 + H = \{1, 3, 5, 7, 9\} = H + 1$

  $= 3 + H = 5 + H$

  Distinct cosets : H, $1 + H$.

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

  $1 + K = K + 1 = \{1, 6\}$ $3 + K = K + 3 = \{3, 8\}$ $|G : K| = 5$

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

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

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

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

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

pf: Define $\sigma : H \to Ha$ by $\sigma(h) = ha$ σ 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 $Ha_1, Ha_2 \dots Ha_k$ be distinct cosets of H.

G is the disjoint union $G = Ha_1 \cup Ha_2 \cup \dots Ha_k$

then $|G| = |Ha_1| + |Ha_2| + \cdots |Ha_k|$

$|G| = \underbrace{|H| + |H| + \cdots |H|}_{k} = k|H|$ 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 $|G : H|$ = 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 $|\langle g \rangle|$ divide $|G|$

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

corollary: Let $|G| = n$

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

pf: pf $|g| = k$

since $|g| \mid |G| \rightarrow |g| \mid n$

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 $|\langle g \rangle| = p$ have $G = \langle g \rangle$

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

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

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

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

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

8 Direct products.

set $G_1, G_2 \cdots G_n$.

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

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

Defn: If $G_1, G_2 \cdots G_n$ are groups.

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

with componentwise operation:

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

$= (g_1 g_1', g_2 g_2' \cdots g_n g_n')$

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

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

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

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

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

$\mathbb{Z}_2 \oplus \mathbb{Z}_3$ 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 $G_1, G_2 \cdots G_n$

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

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

$= g_1 g_1', g_2 g_2', \cdots g_n g_n'$

Sometimes use $\oplus$ instead of $\times$

$\mathbb{Z}_2 \oplus \mathbb{Z}_4 = \{(0,0), (1,3), (0,2) \cdots\}$

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

$|\mathbb{Z}_2 \oplus \mathbb{Z}_4| = 2 \cdot 4 = 8$

theorem: If $G_1, G_2 \cdots G_n$ are finite,

then $|G_1 \times G_2 \cdots G_n| = |G_1||G_2| \cdots |G_n|$

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

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

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

so $\cong \mathbb{Z}_6$

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) $|G|$ and $|H|$ are relatively prime.

Corollary: let $G_1, G_2 \cdots G_n$ be finite cyclic groups.

then $G_1 \oplus G_2 \oplus \cdots G_n$ is cyclic

iff $|G_i|$ and $|G_j|$ are realitively prime $\forall i \neq j$

Corollary: $m = n_1 n_2 \cdots n_k$

then $\mathbb{Z}_m \cong \mathbb{Z}_{n_1} \oplus \mathbb{Z}_{n_2} \oplus \cdots \mathbb{Z}_{n_k}$.

iff n_i and n_j are realitively prime $\forall i \neq j$

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

9. Normal subgroups and Factor Groups

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

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

then $\sigma^2 = (1\,3\,2)$ $\quad \sigma^3 = \varepsilon$

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

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

$\sigma^3 = \varepsilon = \tau^2$ $\qquad \sigma\tau\sigma = \tau$

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

let $H = \{\varepsilon, \tau\}$, $H \leq S_3$

$H\sigma = \{\sigma, \tau\sigma\}$ $\qquad \sigma H = \{\varepsilon, \sigma\tau\} = \{\varepsilon, \tau\sigma^2\}$

So $H\sigma \neq \sigma H$ $\qquad$ Non abelian

Defn: A subgroup H of a group G is normal

if $gH = Hg$ $\quad \forall g \in G$

We write $H \trianglelefteq G$

ex: $S_3 = \{\varepsilon, \sigma, \sigma^2, \tau, \tau\sigma, \tau\sigma^2\}$

let $K = \{\varepsilon, \sigma, \sigma^2\}$ $\qquad \sigma\tau\sigma = \tau$, $\sigma\tau = \tau\sigma^2$

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

$K\tau = \{\tau, \sigma\tau, \sigma^2\tau\} = \{\tau, \tau\sigma^2, \tau\sigma\} = K\tau\sigma = K\tau\sigma^2$

$\tau K = \{\tau, \tau\sigma, \tau\sigma^2\} = \tau\sigma K = \tau\sigma^2 K$

$\Rightarrow \tau K = K\tau$ So $K \trianglelefteq S_3$.

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 $GL(2,\mathbb{R}) = \left\{ \begin{pmatrix} a & b \\ c & d \end{pmatrix} \middle| ad - bc \neq 0 \right\}$

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

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

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

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

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

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

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

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

So $\sigma\tau\sigma^{-1} \in A_n$

Consequently $A_n \trianglelefteq S_n$

10/18/19 Exam 2 Friday 10/25

Isomorphisms, cosets, langrange'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 = 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 $K \leq G$, $K \trianglelefteq G$ if $Kg = gK \quad \forall g \in G$

② The product of cosets $KaKb = Kab$ is well defined

pf ① implies ② Suppose $K \trianglelefteq G$, if $Ka = Ka_1$ & $Kb = Kb_1$

then $Kab = Ka_1b_1$

$Kab = Ka_1b_1$

$Kab = Ka_1b = a_1Kb = a_1Kb_1 = Ka_1b_1$

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 $KaKb = Kab$

proof: $ke\,Ka = Kea = Ka = Kae = Ka\,Ke$

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

Inverse of Ka is Ka^{-1}

$KaKa^{-1} = Kaa^{-1} = K = Ka^{-1}a = Ka^{-1}Ka$

Associative:

$Ka(KbKc) = Ka(Kbc) = Ka(bc) = Kabc = (KaKb)Kc$

10/21/19

Factor / Quotient groups

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

if $Hg = gH \quad \forall g \in G$

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.

$HaHb = Hab$. G/H is a quotient, factor group.

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

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

cosets of K in G. $K = \{e, a^4, a^8\}$ $\quad Ka^2 = \{a^2, a^6, a^{10}\}$

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

Quotient group.

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

Cayley table

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 $|G/K| = |G|/|K| = |G:K|$

pf: ① If G is abelian, then $KaKb = Kab = Kba = KbKa$

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

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

③ $|G/K|$ = number of distinct cosets of K in G. $= |G:K|$

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

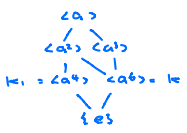
So $|G:K| = |G|/|K|$

So $|G/K| = |G:K| = |G|/|K|$

ex: let $G = \langle a \rangle = 12$, $|a| = 12$

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

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



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 G/K 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 G/K

$G/K = \langle Ka\rangle$

$\langle Ka^2\rangle$ $\langle Ka^3\rangle$

$\{K\}$

For G/K_1, $|G/K_1| = |G|/|K_1| = 12/3 = 4$.

since $G = \langle a\rangle$ is cyclic, G/K_1 is cyclic with K_1a

$G/K_1 = \langle K_1a\rangle = \{K_1, K_1a, K_1a^2, K_1a^3\}$

trivial proper subgroup $\langle K_1a^3\rangle = \{K_1, K_1a^2\}$

lattice of subgroups of G/K_1

$G/K_1 = \langle K_1a\rangle$

$\langle K_1a^2\rangle$

$\{K_1, 3\}$

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

theorem, (correspondence theorem)

Let $K \trianglelefteq G$, then the correspondence between $H \longleftrightarrow H/K$ is a bijection between the subgroups H of G that contain K and the subgroups of G/K

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

Determine the order of Ka^5 in G/K.

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

$|G/K| = 18/3 = 6$

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

Since $|G/K| = 6$. by lagrange theorem $|Ka^5| = 1, 2, 3,$ or 6.

Since $Ka^5 \neq K$, $|Ka^5| \neq 1$

$(Ka^5)^2 = Ka^{10} \neq K$ Since $a^{10} \notin K$ $|Ka^5| \neq 2$

$(Ka^5)^3 = Ka^{15} \neq K$ $a^{15} \notin K$ $|Ka^5| \neq 3$.

