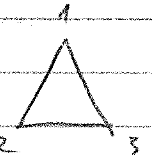
MA333: ABSTRACT ALGEBRA

Prof: Tamar Friedmann

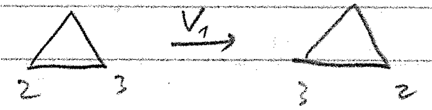
Sep 4, 2019

Groups

Consider equilateral triangle



Flip



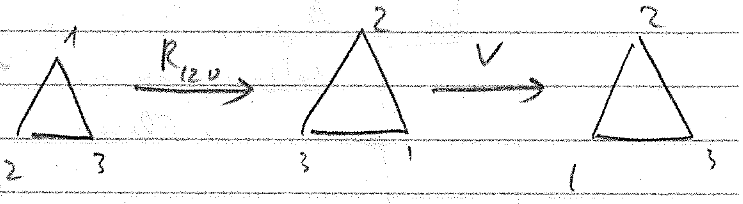
, V_2, V_3

Nothing

Rotate 120° **Rotate 240°**

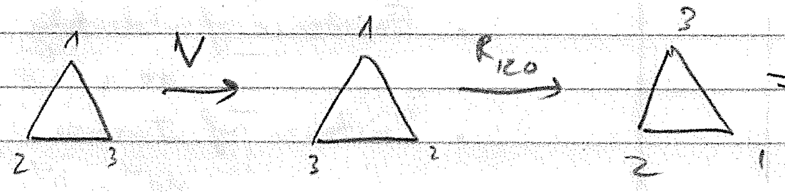
} 6 total

What if $V \cdot R_{120}$



So $V \cdot R_{120} = A$

$R_{120} \cdot V$

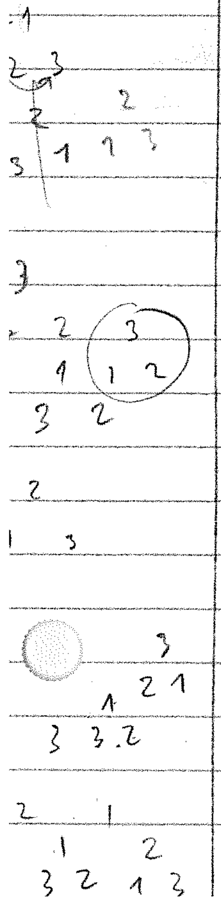


$= B$

Cayley table

Complete table
associativity
"opposite" →

	N	R_{120}	R_{240}	V_1	A_2	B_3
N	N	R_{120}	R_{240}	V_1	A_2	B_3
R_{120}	R_{120}	R_{240}	N	B	V_1	A
R_{240}	R_{240}	N	R_{120}	A	B	V_1
V_1	V_1	A_2	B	N	R_{120}	R_{240}
A_2	A	B_1	V	R_{240}	N	R_{120}
B_3	B	N_2	A_1	R_{120}	R_{240}	N



Definition ⇒ (Group)

A group G is a non-empty set with a rule that <u>assigns</u> to every pair (a, b) of elements in G another element, a product, $ab \in G$ with some properties

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

② There is an element "e" $\in G$ s.t. $ae = ea = a$ $\forall a \in G$ (the identity element)

③ For any $a \in G$ there is an element $a^{-1} \in G$ such that

$$aa^{-1} = a^{-1}a = e$$

"a^{-1}" is called the <u>inverse</u> of a

~~4~~

ep 6, 2019

<u>Recall</u>

<u>Defn</u> A group G is a set with a $\overbrace{\text{binary operation}}^{\text{"group multiplication"}}$ satisfying the following axioms:

- Closure: If $a, b \in G$ then $a \cdot b \in G$ where "$\cdot$" is the binary operation
- Associativity: $(a \cdot b) \cdot c = a \cdot (b \cdot c)$
- Existence of Identity: $\exists\, e \in G$ s.t. for all $a \in G$
  $$ae = ea = a$$
- Existence of Inverse: $\forall a \in G,\ \exists\, \overset{\in G}{a^{-1}}$ s.t.
  $$aa^{-1} = a^{-1}a = e$$

We then say that G is a group <u>under</u> this operation.

<u>Example</u> Do matrices form a group under some operations?

Yes: $+$

☒ $S = \{2 \times 2 \text{ matrices over } \mathbb{R}\}$. $A, B \in S$

Check: $A + B \in S$ ✓

Asso.: $(A+B)+C = A + (B+C)$ ✓

Identity: $\begin{bmatrix} 0 & 0 \\ 0 & 0 \end{bmatrix}$ ✓

Inverse: $-A$ ✓

↳ $n \times m$ matrices under $+$ form a group...

☒ $S = \{$ 2x2 invertible matrices under multiplication $\}$ ✓

☒ $S = \{$ integers under addition $\}$ ✓

☒ $V =$ Vector space? ✓ Vector space → group!

Let V be a vector space. If $v_1, v_2 \in V$ then $v_1 + v_2 \in V$, ✓

$\exists\, 0 \in V \rightarrow$ identity ✓

$\forall\, v, \ \exists\, -v$ s.t. $v + (-v) = 0$ ✓

* * *

$\boxed{\text{A group } G \text{ for which } \forall\, a, b \in G, \text{ we have } ab = ba \text{ is a commutative, or Abelian, group}}$

Ex Dihedral groups:

- sym of △ (D_3) (or S_3)
- sym of □ (D_4)
- sym of regular n-gons (D_n)

△ : 6 elements

□ : 8 elements

n-gons? : $\boxed{?}$

Defn $\boxed{\text{The Order of a finite group } G, \text{ denoted } o(G), \text{ is the number of elements of } G}$

$o(D_3) = 6$

$o(D_4) = 8$ (needs proof)

* * *

$\boxed{\text{Groups of order 1}}$ → {identity}

	e
e	e

{1} under multiplication
{0} under addition

Integers under subtraction → NOT a group (not associative

$\boxed{\text{Groups of order 2}}$

	a	b
a	a	b
b	b	a

$\boxed{\text{What abt } \mathbb{R} \text{ under } \times ?}$ NO! bcz of 0

$\boxed{2\times 2 \text{ real matrices under } \times ?}$

▨ $\mathbb{R}\setminus\{0\}$ is now a group, an Abelian group.

▨ 2×2 invertible matrices form a group under multiplication

↳ $\boxed{GL(2,\mathbb{R})}$, similarly ⇒ $\boxed{GL(n,\mathbb{R})}$

▨ $\boxed{\text{Uniqueness of Identity}}$ (by contradiction)

Suppose e & e' are identity. Then $\forall\, a \in G$,

$\left.\begin{array}{l} ae = a \\ ae' = a \end{array}\right\}$ Let $a = e'$, then $e'e = e'$ b/c e id.

Also, similarly, $ee' = e^{*}$ bcz e' id
$= e'e$

So $e' = e'e = e$ So $e' = e$ ⇒ $\boxed{\text{identity is unique}}$

Sep 9, 2019

Cancellation In a group G, if $a, b, c \in G$, then $ab = ac \Rightarrow b = c$
$ba = ca \Rightarrow b = c$

Pf $ab = ac \Rightarrow a^{-1}(ab) = a^{-1}(ac)$

$\Rightarrow (a^{-1}a)\, b = (a^{-1}a)\, c$ by associativity

$\Rightarrow eb = ec$

$\Rightarrow b = c$

Similarly $ba = ca$ ....

Cayley table & Cancellation

$$\begin{array}{c|ccc} & \cdots & g & \cdots \\ \hline e & & eg & \\ a & & ag & \\ b & & bg & \\ \vdots & & \vdots & \end{array}$$

If $o(G) = 6$, how many different elements of the group appears in the column?