$(Ka^5)^6 = Ka^{30} = Ka^{12}$ therefore $|Ka^5| = 6$

OR. since $G/K = \langle Ka\rangle$ is cyclic of order 6

we know $(Ka)^5 = Ka^5$ is also a generator, so $|Ka^5| = 6$

OR. $\gcd(5, 18) = 1$

$G = \langle a^5\rangle$ so $G/K = \langle Ka^5\rangle$ $|Ka^5| = 6$

10/28/19

10. Group Homorphisms

Let G and G_1 be groups.

we say a map $\varphi: G \to G_1$ is a homorphism

if $\varphi(ab) = \varphi(a)\varphi(b)$ $\forall a, b \in G$

ex: 1) An isomorphism is a homophism that is one to one and onto

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

3) $Id: G \to G$ $Id(a) = a$

4) The determinat 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 $K \trianglelefteq G$. The coset map or canonical map

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

is a homorphism

OP: $\varphi(ab) = Kab = Ka\,Kb = \varphi(a)\varphi(b)$

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

$m \mapsto [m]$

Theorem: $\varphi: G \to G_1$ a homorphism

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

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

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

pf: 1) $\varphi(e) = \varphi(e \cdot e) = \varphi(e)\varphi(e)$

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

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

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

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

3) $\varphi(a^k) = \varphi(a \cdots a) = \varphi(a) \cdots \varphi(a) = \varphi(a)^k$

let $\varphi: G \to G_1$ a homorphism,

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

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

Theorem: let $\varphi: G \to G_1$ be a homorphism.

then 1) $Im\,\varphi \leq G_1$

2) $\ker\varphi \trianglelefteq G$

pf: 1) Apply the subgroup test.

- $\varphi(e) = e$, so $e \in Im\,\varphi$

closed - let $b_1, b_2 \in Im\,\varphi$

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

then $\varphi(a_1 a_2) = \varphi(a_1)\varphi(a_2) = b_1 b_2$

so $b_1 b_2 \in Im\,\varphi$.

- If $b \in Im\,\varphi$, then $b = \varphi(a)$ for some $a \in G$

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

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

By the subgroup test $Im\,\varphi \leq G_1$.

2) Apply the subgroup test.

① to show $\ker\varphi \leq G$ ...

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

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

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

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

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

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

ex: 1) multiplication by n map

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

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

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

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

$\ker \varphi = \{0\}$ trivial kernal = φ is 1-1

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

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

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

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

3) let $K \trianglelefteq G$ kanonical map $q: G \to G/K$ $q(a) = Ka$

$\ker q = K$ because $q(a) = Ka = K$ iff $a \in K$

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

Given $Ka \in G/K$, $q(a) = Ka$ $\operatorname{Im} q = G/K$

Every normal subgroup is a kernal of an onto homorphism

4) determinant mapping

$\det \quad GL(2,\mathbb{R}) \to \mathbb{R}^*$

$\ker \det = \{ A \in GL(2\mathbb{R}) \mid \det A = 1\}$

$\ker \det = SL(2,\mathbb{R})$

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

5) Sign mapping

$\operatorname{sgn} \quad S_n \to \{1, -1\}$

$\operatorname{sgn} \sigma = \begin{cases} 1 & \text{if } \sigma \text{ is even} \\ -1 & \text{if } \sigma \text{ is odd} \end{cases}$

$\operatorname{sgn}(\sigma\tau) = \operatorname{sgn}\sigma \operatorname{sgn}\tau \quad \forall \sigma\tau \in S_n.$

homorphism

$\operatorname{sgn}: S_n \to \{1, -1\}$

$\ker \operatorname{sgn} = \{\sigma \in S_n \mid \sigma \text{ is even}\} = A_n$

therefore $A_n \trianglelefteq S_n$

10/30/19

11 Fundamental Theorem of finite abelian groups

$\mathbb{Z}_{15} \cong \mathbb{Z}_3 \oplus \mathbb{Z}_5$

Only one abelian group of order 15

Isomorphism classes of abelian group of order 12

$12 = 2^2 \cdot 3$ $\quad \mathbb{Z}_{12} \cong \mathbb{Z}_3 \oplus \mathbb{Z}_4$

$\mathbb{Z}_{12} \cong \mathbb{Z}_2 \oplus \mathbb{Z}_2 \oplus \mathbb{Z}_3$ $\quad \mathbb{Z}_2 \oplus \mathbb{Z}_2 \ncong \mathbb{Z}_4$

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 $\mathbb{Z}_{p_1^{n_1}} \oplus \mathbb{Z}_{p_2^{n_2}} \oplus \cdots \mathbb{Z}_{p_k^{n_k}}$

where $p_1 \cdots p_k$ are prime, not necessary distinct primes. and the prime powers $p_1^{n_1}, p_2^{n_2} \cdots p_k^{n_k}$ are uniquely determined by G.

ex: $|G| = p^k$ $p \in$ prime $k \in \mathbb{Z}^+$

A partition of k is a set of positive integers $n_1 \cdots n_l$, who sum is k.

$n_1 + n_2 + \cdots n_l = k$.

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	→	$\mathbb{Z}_{16}$
1+3	→	$\mathbb{Z}_2 \oplus \mathbb{Z}_8$
2+2	→	$\mathbb{Z}_4 \oplus \mathbb{Z}_4$
1+1+2		$\mathbb{Z}_2 \oplus \mathbb{Z}_2 \oplus \mathbb{Z}_4$
1+1+1+1		$\mathbb{Z}_2 \oplus \mathbb{Z}_2 \oplus \mathbb{Z}_2 \oplus \mathbb{Z}_2$

ex: G is abelian $|G| = 72 = 8 \cdot 9 = 2^3 \cdot 3^2$

partition of 3	/	2	Group
3		2	$\mathbb{Z}_{72} \cong \mathbb{Z}_8 \oplus \mathbb{Z}_9$
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	$\mathbb{Z}_2 \oplus \mathbb{Z}_3 \oplus \mathbb{Z}_3 \oplus \mathbb{Z}_{25} \oplus \mathbb{Z}_7 \cong \mathbb{Z}_3 \oplus \mathbb{Z}_{1050}$
	$\mathbb{Z}_2 \oplus \mathbb{Z}_9 \oplus \mathbb{Z}_5 \oplus \mathbb{Z}_5 \oplus \mathbb{Z}_7 \cong \mathbb{Z}_5 \oplus \mathbb{Z}_{630}$
	$\mathbb{Z}_2 \oplus \mathbb{Z}_3 \oplus \mathbb{Z}_3 \oplus \mathbb{Z}_5 \oplus \mathbb{Z}_5 \oplus \mathbb{Z}_7 \cong \mathbb{Z}_3 \oplus \mathbb{Z}_5 \oplus \mathbb{Z}_{210}$
	$\cong \mathbb{Z}_{15} \oplus \mathbb{Z}_{210}$

prime power decomposition. Invariant factor decomposition

11/1/19

Fundamental Theorem of Finite Abelian Groups

G a finite abelian group.

$G \cong \mathbb{Z}_{p_1^{n_1}} \oplus \mathbb{Z}_{p_2^{n_2}} \cdots \oplus \mathbb{Z}_{p_k^{n_k}}$ $p_1 \cdots p_k$ not necessary distinct prime

$p_1^{n_1} \cdots p_k^{n_k}$ are uniquely determined by G

All abelian groups (up to isomorphism) of order 36

$|G| = 36 = 4 \cdot 9 = 2^2 3^2$

$\mathbb{Z}_4 \oplus \mathbb{Z}_9 \cong \mathbb{Z}_{36}$

$\mathbb{Z}_4 \oplus \mathbb{Z}_3 \oplus \mathbb{Z}_3 \cong \mathbb{Z}_3 \oplus \mathbb{Z}_{12}$

$\mathbb{Z}_2 \oplus \mathbb{Z}_2 \oplus \mathbb{Z}_9 \cong \mathbb{Z}_2 \oplus \mathbb{Z}_{18}$

$\mathbb{Z}_2 \oplus \mathbb{Z}_2 \oplus \mathbb{Z}_3 \oplus \mathbb{Z}_3 \cong \mathbb{Z}_6 \oplus \mathbb{Z}_6$

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 $\mathbb{Z}_{rs} \cong \mathbb{Z}_r \oplus \mathbb{Z}_s$ iff $\gcd(r,s) = 1$

we write $G \cong \mathbb{Z}_{m_1} \oplus \mathbb{Z}_{m_2} \oplus \cdots \mathbb{Z}_{m_s}$

$m_1 | m_2$, $m_2 | m_3$ .... 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

$108 = 2 \cdot 54 = 2 \cdot 9 \cdot 6 = 2^2 \cdot 3^3$

$\mathbb{Z}_4 \oplus \mathbb{Z}_{27} \cong \mathbb{Z}_{108}$

$\mathbb{Z}_2 \oplus \mathbb{Z}_2 \oplus \mathbb{Z}_{27} \cong \mathbb{Z}_2 \oplus \mathbb{Z}_{54}$