If 2 entries in the column are equal, say $ag = bg$, then $a = b$, which is a contradiction. It follows that all entries are distinct $\Rightarrow$ at least $o(G)$ entries. But there are at most $o(G)$

$\Rightarrow$ & all elements in G appear in every column

Same with rows ... (cancellation at front...)

? Sudoku solutions & Cayley table?

Uniqueness of Inverse Suppose b, b' are both inverses of a,

then $ab = e = ab' \Rightarrow b = b'$ by cancellation

$\Rightarrow$ The inverse is unique

Notation if a group is under addition we often write "ng"
if it's under ×, "g^n"

Integers inspired groups – Prime numbers – mod n

$\mathbb{Z}_n = \{0, 1, \ldots, n-1\}$ $n \geq 1$ is a group under addition "mod n

Theorem Division algorithm

- If $a, n \in \mathbb{Z}$ and $n > 0$ then we can divide a by n and write
$$a = nq + r$$
where q is the quotient and r is the remainder $0 \leq r <$
- For given a, n, the q & r are unique

Pf of uniqueness Given a, n. Suppose we have 2 solutions, i.e.

$$a = nq_1 + r_1 = nq_2 + r_2$$

$r_2 = kn + r_1$

To show: $q_1 = q_2$, $r_1 = r_2$

~~well.. $n(q_1 - q_2) + (r_1 - r_2) = 0$~~

$= kn$

$n(q_1 - q_2) + (r_1 - r_2) = 0$, so $r_2 - r_1$ = some multiple of n
$\Rightarrow r_2 > n$
$\Rightarrow$ contradiction.

Pf of existence Consider $S = \{a - nk \mid k \in \mathbb{Z}, a - nk \geq 0\}$

Next time we'll use well-ordering principle to complete the pf

↳ Every set of positive ~~numbers~~ integers has a smallest element.

ep 11, 2019

Existence? → need well-ordering principle!

Axiom (well-ordering principle) → $\boxed{\text{Every nonempty set of positive integers contains a smallest member}}$

↳ use this to prove existence of q, r.

pf

Consider the set $S = \{ a - nk \mid k \in \mathbb{Z}, a - nk \geq 0 \}$

There are 2 cases:

(1) if n divides a, then $a = q \cdot n$ for some q and $r = 0$

(2) if n does not divide a. Then $S = \{ a - nk \mid k \in \mathbb{Z}, a - nk > 0 \}$

S is a set of positive integers, so axiom applies. So, S has a smallest number, called $r = a - n\ell$.

Now, we need to show $0 < r < n$.

- By contradiction, suppose $r \geq n$, then $r - n \geq 0$

So $(a - n\ell) - n \geq 0$

$a - (n)(\ell + 1) \geq 0$

But since n does not divide a, there is no equality

So

$a - n(\ell + 1) > 0 \Rightarrow a - n(\ell + 1) \in S$

But

$a - n(\ell + 1) < r$. So r is NOT the smallest

$\Rightarrow$ (contradiction)

↯

Ex Addition mod 6 $a \equiv b \bmod 6$ when the remainders of a, b when dividing by 6 are equal

Ex $8 \equiv 2 \bmod 6$, $36 \equiv 42 \bmod 6$

well... $\mathbb{Z}_6 = \{0, 1, 2, 3, 4, 5\}$ under addition...

- Identity : 0
- Inverse of a is $6-a$ since $a + (6-a) = 0 \bmod 6$
- associativity...
- closure...

☒ what about $\mathbb{Z}_6^* = \{1, 2, 3, 4, 5\}$? Is this a group under multiplication mod 6? when is $\mathbb{Z}_n^* = \{1, \ldots n-1\}$ a group under multiplication?

☒ $\mathbb{Z}_6^*$ is not a group under $*$ mod 6.

→ not everybody has an inverse (the last one is always inverse of itself,

$2 \cdot 1 \equiv 2 \cdot 4 \equiv 8 \bmod 6 = 2$

☒ If n prime then n cannot be written as a product of 2 elements. To show $\mathbb{Z}_p^*$ is a group, what do we need to prove?

→ Inverse!

Prime? → A prime is an integer ≥ 2 , divisible only by 1 and itself

t is a divisor of s if $\exists u$ s.t. $s = tu$.

We write t/s. Also, s is a multiple of t.

Relative primeness → Two nonzero integers a & b are relatively prime if they have no common divisors.

$\gcd(a, b) = 1$ ⟸

Thm (Bezout's Lemma) $\boxed{\text{If } \gcd(a,b) = 1 \text{ then } \exists \text{ integers } s, t \text{ such that } as + bt = 1}$

Pf Let $S = \{ am + bn \mid m, n \text{ integers}, am + bn > 0 \}$

It has a smallest element. We will show this element $= 1$.

• Let d be the smallest element. Let $d = as + bt$.

Write $a = d \cdot q + r \quad 0 \le r < d$

$$\text{If } r > 0, \text{ then } r = a - dq = a - (as + bt)q$$
$$= a(1-s)q + b(-tq) \in S$$

$\rightarrow$ contradiction since $r < d$

• So $r = 0$, which means d divides a.

Now, divide d into b... Similarly, d divides b

But because $\gcd(a,b) = 1$, so $\boxed{d = 1}$

Now prove that $\mathbb{Z}_p^*$ is a group (existence of inverses)

p 13, 2019

Existence of inverse in $\mathbb{Z}_p^* = \{1, \ldots p-1\}$, p prime.

Pf = ? To show: if $x \in \mathbb{Z}_p^*$, find $y \in \mathbb{Z}_p^*$ s.t. $xy = 1 \bmod p$.
so that ~~p~~ $y = x^{-1}$

p is prime. $x \in \mathbb{Z}_p^*$, so $\gcd(x, p) = 1$.

So $\exists$ s.t s, t $sx + tp = 1$ (Bezout's Thm)

Thus $(sx + tp) \bmod p \equiv 1 \bmod p \Rightarrow sx \equiv 1 \bmod p$ ~~$\Rightarrow$~~

~~Now, is $x \in \mathbb{Z}_p^*$~~. Let $s = \ell \bmod p$ for some $\ell \in \mathbb{Z}_p^*$

$$1 \bmod p = xs = x(np + \ell) = \underbrace{xnp}_{0 \bmod p} + x\ell \equiv x\ell \bmod p$$

So ℓ is x^{-1}

//

Generalize Bezout's Thm

If $\gcd(a,b) = d$ then $\exists$ integers s,t such that

$as + bt = d$ and $\gcd(a,b)$ is the smallest integer of this form $as + bt$

Pf: We can show the smallest element in $S = \{ma+nb \mid m,n \in \mathbb{Z}, ma+nb>0$ divides both a & b. ~~Let~~ d be the smallest in S. Then $d|a$, $d|b$. Show that d is the greatest common divisor...

- Suppose d' is another common divisor of a & b. Then $\begin{cases} a = d'h \\ b = d'k \end{cases}$

We have $d = as + bt$ for some s,t. So

$$d = d'hs + d'kt = d'(hs+kt) \Rightarrow d > d'$$

So d is the greatest common divisor

//

Euclid's algorithm for finding gcd(a,b)

a into b $\quad a = bq_1 + r_1 \quad 0 \le r_1 < b$

b into r_1 $\quad b = r_1 q_2 + r_2 \quad 0 \le r_2 < r_1$

r_1 into r_2 $\quad r_1 = r_2 q_3 + r_3 \quad 0 \le r_3 < r_2$

$\vdots$

$\vdots$

$$r_{k-2} = r_{k-1} q_k + r_k$$
$$r_{k-1} = r_k q_{k+1}$$

By back-substituting, we can show that $r_k | a$ & $r_k | b$

Exercise (Show that r_k is the greatest common divisor)

Euclid's Lemma : If p is prime, then $p|ab$ then $p|a$ or $p|b$

Hint suppose $p|ab$ but $p \nmid a$. Show $p|b$.

$$\left.\begin{array}{l} a = pk + r_1 \\ b = pn + r_2 \end{array}\right\} \rightarrow ab = p(\quad) + \underbrace{r_1 r_2}_{\neq 0 \bmod p}$$

$\Rightarrow p \nmid ab \rightarrow (\Leftarrow)$ true by contraposition... ✓

Another approach

$$\gcd(a,p) = 1 \Rightarrow 1 = ps + at \Rightarrow b = pbs + \overset{\frown}{abt} = \underbrace{pbs}_{\text{mult } p} + \underbrace{pkt}_{\text{mult of } p}$$

$\Rightarrow b$ is a multiple of p ✓

↯

$(pk+r)b = ph - br = hp - pk \Rightarrow b = \frac{p}{r}(h-k)$ $r < p$ ✓

$b\cancel{0} = p(\,) - pk$

$(pk+ra)b = p(\,)$ $b = p(\,)$

$ab = (pkb) + br = (pk)$

$\boxed{b = pk + r}$ $r + 0$

~~$\gcd(a,p) = 1 \Rightarrow ps + at = 1 \Rightarrow (ab)ks + at = 1 \Rightarrow a(bks + t) = 1$~~

Unique factorization { Every integer > 1 is a prime or a product of primes, and the product is unique up to ordering of the prime factors }

Pf Existence → induction
Uniqueness → use lemma

—//—

Next time ⇝ Subgroup.

Sep 16, 2019 $p|ab \Rightarrow p|a$ or $p|b$ revisited

$ab = (pq_1 + r_1)(pq_2 + r_2) = p(\cdots) + r_1 r_2$

Want r_1 or $r_2 = 0$ if $p|ab$. well… $r_1 r_2 \equiv 0 \bmod p$.

SUBGROUPS

{ A subset $H \subset G$ is a subgroup of a group G if it is itself a group under the same operation, identity, inverses, … }

Thm (If G is a group and H is a non-empty subset of G then
$H \underset{\substack{\uparrow \\ \text{subgroup}}}{\leq} G$ iff $\forall a,b \in H \Rightarrow \underset{\substack{\uparrow \\ \text{closure} \\ \text{multiplication}}}{ab \in H}$ & $\underset{\substack{\uparrow \\ \text{closed under inverse}}}{a^{-1} \in H}$)

Id ↓

Pf Suppose $a \in H \Rightarrow a^{-1} \in H \Rightarrow a(a^{-1}) \in H \Rightarrow e \in H$

Associativity $\forall a,b,c \in H$, $a,b,c \in G$. G is associative, so is H.

[illegible]

non empty

Thm If G is a group and $H \subseteq G$, then if $\forall a,b \in H$, $\underline{ab^{-1}} \in H$, then $H \leq G$

Pf (id). Let $a \in H$. Then $a(a^{-1}) \in H \Rightarrow e \in H$

(associativity) G is associative, so is H

(inverses) Let $a = e$, $b \in H$ then $ab^{-1} \in H \Rightarrow eb^{-1} \in H \Rightarrow b^{-1} \in H$

(closure) Let $x, y \in H \Rightarrow y^{-1} \in H \Rightarrow x(y^{-1})^{-1} \in H \Rightarrow xy \in H$.

Recall $o(G)$ = order of G = # elements in G.

Def Let $g \in G$. The order of g is the smallest positive integer n such that $g^n = e$. The order is denoted $|g|$.

If there is no such n, then $|g|$ is infinite.

Let

$\langle g \rangle = \{ g^m \mid m \in \mathbb{Z} \}$ is the set (group) generated by g.

Thm $\langle g \rangle$ is a subgroup

Pf

(id) : $g^0 = e$ (by def)

(closure) : $g^m g^n = g^{m+n} \in \langle g \rangle$

(inverses) : $g^m g^{-m} = e$

(associativity) : $\langle g \rangle$ is Abelian $\Rightarrow$ associativity follows...

More exs of subgroups

Defn The center of a group, $Z(G)$, is defined by

$$Z(G) = \{a \in G \mid ax = xa \ \forall x \in G\}$$

Fact If G is Abelian, then $Z(G) = G$.

Pf ($Z(G)$ is a subgroup)

(id) $\forall x \in G$, $xe = ex = x \Rightarrow e \in Z(G)$

(closure) Suppose $a, b \in Z(G)$, then $\forall x$, want $(ab)x = x(ab)$

well. $$(ab)x \overset{a(bx)}{\underset{\substack{\uparrow \\ b \in Z(G)}}{=}} a(xb) = axb = (ax)b \to ab \in Z(G)$$

(inv) Show $a^{-1}g = ga^{-1}$ if $a \in Z(G)$

$a \in Z(G)$ so $ag = ga \ \forall g \in G$

so $a^{-1}(ag)a^{-1} = a^{-1}(ga)a^{-1}$

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

$\to a^{-1}g = ga^{-1} \ \forall g \in G \to a^{-1} \in Z(G)$

ep 18, 2019

$o(g) \to$ smallest n s.t. $g^n = e$

Thm Suppose $a \in G$, then

(1) If a has infinite order then all a^i, $i \in \mathbb{Z}$ are distinct
(2) If a has order n, then $\langle a \rangle = \{e, a, \dots a^{n-1}\}$ and if

if $a^i = a^j \Longleftrightarrow i \equiv j \mod n$.

Pf (1) Spose $a^i = a^j$ then

$(a^i)(a^j)^{-1} = e$, so $a^{i-j} = e$. Since order of a is infinite, must have $i = j$.

Pf (2) Suppose $a^i = a^j$ then $a^{i-j} = e$. So $i-j$ can be 0 or n but also more ...

Divide $(i-j)$ into n $\quad i-j = nq + r \quad 0 \le r < n$

So $a^{i-j} = a^{nq+r} = e = a^{qn} \cdot a^r = (a^n)^q a^r = e^q a^r$
$= a^r$

So $a^r = e$, but $r < n$. so $r = 0$

So $i - j = nq$; i.e. $i \equiv j \mod n$

CYCLIC GROUPS

Defn A group G is called cyclic if $\exists a \in G$ s.t. $G = \langle a \rangle$

↳ a cyclic group is always Abelian ...

Ex $\mathbb{Z}$ under addition, generator is 1, −1

$\mathbb{Z}_{12}$: group under + mod 12

{ Find all generators of $\mathbb{Z}_{12}$ & order of all its elements
observations? }

$3 . x = 12t + 1$

$0, 3, 6,$

$\mathbb{Z}_{12} = \{ 1, 2, \ldots\ldots, 11 \}$

Generators: $1, 5, 7, 11$

<u>elements</u>: $1, 2, \ldots\ldots, 11$

<u>order</u> $12, 6, 4, 3, \ldots 12$

If $\gcd(k, 12) = 1$ then k generates $\mathbb{Z}_{12}$

$$o(k) = \frac{12}{\gcd(k, 12)}$$

All orders divide 12

~~**Thm**~~ ~~If k is a generator, then $\langle k \rangle = \langle 1 \rangle = \mathbb{Z}_n$~~

Thm Let $G = \langle a \rangle$. Let $o(G) = o(a) = n$.
Suppose $\gcd(k, n) = 1$. Want: $\langle a^k \rangle = \langle a \rangle$

<u>Want to show</u> $\langle a^k \rangle \subseteq \langle a \rangle$ and $\langle a \rangle \subseteq \langle a^k \rangle$ . .

$$\langle a^k \rangle = \{ e, a^k, a^{2k}, \ldots \} \subseteq \{ e, a, a^2, \ldots \} = \langle a \rangle$$

Need $\langle a \rangle \subseteq \langle a^k \rangle$.