$\mathbb{Z}_4 \oplus \mathbb{Z}_3 \oplus \mathbb{Z}_9 \cong \mathbb{Z}_3 \oplus \mathbb{Z}_{36}$

$\mathbb{Z}_4 \oplus \mathbb{Z}_3 \oplus \mathbb{Z}_3 \oplus \mathbb{Z}_3 \cong \mathbb{Z}_3 \oplus \mathbb{Z}_3 \oplus \mathbb{Z}_{12}$

$\mathbb{Z}_2 \oplus \mathbb{Z}_2 \oplus \mathbb{Z}_3 \oplus \mathbb{Z}_9 \cong \mathbb{Z}_6 \oplus \mathbb{Z}_{18}$

$\mathbb{Z}_2 \oplus \mathbb{Z}_2 \oplus \mathbb{Z}_3 \oplus \mathbb{Z}_3 \oplus \mathbb{Z}_3 \cong \mathbb{Z}_3 \oplus \mathbb{Z}_6 \oplus \mathbb{Z}_6$

First Isomorphism Theorem

$\varphi: G \to G$ homomorphism: $\varphi(ab) = \varphi(a)\varphi(b) \quad \forall a, b \in G$

$\ker \varphi = \{a \in G \mid \varphi(a) = e\}$

Theorem: If $\varphi: G \to G$ is a homomorphism,

then $\ker \varphi = \{e\}$ iff φ is one-to-one

pf: suppose φ is one to one

then since $\varphi(e) = e$, $\ker \varphi = \{e\}$

conversely, let $\ker \varphi = \{e\}$, $\varphi(a) = \varphi(b)$

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

since $\ker \varphi = \{e\}$ $ab^{-1} = e$ $a = b$

Theorem (first isomorphism theorem)

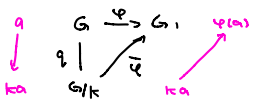
Suppose $\varphi: G \to G_1$ is a homomorphism, and let $K = \ker \varphi$

then φ induces an isomorphism $\bar{\varphi}: G/K \to \operatorname{Im} \varphi$

$\bar{\varphi}(Ka) = \varphi(a)$

that is $G/\ker\varphi \cong \operatorname{Im} \varphi$

thus φ factors as $\bar{\varphi} = \bar{\varphi} q$



where $q: G \to G/K$ is the canonical map $q(a) = Ka$

Suppose we have an onto homomorphism $\varphi: G \to G_1$ with $\ker \varphi = K$.

then by the isomorphism theorem, $G/K \cong G_1$

11/4/19

a) $n\mathbb{Z} \cong m\mathbb{Z}$

Define $\varphi: n\mathbb{Z} \to m\mathbb{Z}$ by $\varphi(nk) = mk$

$\varphi(nk) = \varphi(n\ell)$

$mk = m\ell \qquad k = \ell \Rightarrow nk = n\ell$

if $mk \in m\mathbb{Z}$

then $\varphi(nk) = mk$

$\varphi(nk+nl) = \varphi(n(k+l)) = m(k+l) = mk+ml = \varphi(nk) + \varphi(nl)$

c) Aut $\mathbb{Z}$ $\quad \mathbb{Z} \xrightarrow{\varphi} \mathbb{Z}$ $\quad \varphi(1)$ must be a generator of $\mathbb{Z}$.

$\varphi(1) = 1$ or $\varphi(1) = -1$

$\varphi : \mathbb{Z} \to \mathbb{Z}$ $\quad \varphi(x) = x$

$\varphi : \mathbb{Z} \to \mathbb{Z}$ $\quad \varphi(x) = -x$

Aut $\mathbb{Z} \cong \{1, -1\} \cong \mathbb{Z}_2$

4) $\varphi : G \to G_1$ $\quad H \trianglelefteq G$

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 $g \in G$ so that $\varphi(g) = g_1$.

let $\varphi(h) \in \varphi(H)$

then $g_1 \varphi(h) g_1^{-1} = \varphi(g)\varphi(h)\varphi(g^{-1}) = \varphi(ghg^{-1})$

and $gHg^{-1} \in H$. since $H \trianglelefteq G$.

so $\varphi(ghg^{-1}) \in \varphi(H)$

therefore $\varphi(H) \trianglelefteq G_1$.

The Isomorphism theorem

theorem : let $\varphi : G \to G_1$ be an onto homomorphism. with $\ker \varphi = K$

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: $\mathbb{Z} \xrightarrow{\varphi} \mathbb{Z}_5$

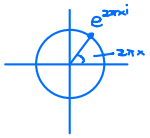
$7 \longmapsto 2$

$5 \longmapsto 0$ $\quad 10 \longmapsto 0$

ex: $\mathbb{R}/\mathbb{Z} \cong S^1$ $\quad S^1$ is the circle group

$S^1 = \{z \in \mathbb{C} \mid |z| = 1\}$

Define $\varphi : \mathbb{R} \longrightarrow S^1$ $\quad$ by $\varphi(x) = e^{2\pi x i}$



$\varphi(x+y) = e^{2\pi(x+y)i} = e^{2\pi x i} e^{2\pi y i} = \varphi(x)\varphi(y)$ is OP.

φ is onto for any $e^{2\pi x i} \in S^1$ $\quad \varphi(x) = e^{2\pi x i}$

For the $\ker(\varphi : \mathbb{R} \to S^1)$

$e^{2\pi x i} = 1$ 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

$(R, +)$ is abelian group

1) $a + b = b + a$
2) $a + (b + c) = (a + b) + c$
3) $\exists\, 0 \in R$ such that $a + 0 = a$ $\quad \forall a \in R$
4) $\forall a \in R$ $\quad \exists\, -a \in R$ such that $a + (-a) = 0$
5) $a(bc) = (ab)c$

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) $\exists\ 1 \in R$ 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: $\mathbb{Z}$ multiplicative inverses are missing

$2\mathbb{Z}$ ring with no unity

$\mathbb{Q}, \mathbb{R}, \mathbb{C}$ all commutative. $\exists a^{-1}$ $\forall a \neq 0$ these are fields.

$\mathbb{Z}_n$ $[a]+[b] = [a+b]$, $[a][b] = [ab]$.

$[a]^{-1}$ is missing in general (units $\mathbb{Z}_n^\times$)

special case:

$\mathbb{Z}_p$. $p \in$ prime. Then $[a]^{-1}$ exists for all $a \neq 0$

$\mathbb{Z}_p$ is a field.

ex: $R = \mathbb{Z}, \mathbb{Q}, \mathbb{R}, \mathbb{C}$

$M(2,R)$ = 2×2 matrices over R

Is a noncommutative ring.

ex: Let $R = \mathbb{Z}, \mathbb{Q}, \mathbb{R}, \mathbb{C}$.

Ring of polynomials over R.

$R[x] = \{ a_0 + a_1 x + a_2 x^2 + \cdots a_n x^n \mid a_i \in R \}$

polynomials of indeterminate x coefficients in R.

Add / multiply polynomials like usual

Direct product of Rings:

Let $R_1, R_2 \ldots R_n$ be rings

$R_1 \times R_2 \times \cdots R_n = R_1 \oplus R_2 \oplus \cdots R_n = \{ (r_1, r_2 \ldots r_n) \mid r_i \in R_i, i = 1 \ldots n \}$

$(r_1, r_2 \ldots r_n) + (s_1, s_2 \ldots s_n) = (r_1+s_1, r_2+s_2 \ldots r_n+s_n)$

$(r_1, r_2 \ldots r_n)(s_1, s_2 \ldots s_n) = (r_1 s_1, r_2 s_2, r_3 s_3 \ldots r_n s_n)$

11/6/19

Intro to Rings

A Ring R has operations $a+b$, ab so that $(R,+)$ is an abelian group

- $a(bc) = (ab)c$
- $a(b+c) = ab+ac$

  $(b+c)a = ba+bc$

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 multiplive 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 $0 \in S$ and $1 \in S$

② if $s \in S$ and $t \in S$, then $s \pm t$, st, $-s$ are in S

Ex. The ring of Gaussian integers:

$\mathbb{Z}[i] = \{n + mi \mid n + mi \in \mathbb{C},\ m, n \in \mathbb{Z}\}$

this is a subring of $\mathbb{C}$.

ex: Let R be a ring, the ring of upper triangular matrices over R

$\left\{ \begin{pmatrix} a & b \\ 0 & c \end{pmatrix} \mid a, b, c \in R \right\}$ 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.