Bézout $\exists\, s, t$ such that $1 = ns + kt$

$$a^1 = a^{ns+kt} = \underbrace{a^{ns}}_{e} \cdot a^{kt} = a^{kt} \in \langle a^k \rangle$$

Thm Let a be an element of order n in G and let k be a positive integer. $(o(a) = n)$

If $\gcd(k,n) = 1$ then $\langle a^k \rangle = \langle a \rangle$

Thm Let a be an element of order n in G & let k be a positive integer, then $o(a) = n$.

$$\langle a^k \rangle = \langle a^{\gcd(n,k)} \rangle \text{ and } o(a^k) = \frac{n}{\gcd(k,n)}$$

Pf Show, $\langle a^k \rangle \subseteq \langle a^{\gcd(n,k)} \rangle$ and $\langle a^{\gcd(n,k)} \rangle \subseteq \langle a^k \rangle$

Suppose $d = \gcd(k,n)$ and suppose $k = dr$

Then $a^k = a^{dr} = (a^d)^r \Rightarrow \langle a^k \rangle \subseteq \langle a^d \rangle$ ✓

By Bézout's ... $d = ns + kt$

$$a^d = a^{ns+kt} = \underbrace{(a^n)^s}_{e} a^{kt} = a^{kt} = (a^k)^t \in \langle a^k \rangle$$

So $\langle a^k \rangle = \langle a^{\gcd(k,n)} \rangle$

Next, show $o(a^k) = \frac{n}{\gcd(n,k)}$

Consider $|a^d| = o(a^d)$ where d divides n.

Well $(a^d)^{n/d} = a^n = e \Rightarrow |a^d| \leq n/d$

If $|a^d| < \frac{n}{d}$, then $\exists\, m < \frac{n}{d}$ s.t. $(a^d)^m = e = a^{dm}$. But $dm < n$

$\Rightarrow$ n is NOT the order of a

$\Rightarrow$ CONTRADICTION

If g generates $\langle g \rangle$, then $|g| = |\langle g \rangle|$

So $|a^d| = n/d$. Now, need to justify

$$|a^k| = |\langle a^k \rangle| = |\langle \underbrace{a^{\gcd(k,n)}}_{\text{divisor of } n} \rangle| \overset{?}{=} |a^{\gcd(k,n)}| = \frac{n}{\gcd(k,n)}$$

Fact $|a^k| = |\langle a^k \rangle|$ ▨

Question If $|a| = n$, then $|\langle a^i \rangle| = |\langle a^j \rangle| \iff \gcd(n,j) = \gcd(n,i)$

Classifying (subgroups of) Cyclic Groups

Question → classify all cyclic groups...

G is cyclic if $\exists\, a \in G$ s.t $G = \{a^i \ldots\}$

Claim For all $n \geq 1$, $\exists!$ cyclic group $\mathbb{Z}_n$ (up to isomorphism)

classification of cyclic groups.

☆ {Classification of subgroups of cyclic groups}.

Thm Every subgroup of cyclic group is cyclic ①

Thm If $G = \langle a \rangle$ and $|G| = n$ then the order of any subgroup is a divisor of n ②

Thm For each positive divisor k of n, $\exists!$ subgroup of G of order k ~~and~~ namely $\langle a^{n/k} \rangle$ ⑦

Pf Let $H \leq \langle a \rangle$. To show it is cyclic.

① . So $H = \{e, a^{k_1}, \dots, a^{k_j}\}$.

. Let S = set of positive powers of a in H.

. If $H \neq \{e\}$, $S \neq \emptyset$, ~~Because~~ if $k_1 < 0$ then $(a^{k_1})^{-1} = a^{-k_1} \in H$ and $-k_1 > 0$

So $-k_1 \in S$. So S is nonempty.

. Suppose $m \in S$ is the smallest number of S. Let $a^k \in H$ for some k. Then $\underset{H}{\underset{\cap}{\boxed{a^k}}} = a^{mq+r} = a^{qm} \cdot a^r$.

$a^m \in H$, $a^k \in H \Rightarrow a^{qm} \in H$ by closure, [illegible].

But $a^r = a^{k-qm} \in H$ by closure. But $r \geq 0$ and $r < m$. And since m smallest, $r = 0$. So $k = qm$, which means

$H = \langle a^m \rangle$. So H is cyclic... //

② If $H \leq \langle a \rangle$ then $H = \langle a^m \rangle$ for some m.

We also show $\langle a^m \rangle = \langle a^{\gcd(n,m)} \rangle$.

So $|H| = \dfrac{n}{\gcd(n,m)}$ is a divisor of n b/c $\dfrac{n}{\gcd}$, $\gcd = n$ //

③ <u>Existence of subgroup of order k</u>

Take $\langle a^{n/k} \rangle$, has order $\dfrac{n}{\gcd(n, n/k)} = k$ ✓

<u>Uniqueness</u> Suppose $H \leq \langle a \rangle$, and $|H| = k$. Then H is cyclic $\Rightarrow H = \langle a^m \rangle$ for some m. To show $H = \langle a^m \rangle = \langle a^{n/k} \rangle$

$$|\langle a^m\rangle| = |\langle a^{\gcd(m,n)}\rangle| = \frac{n}{\gcd(m,n)} = |H| = k$$

So $\gcd(m,n) = \frac{n}{k} \Rightarrow |\langle a^m\rangle| = |\langle a^{n/k}\rangle|$

and here $\langle a^m\rangle = \langle a^{\gcd(m,n)}\rangle = \{a^{n/k}\rangle$

▨

* * *

Ⓟ $\boxed{Q}$ ① How many elements of each order are there in $\mathbb{Z}_{12}$? in $\mathbb{Z}_n$?

② How many elements of each order are there in any group G?

* * *

<u>Verify</u> $\mathbb{Z}_{12}$: $\langle 1\rangle = \{0, \dots, 11\}$ order 12

$\langle 1^{12/6}\rangle = \langle 2\rangle = \{0, 2, \dots, 10\}$ order 6

$\langle 1^{12/4}\rangle = \langle 1^3\rangle = \langle 3\rangle = \{0, 3, 6, 9\}$ order 4

$\langle 1^{12/3}\rangle = \langle 4\rangle = \{0, 4, 8\}$ order 3

$\langle 1^{12/2}\rangle = \langle 6\rangle = \{0, 6\}$ order 2

$\langle 1^{12/1}\rangle = \langle 0\rangle$ order 1

↳ one subgroup per order.

How many <u>elements</u> of a given order are there? $\mathbb{Z}_{12}$, $\mathbb{Z}_n$?

~~⇝ 12 elements of order 12~~
~~1 order 11~~
~~2 10~~
~~3 9~~
~~4 8~~

element	0	①	2	3	4	⑤	6	⑦	8	9	10	⑪
	ϕ	12	6	4	3	12	2	12	3	4	6	12

		#		
order 12	→	4	{1, 5, 7, 11}	gcd(x, 12) = 1 = 12/12 = 1
order 3	→	2	{4, 8}	gcd(x, 12) = 12/3 = 4
order 4	→	2	{3, 9}	gcd(x, 12) = 12/4 = 3
order 6	→	2	{2, 10}	gcd(x, 12) = 12/6 = 2
order 2	→	1	{6}	gcd(x, 12) = 12/2 = 6
order [illegible]	→	1	{0}	gcd(x, 12) = 12/1 = 12

In general...

Euler ϕ function $\phi(n)$ ..

$\phi(1) = 1$

$\phi(n)$ for $n > 1$ is # of positive integers less than n, and relatively prime to n

$\phi(2) = 1$	1
$\phi(3) = 2$	1, 2
$\phi(4) = 2$	1, 3
$\phi(5) = 4$	1, 2, 3, 4
$\phi(6) = 2$	1, 5
$\phi(12) = 4$	1, 5, 7, 11

$|U(n)| = \phi(n)$

$\phi(p) = p - 1$ for p prime.

Thm If d is a divisor of n then # elements of order d in a cyclic group of order n is $\phi(d)$

Pf

We know that there is one subgroup of order d, call it H. H is cyclic.

Suppose $H = \langle a \rangle$ for some $a \in H$. H's generators are of the form

a^k where $\gcd(k, d) = 1$.

So, by defn, # of generators is $\phi(d)$.

Thm ⤳ What is the number ~~ele~~ of elements of order d in a (not necessarily cyclic) group G?

Suppose a has order d. Then $\langle a \rangle$ is cyclic and $\langle a \rangle \subseteq G$.

and $\langle a \rangle$ has $\phi(d)$ elements of order d.

Suppose $b \in G \setminus \langle a \rangle$. Then $\langle b \rangle$ is cyclic and also has $\phi(d)$ elements of order d.

- Does $\langle a \rangle$ & $\langle b \rangle$ share any elements of order d?

Suppose $c \in \langle a \rangle$ & c has order d. $\Rightarrow \langle c \rangle = \langle a \rangle$

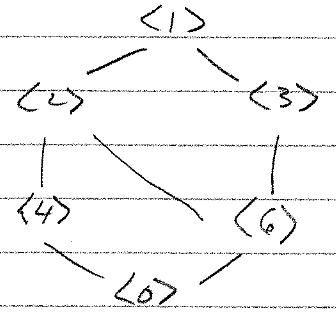
Similarly, $\langle c \rangle = \langle b \rangle$, which means $\langle c \rangle = \langle a \rangle = \langle b \rangle$

So...

Thm The # of elements of order d in a group G is divisible by $\phi(d)$

The set of subgroups of a cyclic group G is an example of a partially ordered set (poset)

$\mathbb{Z}_{12}$



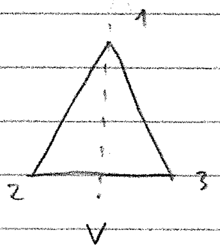
Lines indicate subgroup relation...

Sep 25, 2019

PERMUTATION GROUP

Back to Δ! P_3 sym of Δ. Write all elements of D_3 in the following notation:

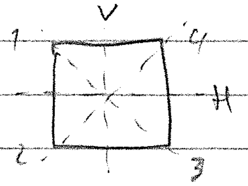
$$\begin{array}{ccc} 1 & 2 & 3 \\ a & b & c \end{array} \rightsquigarrow \text{vertices}$$



$$\begin{pmatrix} & 1 & 2 & 3 \\ V = & 1 & 3 & 2 \end{pmatrix}$$

. Write all 6 of elements of P_3 in this notation & check whether there are any other possibilities for a, b, c not arising ?

Try the same w/ square. (8)



Δ

	1	2	3
V	1	3	2
A	3	2	1
B	2	1	3
R_{120}	3	1	2
R_{240}	2	3	1
e	1	2	3

↳ all perm appeared as sym of Δ of $\{1,2,3\}$

$\square$

	1	2	3	4
e	1	2	3	4
V				
H				

↳ not the case. Many more Perm $\{1,2,3,4\}$ than sym. of $\square$

Defn

The symmetric group S_n consists of all bijections from the set $\{1, 2, 3, \dots, n\}$ to itself, with composition of functions as group multiplication

The elements $\pi \in S_n$ are called "permutations". We multiply right to left, i.e.

$\pi\sigma$ is obtained by applying σ first, then π.

$(f \circ g)(x) = f(g(x))$

Recall: A fn $\phi : A \longmapsto B$ assigns to each element $a \in A$ a unique element $b \in B$ called $\phi(a)$.

A is called the domain, B is the target / co-domain.

$\phi(A) \rightsquigarrow$ image of ϕ = $\mathrm{Im}\,\phi = \{ b \in B \text{ s.t } \phi(a) = b$ for some $a \in A \}$

One-to-one : $\forall b \in \mathrm{Im}\,\phi$, $\exists!\, a \in A$ s.t $\phi(a) = b$

i.e.

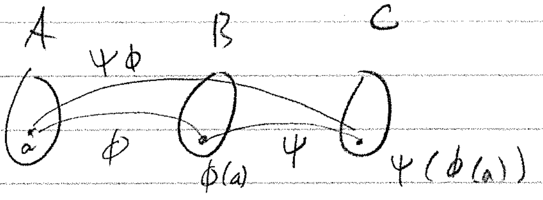
$\phi(a_1) = \phi(a_2) \Rightarrow a_1 = a_2$

Onto $\forall b \in B$, $\exists a \in A$ s.t $\phi(a) = b$., i.e.

$\mathrm{Im}\,\phi = B$

Bijection → One-to-one and onto.

Composition



25

To show associativity

$\phi : A \to B$

$\psi : B \to C$

$\Gamma : C \to D$

To show $\underbrace{\Gamma(\psi\phi)}_{} = \underbrace{(\Gamma\psi)\phi}_{}$

are : $A \longmapsto D$

Test on $a \in A$. $\Gamma(\psi\phi)[a] = \Gamma\left(\psi\phi(a)\right)$

$= \Gamma\left(\psi(\phi(a))\right)$

$= (\Gamma\psi)[\phi(a)]$

$= (\Gamma\psi)\phi(a) \quad \forall a \in A.$

Look at S_5.

	1	2	3	4	5
σ	5	4	1	2	3
π	2	3	1	5	4
$\pi\sigma$	4	5	2	3	1

} line notation

Cycle notation...

$\sigma : 1 \to 5 \to 3 \to 1$ Write $\sigma = (1\ 5\ 3)(2\ 4)$

$2 \to 4 \to 2$

$\pi : (1\ 2\ 3)(4\ 5)$

$\pi\sigma : (1\ 4\ 3\ 2\ 5)$ 👁

$\pi\sigma = (1\,2\,3)(4\,5)(1\,5\,3)(2\,4)$ ⤳ note that there are repeats...

n ⟶ • What is the order of a cycle of length n?

lcm(orders) ⟶ • If $\pi \in S_n$ is written as a product of disjoint cycles, what is its order as a function of the order of cycles?

$$\alpha = (a_1 \ldots a_n)$$

$$\alpha^n(a_1) = a_1 = e(a_1)$$

$$\alpha^n(a_j) = \alpha^n(\alpha^{j-1}(a_1)) = \alpha^{n+j-1}(a_1) = \alpha^{j-1}(\underbrace{\alpha^n(a_1)}_{a_1}) = a_j$$

---

ep 27, 2019

The order of a permutation written in cycle notation is lcm of the lengths of the cycles

Suppose $\sigma = \alpha\beta$ where $|\alpha| = m$, $|\beta| = n$, then $|\sigma| = \text{lcm}(m, n)$

$(\alpha\beta)^k = \alpha^k\beta^k$ because α, β are **disjoint** in cycle notation ...

Suppose $S_n = \{a_1 \ldots a_m\, b_1 \ldots b_n \ldots\}$

↳ then α, β commutes. $(\alpha\beta)x = (\beta\alpha)x$ ...

Want smallest k such that $(\alpha\beta)^k = \alpha^k\beta^k = e$.