$2 \cdot 3 = 0$. $3 \cdot 4 = 0$

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 is 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 $c \neq 0$.

ex $M(2, \mathbb{Z})$ $\begin{pmatrix} 1 & 0 \\ 0 & 0 \end{pmatrix}\begin{pmatrix} 0 & 0 \\ 0 & 1 \end{pmatrix} = \begin{pmatrix} 0 & 0 \\ 0 & 0 \end{pmatrix}$

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 domains.

Not integral domains:

1) $\mathbb{Z}_n$, n not prime

2) $\mathbb{Z} \oplus \mathbb{Z}$ $(1, 0)(0, 1) = (0, 0)$

3) $M(2, \mathbb{Z})$ 2x2 matrices with $\mathbb{Z}$ entries. $\begin{pmatrix} 1 & 0 \\ 0 & 0 \end{pmatrix}\begin{pmatrix} 0 & 0 \\ 0 & 1 \end{pmatrix} = \begin{pmatrix} 0 & 0 \\ 0 & 0 \end{pmatrix}$

Theorem: Let R be an integral domain.

if $ab = ac$ and $a \neq 0$, then $b = c$

pf: $ab = ac$ $\quad ab - ac = 0$ $\quad a(b-c) = 0$

since R is an integral domain and $a \neq 0$,

then $b - c = 0$, $b = c$

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: $a \cdot u = 0$

$a u u^{-1} = 0 \cdot u^{-1}$

$a = 0$

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 $a, a^2, a^3 \cdots$ cannot all be distinct.

So $a^i = a^j$ for some $i > j$

$a^{i-j} = 1$

$a \cdot a^{i-j-1} = 1$

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 $\operatorname{char} R$.

is the smallest positive integer n such that $na = 0$ $\forall a \in R$

$\operatorname{char} R = 0$, if no such integer exists.

ex: 1) $\operatorname{char} \mathbb{Z} = 0$

2) $\operatorname{char} \mathbb{Z}_n = n$.

3) $\mathbb{Z}_2[x] = \{ a_0 + a_1 x + \cdots a_n x^n \mid a_0 \in \mathbb{Z}_2 \}$ infinite ring with finite characteristic.

$\operatorname{char} \mathbb{Z}_2[x] = 2$

11/11/19

13 Integral Domains

R a ring, $a \in R$ is a zero domain 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

$\operatorname{char} R = n$ means n is the smallest positive integer

such $nx = 0$ $\forall x \in R$

If no such n exists, then $\operatorname{char} R = 0$

ex: $\operatorname{char} \mathbb{Z}_n = n$ $\quad \operatorname{char} \mathbb{Z} = 0$

Theorem: Let R be a ring with 1

If 1 has infinite order under addition, then $\text{char } R = 0$

If 1 has order n under addition then $\text{char } R = n$

because $\forall x \in R \quad nx = (n \cdot 1)x$

ex: $M(2, \mathbb{Z}_2) = \left\{ \begin{pmatrix} a & b \\ c & d \end{pmatrix} \mid a,b,c,d \in \mathbb{Z}_2 \right\}$

$n \begin{pmatrix} 1 & 0 \\ 0 & 1 \end{pmatrix} = \begin{pmatrix} n & 0 \\ 0 & n \end{pmatrix} = \begin{pmatrix} 0 & 0 \\ 0 & 0 \end{pmatrix} \qquad n \begin{pmatrix} 1 & 0 \\ 0 & 1 \end{pmatrix} = \begin{pmatrix} n & 0 \\ 0 & n \end{pmatrix} = \begin{pmatrix} 0 & 0 \\ 0 & 0 \end{pmatrix}$

$\text{char } M(2, \mathbb{Z}_2) = 2$

Theorem: The characteristic of every domain D is either 0 or a prime.

pf: suppose $\text{char } D = n \neq 0$

suppose $n = st \qquad 0 = n \cdot 1 = (s \cdot 1)(t \cdot 1)$

because D is a domain, $s \cdot 1 = 0$ OR $t \cdot 1 = 0$

because n is the smallest positive integer with this property.

$s = n$ OR $t = n$ so n is prime.

Field: A field is a commutative ring with unity where every nonzero element is a unit.

example of fields: 1) $\mathbb{Q}(\sqrt{2}) = \{ r + s\sqrt{2} \mid r, s \in \mathbb{Q} \}$

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) $\mathbb{Z}_3(i) = \{ a + bi \mid a,b \in \mathbb{Z}_3 \}$ field of 8 elements

$= \{ 0, 1, 2, i, 2i, 1+i, 1+2i, 2+2i \}$

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 $\forall R$, the trivial ideal

2) $R = \mathbb{Z}$. $I = 5\mathbb{Z}$. ... $I = n\mathbb{Z}$. $n \in \mathbb{Z}^+$

3) $\mathbb{Z}[x] = \{ a_0 + a_1 x + a_2 x^2 \cdots \mid a_i \in \mathbb{Z} \}$

$I = \{ a_1 x + a_2 x^2 \mid a_i \in \mathbb{Z} \}$

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 $(\langle a \rangle, +) \leq (R, +)$

$0 = 0 \cdot a \in \langle a \rangle$

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 $ra \in \langle a \rangle$

then $s(ra) = (sr)a \in \langle a \rangle$ since $rs \in R$

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 ring R.

$R/I = \{r+I \mid r \in R\}$ is a ring under the operations $(r+I)+(s+I) = (r+s)+I$

the unity of R/I is $1+I$ $\qquad (r+I)(s+I) = rs+I$

pf: we show if I is an ideal, then the product is well defined.

If $r+I = r'+I$ & $s+I = s'+I$ then $rs+I = r's'+I$

since $s+I = s'+I$ we have $s-s' \in I$

then $s-s' = a$, $a \in I$ then $s = s'+a$

similarly : $r = r'+b$, $b \in I$

therefore $rs+I = (r'+b)(s'+a)+I$

$= r's' + r'a + s'b + ba + I = r's' + I$

since $r'a \in I$, $s'b \in I$, $ba \in I$

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) $(I,+) \leq (R,+)$

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 ring.

$(r+I)+(s+I) = (r+s)+I$

$(r+I)(s+I) = rs+I$

ex: Gaussian integers

$\mathbb{Z}(i) = \{m+ni \in \mathbb{C} \mid m,n \in \mathbb{Z}\} = R$

principal ideal $\langle 2+i \rangle = R(2+i) = \{(m+ni)(2+i) \mid m+ni \in \mathbb{Z}(i)\}$

Quotient Ring

$\mathbb{Z}(i)/\langle 2+i \rangle = \{(m+ni)+\langle 2+i \rangle \mid m+ni \in \mathbb{Z}(i)\}$

In the quotient ring, $2+i = 0$ $\quad (2+i)+1 = 0+1$

so $i = -2$ hence $-1 = 4$ so $5 = 0$ in the quotient ring.

We can write cosets in $\mathbb{Z}(i)/\langle 2+i \rangle$ in the form

$m+ni+\langle 2+i \rangle = m-2n+\langle 2+i \rangle$ using $i = -2$

where $m-2n \in \mathbb{Z}$ and $5 = 0$

therefore $\mathbb{Z}(i)/\langle 2+i \rangle = \{k+\langle 2+i \rangle \mid k \in \mathbb{Z}_5\}$

$= \{\langle 2+i \rangle, 1+\langle 2+i \rangle, 2+\langle 2+i \rangle, 3+\langle 2+i \rangle, 4+\langle 2+i \rangle\}$

$\mathbb{Z}(i)/\langle 2+i \rangle$ is a field of 5 elements isomorphic to $\mathbb{Z}_5$

ex: Ring of polynomials over $\mathbb{R}$:

$\mathbb{R}[x] = \{a_0 + a_1x + a_2x^2 + \cdots a_nx^n \mid a_i \in \mathbb{R}\} = R$

Principal ideal generated x^2+1 :

$\langle x^2+1 \rangle = R(x^2+1) = \{f(x)(x^2+1) \mid f(x) \in \mathbb{R}[x]\}$

In the quotient ring,

$\mathbb{R}[x]/\langle x^2+1 \rangle = \{g(x)+\langle x^2+1 \rangle \mid g(x) \in \mathbb{R}[x]\}$

$x^2+1=0$ so $x^2=-1$

Also, using the division algorithm, $g(x) = q(x)(x^2+1) + r(x)$

where $0 \le \deg r(x) < 1$

so $\mathbb{R}[x]/\langle x^2+1\rangle = \{(ax+b) + \langle x^2+1\rangle \mid a,b \in \mathbb{R}\}$ with $x^2=-1$

thus $\mathbb{R}[x]/\langle x^2+1\rangle$ is a field isomorphic to $\mathbb{C}$

ex: $((3x-1)+\langle x^2+1\rangle)\cdot((4x+2)+\langle x^2+1\rangle)$

$= (3x-1)(4x+2) + \langle x^2+1\rangle$

$= 12x^2 + 6x - 4x - 2 + \langle x^2-1\rangle$

$= 2x - 14 + \langle x^2+1\rangle$

11/15/19

Prime and maximal ideals

commutative ring R with 1, I is an ideal if:

1) $(I,+) \le (R,+)$

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 R

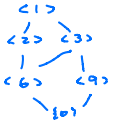
$n\mathbb{Z}$ is a prime ideal when n is prime

if $ks \in p\mathbb{Z}$ either $k \in p\mathbb{Z}$ or $s \in p\mathbb{Z}$

$p\mathbb{Z}$, 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 $\mathbb{Z}/18$



$\langle 2\rangle$, $\langle 3\rangle$ are maximal ideals.