It follows ~~that~~ $\alpha^k\beta^k = e$ that $\alpha^k = e = \beta^k$ ⟶ note that they can't be inverses because the otherwise they would be disjoint

↳ $\alpha^k\beta^k = e \Rightarrow \alpha^k = \beta^{-k} \Leftrightarrow \alpha^k = e = \beta^{-k} = \beta^k$

→ k is a multiple of m, n

↳ Smallest k is $\text{lcm}(m, n)$

Note In S_5

$(123) = (123)(4)(5)$

(Ex) Cycle notation

Suppose $\alpha = (1\ 3\ 5\ 2)$ $\quad 1 \to ③ \to ⑤ \to 2 \to 1$

$\alpha^2 = (1\ 5)(3\ 2)$ $\quad 1 \to 3 \to 5 \to 2 \to 1$

$\alpha^3 = (1\ 2\ 5)3)$

↑ you don't get 4

A permutation that involves swaps just two elements is called a transposition

① Write
$\sigma = (1\ 5\ 3)(2\ 4)$
$\pi = (1\ 2\ 3)(4\ 5)$
$\pi\sigma = (1\ 4\ 3\ 2\ 5)$
$\sigma\pi = (1\ 4\ 3\ 5\ 2)$
e
as products of transpositions...

② Then $(a_1 \cdots a_m)$ as product of transposition...

③ Check if you can do it in more than one way.

$(12)(13) =$ ~~[illegible]~~ $(3\ 2\ 1)$

$(153)(24) =$ ~~(24) [illegible]~~

$= (153)(24) = (13)(15)(24) = (24)(13)(15)$
$(123)(45) = (13)(12)(45)$
$(14325) = (15)(12)(13)(14)$
$(14352) = (12)(15)(13)(14)$
$e = (12)(12)$ ~~[illegible]~~

$\boxed{(a_1 \cdots a_m) = (a_1 m)(a_1 a_{m-1}) \cdots (a_1 a_2)}$ → [illegible] ~~[illegible]~~

→ $\boxed{\text{Can write any permutation as a product of transposition. Not unique!}}$

↪ infinitely many ways to write e ....

ct 2, 2019

Thm If the identity e is written as $e = \beta_1 \cdots \beta_r$ where β are transpositions ... then r even

(EC → find proof of thm that is different from the texts...)

Thm If a permutation σ can be written as a product of an <u>even</u>/<u>odd</u> number of transposition then any decomposition of σ has an <u>even/odd</u> number of transposition

<u>Pf</u> say $\sigma = \gamma_1 \cdots \gamma_s = \beta_1 \cdots \beta_r$ where γ_i, β_i are transpositions

Then $(\gamma_1 \gamma_2 \cdots \gamma_s)^{-1} (\beta_1 \cdots \beta_r) = e$

$\iff (\gamma_s^{-1} \cdots \gamma_1^{-1})(\beta_1 \cdots \beta_r) = e$.

<u>Note</u> $\gamma_i^{-1} = \gamma_i$, So we wrote e as a product of transpositions.

Thus $r+s$ even. So r even $\iff$ s even.

<u>Thm</u> $\boxed{\text{All even permutations in } S_n \text{ form a subgroup of } S_n}$

ISOMORPHISM

Defn An *isomorphism* from group G to group $\bar{G}$ is a bijection from G to $\bar{G}$ that preserves the group operation, i.e.

$$\phi : G \mapsto \bar{G} \text{ and } \phi(ab) = \phi(a)\phi(b) \quad \forall\, a,b \in G$$

If such ϕ exists, we say that G & $\bar{G}$ are *isomorphic* and $G \approx \bar{G}$.

E.g. Isomorphisms of vector spaces...

Let V, W be vector spaces. We want an isomorphism

⇒ want: $T: V \mapsto W$ $\quad T$ 1-1 & onto

→ want $T[u +_V v] = T(u) +_W T[v]$

→ T is an invertible linear transformation.

E.g. G: all real numbers under addition

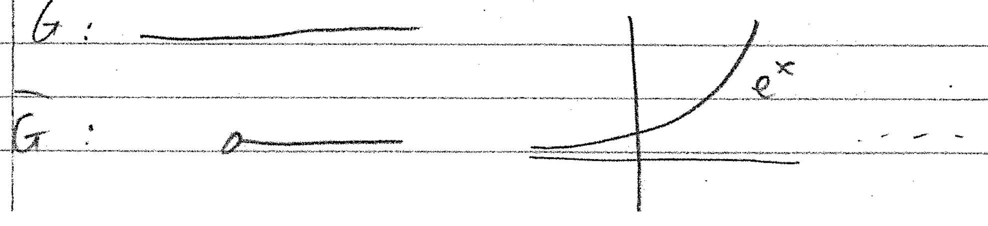
$\bar{G}$: positive real number under multiplication...

Claim these are isomorphic... $\quad , a,b \in \mathbb{R}.$

Pf need $\phi : G \mapsto \bar{G}$ s.t. $\phi[a \overset{\mathbb{R}}{+} b] = \phi(a) \overset{\times}{\cdot} \phi(b)$

↳ $\phi(z) = e^z$.

∎



$\boxed{\text{Ex}}$ Conjugation of $\underbrace{SL_2\mathbb{R}}$ → all (2x2) matrices with det = 1 and real entries ... under matrix multiplication ...

Conjugation: $\phi_M(A) = MAM^{-1}$, M is any real inv 2x2 matrix.

$$\phi : SL_2\mathbb{R} \to SL_2\mathbb{R}$$

<u>Claim</u> ϕ is an isomorphism.

<u>Pf</u> check that $\phi_M(A) \in SL_2\mathbb{R}$

$$\det(MAM^{-1}) = \cancel{\det}(M)\det(A)\cancel{\det(M^{-1})} = \det(A) = 1$$

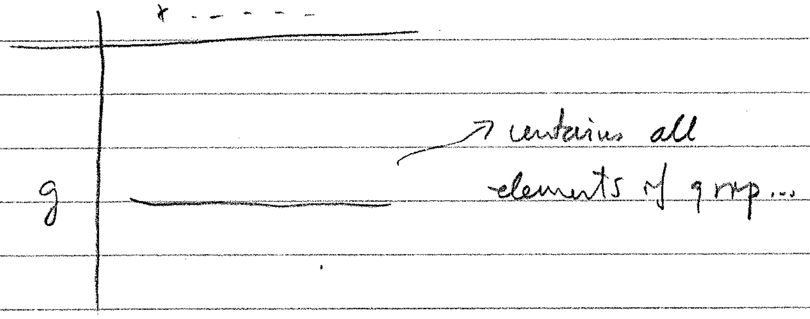
Bijection
$$\begin{cases} MAM^{-1} = MBM^{-1} \Rightarrow A = B \Rightarrow \text{1-to-1} \\ \text{Let } B \in SL_2\mathbb{R}, \text{ Let } A = M^{-1}BM \Rightarrow \phi(A) = B \Rightarrow \text{onto} \end{cases}$$

<u>Preserves multiplication?</u> To show $\phi_M(AB) = \phi_M(A)\cdot\phi_M(B)$

$$\phi_M(AB) = MABM^{-1} = MAM^{-1}MBM^{-1} = \phi_M(A)\phi_M(B)$$

<u>Note</u> $\boxed{\text{Every group can be thought of a group of permutations}}$

For any $g, x \in G$, define $T_g(x) = gx$



Each g can be associated with a permutation.

$8 \equiv 3$ mod
$8 \equiv -3$

(31)

ct 4, 2019

$T_g(x) = gx$ → NOT isomorphism ~~because $T_g(e) = ge \neq e$...~~

↳ $T_g(xy) = g(xy)$, But $T_g(x)T_g(y) = gxgy \neq gxy$. So $T_g(x)$ not ISOM...

$//$

Let

$\overline{G} = \{T_g \mid g \in G\}$. This is a group.

Let

$\phi : G \longmapsto \overline{G}$ be given by $\phi(g) = T_g$. This is an ISOM...

① Onto: any element of $\overline{G}$ is an image of sth in G → ✓ (by defn)

② 1-1: If ~~∀~~ $T_g = T_h$ then $g = h$.

↳ well... If $T_g = T_h$, then $T_g(e) = T_h(e) \Rightarrow ge = he \Rightarrow g = h$ ✓

③ Preserve operation

↳ $\phi(gh) = \phi(g)\phi(h) = T_g T_h$

well.. ↓ ‖

$T_{gh}(x) = ghx = g(hx) = g(hx)$ $\forall x \in G$ ✓

⇒ ϕ is isom... ☐

Recall: Defn of Isomorphism: bijection that preserves operation.

Recall: If T is a lin transform $T: V \to W$ then $\begin{cases} T(0) = 0, \ \text{Im}\,T \to \text{subspace} \\ \ker T \to \text{subspace} \end{cases}$

$\boxed{\text{What properties do isomorphisms have in general?}}$

① $\phi(e) = \overline{e}$, $e \in G$, $\overline{e} \in \overline{G}$

② If $H \leq G$, then $\phi(H) \leq \overline{G}$

③ Set of all isom : $G \longmapsto G$ forms a group, Automorphism

④ $\phi(a^{-1}) = \phi^{-1}(a)$

⑤ $|\phi(a)| = |a|$

⑥ Comp of Isomorphism is an isomorphism

⑦ ϕ^{-1} is an isomorphism...

⑧ If G abelian, and $\phi : G \to \overline{G}$ → $\overline{G}$ abelian...

⑨ $\phi(Z(G)) = Z(\overline{G})$

⑩ $\phi(g^n) = \phi^n(g)$

Pf ① $\phi(e) = \phi(e\cdot e) = \phi(e)\cdot\phi(e)$ ⇒ $\bar{e} = \phi(e)$ by cancellation.

⑩ $\phi(g^n) = \phi^n(g)$?

$n=2$ $\phi(g^2) = \phi(g\cdot g) = \phi^2(g)$ ... then induction ---

$\boxed{\text{Automorphism}}$

An isomorphism from G to itself is an automorphism of G

Ex $SL_2\mathbb{R}$. If $M_{2\times 2}$ invertible then conjugation by M is automorphism of $SL_2\mathbb{R}$.

In general, conjugation by an element in a group is an isomorphism

↳ called $\boxed{\text{inner automorphism}}$

Oct 7, 2019

Defn

G is a group, $a \in G$. Then $\phi_a : G \to G$ given by

$\phi_a(x) = axa^{-1}$ ⇝ is the inner automorphism of the group G induced by a

$\boxed{\text{e.g.}}$ $\mathbb{R}^2$ is a group under addition...

Let $\phi : (x,y) \to (y,x)$ → Automorphism? → Inner?

Fact $\boxed{\text{Innermorphisms of } G \text{ from a group}}$

Pf

ϕ_a, ϕ_b are innermorphisms. Is $\phi_a\phi_b$ also innermorphism?

Closure → $\phi_a\phi_b(x) = \phi_a(bxb^{-1}) = abxb^{-1}a^{-1} = (ab)x(ab)^{-1} = \phi_{ab}(x)$

Inverse → $(\phi_a)^{-1} = \phi_{a^{-1}}$

Associativity holds for composition of functions...

Identity.

Back to example $\mathbb{R}^2$ is abelian $\Rightarrow$ $axa^{-1} = x$

$\rightarrow$ Inner automorphism $=$ Id

$$\boxed{\text{When } G \text{ abelian, an inner automorphism is just the identity}}$$

↳ G abelian $\text{Inn}(G) = \{e\}$ ⇝ trivial group).

So if $\Phi(x,y) = (y,x)$, $\phi \neq e$.

$\boxed{\text{e.g.}}$ $\mathbb{Z}_{10}$. Find $\text{Inn}(\mathbb{Z}_{10})$ and $\text{Aut}(\mathbb{Z}_{10})$. Find structure of

under addition mod 10

↳ all elements in $\text{Aut}(\mathbb{Z}_{10})$. Group structure of $\text{Aut}(\mathbb{Z}_{10})$

$\mathbb{Z}_{10}$ abelian $\Rightarrow$ $\text{Inn}(\mathbb{Z}_{10}) = \{e\}$

Note $|\phi(\text{generator})| = |\text{generator}|$

$\Rightarrow$ $\alpha \in \text{Aut}(\mathbb{Z}_{10})$ takes generator to a generator.

Generators of $\mathbb{Z}_{10}$: $1, 3, 7, 9$

$\alpha_1(1) = 1$ $\quad$ $\alpha_1(3) = \alpha_1(1^3) = \alpha_1(1) + \alpha_1(1) + \alpha_1(1) = 3$

$\alpha_3(1) = 3$

$\alpha_7(1) = 7$ $\quad\vdots$

$\alpha_9(1) = 9$

$$\alpha(k) = \alpha(\underbrace{1 + \dots + 1}_{k}) \underset{\uparrow \atop \text{iso}}{=} \underbrace{\alpha(1) + \dots + \alpha(1)}_{k \text{ times}} = k\alpha(1)$$

$$\boxed{\begin{array}{l}\alpha_1(k) = k\\ \alpha_3(k) = 3k\\ \alpha_7(k) = 7k\\ \alpha_9(k) = 9k\end{array}} \rightsquigarrow \text{This is all of } Aut(\mathbb{Z}_{10})$$

The set of all automorphisms of $\mathbb{Z}_{10}$ is itself a group.

<u>In fact</u> { Aut(G) is a group $\forall G$ }

☆ $|Aut(\mathbb{Z}_{10})| = |\alpha| = 4$, α_1 is the identity.

Find $\alpha_3^2 \Rightarrow \alpha_3(k) = 3k \Rightarrow \alpha_3^2(k) = \alpha_3(3k) = 9k = \alpha_9(k)$

$$\alpha_3^3(k) = \underbrace{27}k \equiv_{10} 7k = \alpha_7(k) \quad , \alpha_3^4 = \alpha_1$$

$\Rightarrow \alpha_3$ is generator of $Aut(\mathbb{Z}_{10})$

$\rightarrow$ multiplication $\Rightarrow \boxed{Aut(\mathbb{Z}_{10}) \approx \mathcal{U}(10)}$

▨ <u>So</u> in general

$$\boxed{Aut(\mathbb{Z}_n) \approx \mathcal{U}(n)}$$

↳ Find $T: Aut(\mathbb{Z}_n) \longrightarrow \mathcal{U}(10)$, T isomorphism

$$\left\{\begin{array}{l} Aut(\mathbb{Z}_{10}) = \{\alpha_1, \alpha_3, \alpha_7, \alpha_9\} \\ \mathcal{U}(10) = \{1, 3, 7, 9\} \end{array}\right.$$

$$\boxed{T(\alpha_j) = j}$$

This is an isomorphism

In general { $T(\alpha) = \alpha(1)$ }

(35)

Cosets & Lagrange's Thm

Idea every subgroup $H \leq G$ allows us to partition G into blocks of size $|H|$. It follows that $|G| \vdots |H|$.

Coset

Defn If $H \leq G$ and $a \in G$, then the right coset Ha of H in G is

$$Ha = \{ ha \mid h \in H \} \quad (\text{left} = \text{right when } G \text{ abelian})$$

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

E.g Let $H = \{0, 5\} \leq \mathbb{Z}_{10}$. (under addition mod 10)

All cosets of H: $H+0 = \{0,5\} = H+5$.

$H+1 = \{1,6\} = H+6$

$H+2 = \{2,7\} = H+7$

$H+3 = \{3,8\} = H+8$

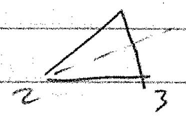
$H+4 = \{4,9\} = H+9$

$H+5 = \{5,0\} = H+0$

$\mathbb{Z}_{10}$ abelian $\Rightarrow$ right & left cosets are the same.