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

suppose $(a+I)(b+I) = I \Rightarrow (ab+I) = I \Rightarrow ab \in I$

Since I is a prime ideal, $a \in I$ or $b \in I$.

So $a+I = I$ or $b+I = I$

therefore R/I has no zero divisors. So its a integral domain.

conversely: Suppose R/I is an integral domain

Suppose $ab \in I$, then $(a+I)(b+I) = ab+I = I$

Since R/I is an integral domain.

$a+I = I$ or $b+I = I$, so $a \in I$ 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, $\varphi: R \to R_1$ is a ring homomorphism if $\forall\, a, b \in R$

1) $\varphi(a+b) = \varphi(a) + \varphi(b)$
2) $\varphi(ab) = \varphi(a)\varphi(b)$
3) $\varphi(1_R) = 1_{R_1}$

ex: 1) canonical map $R \to R/I$, $r \to r+I$, I an ideal of R.

2) natural homomorphism $\mathbb{Z} \to \mathbb{Z}_n$, $k \to [k]$

3) R a ring $\varphi: R[x] \to R$, $\varphi(a_0 + a_1x + \cdots a_nx^n) = a_0$

Properties of Ring homomorphisms

Theorem: Let $\varphi: R \to R_1$ be a ring homomorphism and $r \in R$.

then 1) $\varphi(0) = 0$
2) $\varphi(-r) = -\varphi(r)$
3) $\varphi(kr) = k\varphi(r)$, $k \in \mathbb{Z}$
4) $\varphi(r^n) = \varphi(r)^n$, $n \geq 0$ $n \in \mathbb{Z}$
5) If $u \in R^\times$, $\varphi(u^k) = \varphi(u)^k$ $\forall\, k \in \mathbb{Z}$

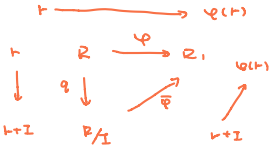
Theorem: Let $\varphi: R \to R_1$ be a ring homomorphism,

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 $R \to R/I$, $r \mapsto r+I$

Isomorphism Theorem for Rings

Let $\varphi: R \to R_1$ be a ring homomorphism with $I = \ker\varphi$, then φ induces the isomorphism of rings $\bar{\varphi}: R/I \to \varphi(R)$ where $\bar{\varphi}(r+I) = \varphi(r)$



Corollary: If $\varphi: R \to S$ 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. $R[x] = \{a_0 + a_1x + \cdots a_nx^n \mid a_i \in R\}$

$\langle x\rangle = R[x]x = \{x\,f(x) \mid f(x) \in R\}$

Define $\varphi: R[x] \to R$ by $\varphi(a_0 + a_1x + \cdots a_nx^n) = a_0$

then φ is an onto ring homomorphism with kernel.

$\ker\varphi = \{a_0 + a_1x + \cdots a_nx^n \mid a_0 = 0\} = \langle x\rangle$

By the isomorphism theorem of ring

$R[x]/\langle x\rangle \cong R$

taking $R=\mathbb{Z}$, we get $\mathbb{Z}[x]/\langle x\rangle \cong \mathbb{Z}$ ($\mathbb{Z}$ an integral domain.)

↳ prime, not maximal bc, $\mathbb{Z}$ not a field.

- R/I is an integral domain $\Leftrightarrow$ I is an 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 an prime ideal.

Theorem: Let R be a ring with 1, then

$\mathbb{Z}\cdot 1_R = \{k\cdot 1_R \mid k\in\mathbb{Z}\}$ is a subring of R.

1) If char $R = n > 0$, then $\mathbb{Z}\cdot 1_R \cong \mathbb{Z}_n$

2) If 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 $\varphi: \mathbb{Z}\to R$ by $\varphi(k) = k\cdot 1_R$

φ is an ring homomorphism with its $\operatorname{Im}\varphi: \varphi(\mathbb{Z}) = \mathbb{Z}\cdot 1_R$

$\ker\varphi: \{k\in\mathbb{Z} \mid k\cdot 1_R = 0\}$

If char $R=n$, then $\ker\varphi = n\mathbb{Z}$, so $\mathbb{Z}_n \cong \mathbb{Z}/n\mathbb{Z} \cong \mathbb{Z}\cdot 1_R$

If char $R=0$, then $\ker\varphi = 0$, so $\mathbb{Z}\cong\mathbb{Z}/\{0\}\cong\mathbb{Z}\cdot 1_R$

Corollary: Let F be a field, If char $F = p$, prime.

then F contains a subfield isomorphic to $\mathbb{Z}_p$.

If char $F=0$, then F contain a subfield isomorphic to $\mathbb{Q}$, rational numbers.

$\mathbb{Q}\subseteq\mathbb{R}\subseteq\mathbb{C}$ $\quad\mathbb{Q} = \{\frac{m}{n} \mid m,n\in\mathbb{Z}, n\neq 0\}$

Exam: from here the rest of finite algebra

ring, ideals, homomorphism

11/20/19

1) a) $\varphi(7) = 7\ \varphi(1) = 6 = 21$

$\varphi(1) = 3$

$\varphi(x) = 3x$

b) $\operatorname{Im}\varphi = \{0, 3, 6, 9, 12\}$

c) $\ker\varphi: \{x\in\mathbb{Z}_{50} \mid \varphi(x) = 0\}$

$\ker\varphi = \{0, 5, 10, 15, 20, 25, 30, 35, 40, 45\}$

d) $\varphi^{-1}(3)$

$\varphi(x) = 3x = 3$ in $\mathbb{Z}_{15}$ $\quad x\in\{1, 6, 11, 16, 21, 26, 31, 36, 41, 46\} = \varphi^{-1}(3)$

2) a) $108 = 2^2\cdot 3^3$

$\mathbb{Z}_4\oplus\mathbb{Z}_{27}\cong\mathbb{Z}_{108}$ ←

$\mathbb{Z}_2\oplus\mathbb{Z}_2\oplus\mathbb{Z}_{27}\cong\mathbb{Z}_2\oplus\mathbb{Z}_{54}$ ←

$\mathbb{Z}_4\oplus\mathbb{Z}_3\oplus\mathbb{Z}_9\cong\mathbb{Z}_3\oplus\mathbb{Z}_{36}$

$\mathbb{Z}_4\oplus\mathbb{Z}_3\oplus\mathbb{Z}_3\oplus\mathbb{Z}_3\cong\mathbb{Z}_3\oplus\mathbb{Z}_3\oplus\mathbb{Z}_{12}$

$\mathbb{Z}_2\oplus\mathbb{Z}_2\oplus\mathbb{Z}_3\oplus\mathbb{Z}_9\cong\mathbb{Z}_6\oplus\mathbb{Z}_{18}$

$\mathbb{Z}_2\oplus\mathbb{Z}_2\oplus\mathbb{Z}_3\oplus\mathbb{Z}_3\oplus\mathbb{Z}_3\cong\mathbb{Z}_3\oplus\mathbb{Z}_6\oplus\mathbb{Z}_6$

b) $\mathbb{Z}_{108}$ has $\{0, 36, 72\}$

$\mathbb{Z}_2\oplus\mathbb{Z}_{54}$ has $\{(0,0), (0,18), (0,36)\}$

3) $S = \{ara \mid r\in R\}$ is a subring.

subring test $\quad 0 = a\cdot 0\cdot a \in S$

$1 = a\cdot 1\cdot a = a^2 = 1 \in S$

suppose ara, $ata \in S$

$ara + ata = a(r+t)a \in S$

$(ara)(ata) = a\,ra^2ta = ar\,ta \in S$

$-ara = a(-r)a \in S$

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

char $\mathbb{Z}_7(\sqrt{3}) = 7$

b) take $a + b\sqrt{3} \neq 0$ in $\mathbb{Z}_7(\sqrt{3})$

$1^2 = 1$, $2^2 = 4$, $3^2 = 2$, $4^2 = 2$, $5^2 = 4$, $6^2 = 1$.

$\sqrt{3} \notin \mathbb{Z}_7$

So if $a + b\sqrt{3} \neq 0$ then $a - b\sqrt{3} \neq 0$

$$\frac{1}{a+b\sqrt{3}} \cdot \frac{a-b\sqrt{3}}{a-b\sqrt{3}} = \frac{a-b\sqrt{3}}{a^2-3b^2} = \frac{a}{a^2-3b^2} - \frac{b}{a^2-3b^2}\sqrt{3}$$

$a^2 - 3b^2 \neq 0$ since $\sqrt{3} \notin \mathbb{Z}_7$

5) a) $(IJ, +) \leq (R, +)$

$(a_1b_1 + a_2b_2 + \cdots a_nb_n) + (a_1'b_1' + a_1'b_1 + \cdots a_n'b_n') = a_1b_1 + a_2b_2 + \cdots a_nb_n + \cdots a_n'b_n' \in IJ$

$0 \in I$, $0 \in J$, $0 \cdot 0 \in IJ$

$-(a_1b_1 + a_2b_2 + \cdots a_nb_n) = -a_1b_1 + (-a_2)b_2 + \cdots (-a_n)b_n \in IJ$

Now let $r \in R$ Since I an ideal.

$r(a_1b_1 + a_2b_2 + \cdots a_nb_n) = (ra_1)b_1 + (ra_2)b_2 + \cdots (ra_n)b_n \in IJ$

therefore IJ an ideal of R

b) $IJ \subseteq I \cap J$

let $a_1b_1 + \cdots a_nb_n \in IJ$ since I ideal $a_ib_i \in I$

since J ideal, $a_ib_i \in J$

$(I \cap J, +) \leq (R, +)$, so $a_1b_1 + \cdots a_nb_n \in I \cap J$

6) $R = \mathbb{Z}[i] = \{m + ni \in \mathbb{C} \mid m, n \in \mathbb{Z}\}$

$I = \langle 1 + 2i \rangle$

$R/I = \mathbb{Z}[i]/\langle 1+2i \rangle = \{m + ni + \langle 1 + 2i \rangle \mid m, ni \in \mathbb{Z}[i]\}$

$3 + i = (1 + 2i)(1 - i) \in \langle 1 + 2i \rangle = I$

So in R/I, $3 + i = 0$ hence $i = -3$

$R/I = \{(m - 3n) + I \mid m, n \in \mathbb{Z}\}$

$= \{k + I \mid k \in \mathbb{Z}\}$

Also in R/I, $1 + 2i = 0$

$2i = -1$

$-4 = 1$ so $5 = 0$

$R/I = \{I, 1 + I, 2 + I, 3 + I, 4 + I\}$ $(5 = 0)$

$\cong \mathbb{Z}_5$

8) Define map $\varphi : \mathbb{Z}[i] \to \mathbb{Z}_3[i]$

by $\varphi(m + ni) = \bar{m} + \bar{n}i$, $\bar{m}, \bar{n}$ reduce mod 3

then φ is an onto ring homomorphism

$\mathbb{Z}[i] \to \mathbb{Z}_n$ 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 $\varphi : \mathbb{Z}[i] \to \mathbb{Z}_3[i]$ is an onto ring homomorphism with $\ker\varphi = 3\mathbb{Z}[i]$

by the isomorphism theorem $\mathbb{Z}[i]/3\mathbb{Z}[i] \cong \mathbb{Z}_3[i]$

11/25/19

1b Polynomial Rings

R a commutative ring with 1.

Ring of Polynomials over R $R[x] = \{a_0 + a_1x + a_2x^2 + \cdots a_nx^n \mid a_i \in R\}$

in the indeterminate x. $f(x) = a_0 + a_1x + a_2x^2 + \cdots$

$g(x) = b_0 + b_1x + b_2x^2 + \cdots$ $f(x) = g(x)$ iff $a_i = b_i$ $\forall i$

$f(x)+g(x) = a_0+b_0 + (a_1+b_1)x + (a_2+b_2)x^2 + \cdots$

$f(x)g(x) = (a_0 + a_1x + \cdots)(b_0 + b_1x + \cdots) = a_0b_0 + (a_0b_1 + a_1b_0)x + (a_0b_2 + a_1b_1 + a_2b_0)x^2 + \cdots$

In general, the coefficient of x^k in $f(x)g(x)$ is $a_0b_k + a_1b_{k-1} + \cdots a_{k-1}b_1 + a_kb_0 = \sum_{i+j=k} a_ib_j$

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 $\deg f(x)g(x) = \deg f(x) + \deg g(x)$

3) The units in $R[x]$ are the units in R

proof: let $f(x) = a_0 + a_1x + a_2x^2 + \cdots$ $g(x) = b_0 + b_1x + b_2x^2 + \cdots$ where $a_n \neq 0$ $b_m \neq 0$

$f(x)g(x) = a_0b_0 + (a_0b_1 + a_1b_0)x + \cdots a_nb_mx^{m+n}$

Since R is a domain and $a_n \neq 0$, $b_m \neq 0$ then $a_nb_m \neq 0$, $f(x)g(x) \neq 0$

hence $R[x]$ is an integral domain. Furthermore $\deg f(x)g(x) = m+n = \deg f(x) + \deg g(x)$

For 3), suppose $f(x) \in R[x]^\times$, then $f(x)g(x) = 1$ for some $g(x) \in R[x]$

so $\deg f(x)g(x) = \deg f(x) + \deg g(x)$

$\deg 1 = \deg f + \deg g$

$0 = \deg f + \deg g$

hence $f(x) \in R$, so $R[x]^\times \subseteq R^\times$, clearly $R^\times \subseteq R[x]^\times$

Ex: $R = \mathbb{Z}_4$ not an integral domain b/c has zero divisors. $2 \cdot 2 = 4$.

$f(x) = 1 + 2x \in \mathbb{Z}_4[x]$ $f(x)^2 = (1+2x)^2 = 1 + 4x + 4x^2 = 1$

$(1+2x)$ is a unit in $\mathbb{Z}_4[x]$ self inverse.

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) either $r(x) = 0$ or $\deg r(x) < \deg f(x)$

Ex: $f(x) = x^2 + x + 2$ $g(x) = x^5 + 2x^4 + x^2 + x + 4$ in $\mathbb{Z}_7[x]$

$$
\begin{array}{r|l}
x^2+x+2 & x^5+x^3+4x+2 \\
\hline
 & x^5+x^4+2x^3 \\
 & \hline
 & x^4+5x^3+x^2+x+4 \\
 & x^4+x^3+2x^2 \\
 & \hline
 & 4x^3+6x^2+x+4 \\
 & 4x^3+4x^2+x \\
 & \hline
 & 2x^2+4 \\
 & 2x^2+2x+4 \\
 & \hline
 & 6x
\end{array}
$$

$g(x) = q(x)f(x) + r(x)$

$x^5+2x^4+x^2+x+4 = (x^3+x^2+4x+2)(x^2+x+2) + 6x$

12/2/19

Exam Three

1. a) $\varphi((a_1, b_1) + (a_2, b_2)) = \varphi(a_1, b_1) + \varphi(a_2, b_2)$

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) $\operatorname{Im}\varphi = ?$

let $a \in \mathbb{Z}$, then $\varphi(a, 0) = a - 0 = a$ φ is onto.

so $\operatorname{Im}\varphi = \mathbb{Z}$

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) $\varphi(a,b) = a - b = 3 \qquad b = a - 3$

$\varphi^{-1}(3) = \{ (a, a-3) \mid a \in \mathbb{Z} \}$

2. a) $3300 = 2^2 \cdot 3 \cdot 5^2 \cdot 11$

$\mathbb{Z}_4 \oplus \mathbb{Z}_3 \oplus \mathbb{Z}_{25} \oplus \mathbb{Z}_{11} \cong \mathbb{Z}_{3300}$

$\mathbb{Z}_2 \oplus \mathbb{Z}_2 \oplus \mathbb{Z}_3 \oplus \mathbb{Z}_{25} \oplus \mathbb{Z}_{11} \cong \mathbb{Z}_2 \oplus \mathbb{Z}_{1650}$

$\mathbb{Z}_4 \oplus \mathbb{Z}_3 \oplus \mathbb{Z}_5 \oplus \mathbb{Z}_5 \oplus \mathbb{Z}_{11} \cong \mathbb{Z}_5 \oplus \mathbb{Z}_{660}$

$\mathbb{Z}_2 \oplus \mathbb{Z}_2 \oplus \mathbb{Z}_3 \oplus \mathbb{Z}_5 \oplus \mathbb{Z}_5 \oplus \mathbb{Z}_{11} \cong \mathbb{Z}_{10} \oplus \mathbb{Z}_{330}$

b) In $\mathbb{Z}_{3300}$, $\langle 10 \rangle$

In $\mathbb{Z}_2 \oplus \mathbb{Z}_{1650}$, $\langle (0,5) \rangle$

In $\mathbb{Z}_5 \oplus \mathbb{Z}_{660}$, $\langle (0,2) \rangle$

In $\mathbb{Z}_{10} \oplus \mathbb{Z}_{330}$, $\langle (0,1) \rangle$

3. a)

b) $\operatorname{char}(\mathbb{Z}_m \oplus \mathbb{Z}_n) = \operatorname{lcm}(m,n)$

$\operatorname{char}\begin{pmatrix} \mathbb{R} & \mathbb{R} \\ 0 & \mathbb{R} \end{pmatrix} = \operatorname{lcm}(m,n)$

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) units $\mathbb{Z}^\times = \{ \pm 1 \}$

units in $\mathbb{Z} \oplus \mathbb{Q} = \{ (\pm 1, q) \mid q \neq 0, q \in \mathbb{Q} \}$

$(\pm 1, q) \cdot (\pm 1, q^{-1}) = (1,1)$

6. a) $\mathbb{Z}[i] = \{ m + ni \in \mathbb{C} \mid m, n \in \mathbb{Z} \}$

$I = \langle 1 + 3i \rangle$

$(1+3i)(1-3i) = 10$, so $10 \in \langle 1+3i \rangle$

In R/I, $10 = 0$

$(1+3i)(1-2i) = 7+i$ so $7+i = 0 \quad i = -7$

$R/I = \{ m + ni + \langle 1+3i \rangle \mid m+ni \in \mathbb{Z}[i] \}$

$= \{ m - 7n + \langle 1+3i \rangle \mid m, n \in \mathbb{Z} \}$

$= \{ k + \langle 1+3i \rangle \mid k \in \mathbb{Z} \}$ and $\omega = 0$

$= \{ I, 1+I, 2+I, \ldots 9+I \} \cong \mathbb{Z}_{10}$

b) a) $\varphi : R \to \mathbb{Z}$

$R = \left\{ \begin{pmatrix} a & b \\ b & a \end{pmatrix} \mid a, b \in \mathbb{Z} \right\}$

$\varphi\begin{pmatrix} 1 & 0 \\ 0 & 1 \end{pmatrix} = 1 - 0 = 1$

$\varphi\left(\begin{pmatrix} a_1 & b_1 \\ b_1 & a_1 \end{pmatrix} + \begin{pmatrix} a_2 & b_2 \\ b_2 & a_2 \end{pmatrix}\right) = \varphi\begin{pmatrix} a_1+a_2 & b_1+b_2 \\ b_1+b_2 & a_1+a_2 \end{pmatrix} = (a_1+a_2) - (b_1+b_2) = (a_1 - b_1) + (a_2 - b_2) = \varphi\begin{pmatrix} a_1 & b_1 \\ b_1 & a_1 \end{pmatrix} + \varphi\begin{pmatrix} a_2 & b_2 \\ b_2 & a_2 \end{pmatrix}$

$\varphi\left(\begin{pmatrix} a_1 & b_1 \\ b_1 & a_1 \end{pmatrix}\begin{pmatrix} a_2 & b_2 \\ b_2 & a_2 \end{pmatrix}\right) = \varphi\begin{pmatrix} a_1a_2 + b_1b_2 & a_1b_2 + b_1a_2 \\ b_1a_2 + a_1b_2 & b_1b_2 + a_1a_2 \end{pmatrix} = a_1a_2 + b_1b_2 - a_1b_2 + b_1a_2$

$= (a_1 - b_1)(a_2 - b_2)$

$= \varphi\begin{pmatrix} a_1 & b_1 \\ b_1 & a_1 \end{pmatrix} \cdot \varphi\begin{pmatrix} a_2 & b_2 \\ b_2 & a_2 \end{pmatrix}$

b) $\ker \varphi = \left\{ \begin{pmatrix} a & a \\ a & a \end{pmatrix} \mid a \in \mathbb{Z} \right\}$

c) Given $a \in \mathbb{Z}$, $\varphi\begin{pmatrix} a & 0 \\ 0 & a \end{pmatrix} = a - 0 = a$

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 $R[x] = \{a_0 + a_1x + a_2x^2 + \cdots a_nx^n \mid a_i \in R\}$

$1+x+x^3$, $x+x^2 \in \mathbb{Z}_2[x]$

$(1+x+x^3)+(x+x^2) = 1+2x+x^2+x^3 = 1+x^2+x^3$

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 $f(x) = b_0 + b_1x + b_2x^2 + \cdots b_nx^n \in R[x]$

if $a \in R$, $f(a) = b_0 + b_1a + b_2a^2 + \cdots b_na^n$ 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 $\deg f(x) < \deg r(x)$

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 $f(a)$)

pf: sps $f(a)=0$ 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 $0 = f(a) = c$

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 $n=1$, $f(x) = a_0 + ax$, $a_1 \neq 0$

Sps $f(b) = a_0 + a_1 b = 0 = a_0 + a_1 c = f(c)$

$a_1 b = a_1 c \Rightarrow a_1(b-c) = 0$

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, $f(x) = (x-a)h(x)$

So since R an integral domain, $\deg h(x) = n-1$

By induction, $h(x)$ 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.

$f(x) = 2(x^2+2) = 2(x+i\sqrt{2})(x-i\sqrt{2})$ reducible over $\mathbb{C}$

② $f(x) = x^2 - 2$ irreducible over $\mathbb{Q}$

$= (x-\sqrt{2})(x+\sqrt{2})$ reducible over R.

③ $f(x) = x^2 + 1$ irreducible over $\mathbb{Z}_3$

$= x^2 + 1 = (x-2)(x-3)$ reducible over $\mathbb{Z}_5$

$x^2 - 3x - 2x + 6 = x^2 - 5x + 6$

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 $p(a) = 0$, then $p(x) = (x-a)h(x)$ 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 $\deg f(x)$ or $\deg g(x) = 0$.

Ex. ① $p(x) = x^3 + 3x^2 + x + 2 \in \mathbb{Z}_5[x]$

$p(0) = 2$, $p(1) = 2$, $p(2) = 4$, $p(3) = 4$, $p(4) = 3$ $p(x)$ has no root, so irreducible over $\mathbb{Z}_5$.

② $p(x) = x^4 + 3x^2 + 2$

$= (x^2+1)(x^2+2)$ reducible in $R[x]$ but has no root in R.

Theorem: Let $f(x) \in \mathbb{Z}[x]$, If $f(x)$ is reducible over $\mathbb{Q}$. then it is reducible over $\mathbb{Z}$

Ex: $f(x) = (3x - \frac{9}{2})(4x + \frac{8}{3})$

$= 12x^2 - 10x - 12 \in \mathbb{Z}[x]$ is reducible over $\mathbb{Q}$

$12x^2 - 10x - 12 = (2x-3)(6x+4)$ $f(x)$ is reducible over $\mathbb{Z}$

12/6/19

Theorem (Rational Roots Theorem)

Let $f(x) = a_0 + a_1x + \cdots a_nx^n \in \mathbb{Z}[x]$ where $a_0, a_n \neq 0$,

Let c/d be a root of $f(x)$ expressed in lowest terms (so $\gcd(c,d) = 1$)

then $c \mid a_0$ and $d \mid a_n$.

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

$\pm 1, \pm \frac{1}{2}, \pm \frac{1}{4}, \pm 3, \pm \frac{3}{2}, \pm \frac{3}{4}$

$f(\frac{3}{4}) = 81/64 + 27/64 - 27/4 + 3 - 3 = 108/64 - 108/64 = 0$ thus $(x - \frac{3}{4})$ is a factor of $f(x)$.

$$x - \frac{3}{4} \;\big|\; 4x^4 + x^3 - 3x^2 + 4x - 3$$

$4x^4 - 3x^3$

$4x^3 - 3x^2 + 4x - 3$

$4x^3 - 3x^2$

$4x - 3$

$4x - 3$

0

$4x^3 + 4x^2 + 4$

So $f(x) = (x - \frac{3}{4})(4x^3 + 4x^2 + 4)$

$= (4x - 3)(x^3 + x^2 + 1)$

$x^3 + x^2 + 1$: possible rational roots ± 1

Hence, irreducible over $\mathbb{Q}$.

$f(x)$ reducible over $\mathbb{Z}[x]$

Theorem (Modular irreducibility test)

Let $f(x) \in \mathbb{Z}[x]$, sps prime p exists

such that ① p does not divide the leading coefficient of $f(x)$

② the reduction $\overline{f(x)}$ modulo p is irreducible in $\mathbb{Z}_p[x]$

Then $f(x)$ is irreducible in $\mathbb{Q}[x]$

Ex: $f(x) = x^3 + 4x^2 + 6x + 2$ we show $f(x)$ is irreducible in $\mathbb{Q}[x]$

Reduce mod 3 to obtain $\overline{f(x)} = x^3 + x^2 + 2 \in \mathbb{Z}_3[x]$

$\overline{f}(0) = 2$, $\overline{f}(1) = 1$, $\overline{f}(2) = 2$

Eisenstein Criterion,

Let $f(x) = a_0 + a_1x + \cdots a_nx^n \in \mathbb{Z}[x]$

sps $\exists$ a prime p such that ① p divides each of $a_0, a_1, \ldots a_{n-1}$

② $p \nmid a_n$ and $p^2 \nmid a_0$

then $f(x)$ is irreducible over $\mathbb{Q}$.

Ex. $f(x) = 2x^5 + 27x^3 - 18x + 12$

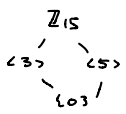
let $p = 3$, $3 \mid 27$, $3 \mid -18$, $3 \mid 12$, $3 \nmid 2$ & $3^2 = 9 \nmid 12$

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



b) $\mathbb{Z}_{15}^\times = \{1, 2, 4, 7, 8, 11, 13, 14\}$ 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

$2^2 = 4$, $2^3 = 8$, $2^4 = 16 = 1$ so $|2| = 4$

So $\mathbb{Z}_{15} \not\cong \mathbb{Z}_2 \oplus \mathbb{Z}_2 \oplus \mathbb{Z}_2$

Note $\mathbb{Z}_8 = \langle 1 \rangle = \langle 3 \rangle = \langle 5 \rangle = \langle 7 \rangle$

$4^2 = 16 = 1$ $|4| = 2$

$7^2 = 49 = 4$ $|7| = 4$

$8^2 = 64 = 4$ $|8| = 4$ that leaves $11, 13, 14 \in \mathbb{Z}_{15}^\times$

$\mathbb{Z}_8$ must contain 4 elements of order 8. So $\mathbb{Z}_{15}^\times \not\cong \mathbb{Z}_8$

We conclude that $\mathbb{Z}_{15}^\times \cong \mathbb{Z}_2 \oplus \mathbb{Z}_4$

c) $H = \langle 5 \rangle = \{0, 5, 10\}$

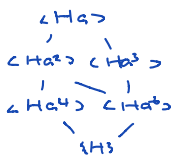
$1 + H = \{1, 6, 11\}$ $2 + H = \{2, 7, 12\}$

$3 + H = \{3, 8, 13\}$ $4 + H = \{4, 9, 14\}$

Index $|G : H| = 5 = |G|/|H| = 15/3$

$G/H = \langle Ha \rangle = \{H, Ha, Ha^2, Ha \dots Ha^{11}\} \cong \mathbb{Z}_{12}$

proper subgroup of G/H are $\langle Ha^2 \rangle \langle Ha^3 \rangle \langle Ha^4 \rangle \langle Ha^6 \rangle$



d) $G/H = \{H, 1+H, 2+H, 3+H, 4+H\} \cong \mathbb{Z}_5$

$G/H = \langle 1 + H \rangle \cong \mathbb{Z}_5$

$\langle 1 + H \rangle$

e) Any homomorphism $\varphi: \mathbb{Z}_9 \to \mathbb{Z}_{15}$ is determined by $\varphi(1)$

$|\varphi(1)|$ will divide 15, so φ is a homomorphism,

$9\varphi(1) = \varphi(9) = \varphi(0) = 0$ therefore $|\varphi(1)|$ also divide 9

$|\varphi(1)|$ divide 9 and 15, So $|\varphi(1)| = 1$ or 3

the homomorphisms $\varphi: \mathbb{Z}_9 \to \mathbb{Z}_{15}$ are

$\varphi(1) = 0$ or $\varphi(k) = 0$

$\varphi(1) = 5$ $\varphi(k) = 5k$

$\varphi(1) = 10$ $\varphi(k) = 10k$

since 5, 10 in $\mathbb{Z}_{15}$ are the only elements of order 3.

$\mathbb{Z}_4 \to \mathbb{Z}_{10}$ is determined by $\varphi(1)$

1, 2 divided 4 & 10, so $|\varphi(1)| = 1$ or 2

$\varphi(1) = 0$ $\varphi(k) = 0$

$\varphi(1) = 5$ $\varphi(k) = 5k$.

2. a) Determine all abelian groups up to isomorphism

a) $72 = 8 \cdot 9 = 2^3 \cdot 3^2$

$\mathbb{Z}_8 \oplus \mathbb{Z}_9 \cong \mathbb{Z}_{72}$

$\mathbb{Z}_2 \oplus \mathbb{Z}_4 \oplus \mathbb{Z}_9 \cong \mathbb{Z}_2 \oplus \mathbb{Z}_{36}$

$\mathbb{Z}_2 \oplus \mathbb{Z}_2 \oplus \mathbb{Z}_2 \oplus \mathbb{Z}_9 \cong \mathbb{Z}_2 \oplus \mathbb{Z}_2 \oplus \mathbb{Z}_{18}$

$\mathbb{Z}_8 \oplus \mathbb{Z}_3 \oplus \mathbb{Z}_3 \cong \mathbb{Z}_3 \oplus \mathbb{Z}_{24}$

$\mathbb{Z}_2 \oplus \mathbb{Z}_4 \oplus \mathbb{Z}_3 \oplus \mathbb{Z}_3 \cong \mathbb{Z}_6 \oplus \mathbb{Z}_{12}$

$\mathbb{Z}_2 \oplus \mathbb{Z}_2 \oplus \mathbb{Z}_2 \oplus \mathbb{Z}_3 \oplus \mathbb{Z}_3 \cong \mathbb{Z}_2 \oplus \mathbb{Z}_6 \oplus \mathbb{Z}_6$

b) How many have exactly three subgroups of order 2?

In $\mathbb{Z}_{72}$, $\langle 36 \rangle$

In $\mathbb{Z}_2 \oplus \mathbb{Z}_{36}$, $\langle 1, 0 \rangle$, $\langle 1, 18 \rangle$, $\langle 0, 18 \rangle$ ✓

In $\mathbb{Z}_2 \oplus \mathbb{Z}_2 \oplus \mathbb{Z}_{18}$, $\langle 1, 0, 0 \rangle$ $\langle 0, 1, 9 \rangle$, $\langle 0, 0, 9 \rangle$, $\langle 0, 1, 9 \rangle$ 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 $\mathbb{Z}_2 \oplus \mathbb{Z}_6 \oplus \mathbb{Z}_6$, $\langle 1, 0, 0 \rangle$, $\langle 1, 3, 0 \rangle$, $\langle 1, 0, 3 \rangle$, ... 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 , $f(x) = q(x)\langle x^2+1 \rangle + r(x)$

where $\deg r(x) < 2$, so $r(x) = a_0 + a_1 x$

$q(x)\langle x^2+1 \rangle \in \langle x^2+1 \rangle = I$

$R/I = \{a_0 + a_1 x + I \mid a_0, a_1 \in \mathbb{Z}_2\}$

$= \{I,\ 1+I,\ x+I,\ 1+x+I\}$