Oct 11, 2014

Let $G = S_3$. $H = \{(1), (13)\}$



Left cosets & right cosets...

$(13)H = eH = \{(1)(13)\}$, $He = \{(1), (13)\}$

$(12)H = \{(12), (12)(13)\}$, $(23)H = \{(23), (23)(13)\} = \{(23), (123)\}$

$= \{(12), (132)\} = (132)H$ $\qquad = (123)H$

$H(12) = \{(12), (13)(12)\} = \{(12), (123)\} = H(123)$

$H(23) = \{(23), (13)(23)\} = \{(23), (132)\} = H(132)$

Properties of cosets

⓪ $\boxed{a \in Ha,\ a \in aH}$

① $\boxed{a \in H \Longleftrightarrow aH = H}$

[illegible] Pf ~~[illegible]~~ if $aH = H$, then since $a \in aH$, $a \in H$.

⇐ if $a \in H$, aH gives row of Cayley table of $H \Rightarrow aH = H$.

② $\boxed{\begin{array}{l} (ab)H = a(bH) \\ H(ab) = (Ha)b \end{array}}$ associativity

③ $\boxed{aH = bH \Leftrightarrow a \in bH}$

$\Rightarrow$ $a \in aH \Rightarrow a \in bH$;

$\Leftarrow$ $a \in bH \Rightarrow a = bh,\ h \in H$

$g \in aH \rightarrow g = ah' = (bh)h' = b(\overbrace{hh'}^{\in H}) \Rightarrow g \in bH.$

$g \in bH \Rightarrow g = bh' \underset{(a \in bH)}{=} (ah^{-1})h' = a(h^{-1}h') \in aH$

④ $\boxed{\text{Either } aH = bH \text{ or } aH \cap bH = \phi}$

$a \in bH$, $b \in aH$ or

If aH ∩ bH ≠ {∅} then aH = bH.

↳ If $g \in aH \cap bH$, then $aH = gH = bH$.

⑤ $\boxed{\text{The number of elements in any coset of } H \text{ is } |H|}$

Pf 1-1, onto correspondence... $T(ah) = bh$. Show T 1-1, onto $aH \to bH$

⑥ $\boxed{aH = bH \iff a^{-1}b \in H}$

⑦ $\boxed{aH = Ha \iff H = aHa^{-1}}$ (not implying Abelian ...)

⑧ $\boxed{aH \leq G \iff a \in H}$

e.g. $\mathbb{R}^3$ under $+$. Subgroup $H = \mathbb{R}^2$ through origin $(0,0,0)$

Cosets ∃ parallel planes not necessarily through origin...

(not subgroup!) ↳ $\underset{\mathbb{R}^2}{\underset{\shortparallel}{H}} + (a+b+c)$

Suppose $g \in G$, $H \leq G$. Then $g \in gH$; $g \in Hg$.
But the cosets are either the same or disjoint ...

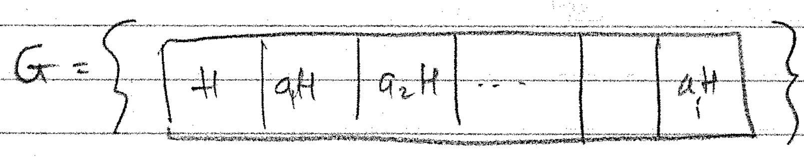
LAGRANGE'S THM

If G is a finite group & $H \leq G$, then $|H|$ divides $|G|$ and the number of distinct cosets of H in G is $|G|/|H| = i_G(H)$, the <u>index</u> of H in G

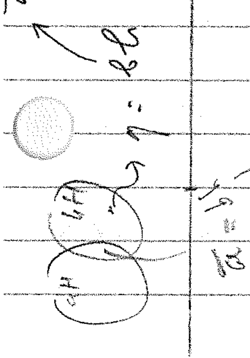
Since cosets are disjoint, and any $g \in G$ is in a coset

$$G = \text{union of cosets} = \bigcup_{a_i}^{r-1} a_iH$$

where a_iH are distinct cosets ...



$$|G| = \text{sum of \# elements in cosets} = \overbrace{|H| + |a_1H| + \dots |a_{r-1}H|}^{r}$$
$$= r|H| \text{ since } |H| = |a_iH|$$



Corollary $\boxed{\text{Any group of prime order is cyclic}}$

$\boxed{|a| \text{ divides } |G| \text{ for any } a \in G}$

If $|G| = p$, then let $a \in G$. ~~But~~

$\langle a \rangle$? $\underset{\overset{\shortparallel}{p}}{|G|} = r \cdot |\langle a \rangle|$ = prime. So either $|\langle a \rangle| = 1$ or $|\langle a \rangle| = p$

So either $\underset{r=p}{|\langle a \rangle| = 1} = \{e\}$ or $\underset{r=1}{\langle a \rangle = G}$ → G cyclic.

Corollary $\boxed{a^{|G|} = e \quad \forall\ a \in G}$

↳ $a^{|G|} = a^{|a| \cdot r} = e^r = e$

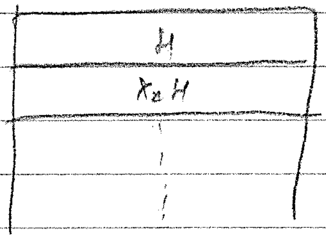
$\boxed{a^p \equiv a \bmod p \quad \text{for prime } p. \quad (\text{think } |U(p)|)}$

$\boxed{\text{If } (a,n) = 1, \text{ then } a^{\phi(n)} \equiv 1 \bmod n}$

Oct 14, 2019

Lagrange's Thm

Picture $G =$



cosets

$H \subset G$

If $|G|$ finite, $|G| = |H| \cdot \underbrace{[G:H]}$

index of H in G # of left cosets...

↳ Apply to when G permutes the elements of some ~~set~~ X.
Let's fix $i \in X$.

What is $\{g \in G \mid g(i) = i\}$ → called STABILIZER of i

$$\boxed{\mathrm{stab}_G(i) = \{g \in G \mid g(i) = i\} \subseteq G}$$

lemma: $\mathrm{stab}_G(i)$ is a subgroup?

Pf
- $1(i) = i$
- $x(i) = i$
- $y(i) = i$ $\Rightarrow xy(i) = x(y(i)) = x(i) = i$

, $x(i) = i \Rightarrow x^{-1}(x(i)) = x^{-1}(i) \Rightarrow i = x^{-1}(i)$

$\Rightarrow \mathrm{stab}_G(i) \leq G$.

□

The orbit of i under G is

$$\boxed{\mathrm{orb}_G(i) = \{g(i) \mid g \in G\} \subseteq X.}$$

Choose a $j \in \mathrm{orb}_G(i)$, then $j = g_0(i)$. What is the set of $g \in G$ s.t. $g(i) = j$?

What is $\{g \in G \mid g(i) = j\}$? ⟶ the left coset $g_0 \cdot \mathrm{stab}_G(i)$

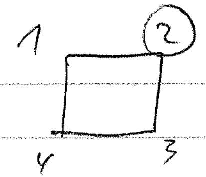
Notice If $h(i) = i$ then $g_0 h(i) = j$

Suppose $g(i) = j = g_0(i) \Rightarrow g_0^{-1} g(i) = g_0^{-1} g_0(i) = 1$

$\Rightarrow g_0^{-1} g \in \mathrm{stab}_G(i)$

So $\boxed{g \in g_0 \cdot \mathrm{stab}_G(i)}$

Ex D_4



What is $\text{stab}_{D_4}(2) = \{d', 1\}$

$D_4 = \{1, r, r^2, r^3, d, d', h, v\}$

Map $2 \to 4$ ... $\{d, r^2\} = d\{1, d'\}$

$\text{orb}_{D_4}(2) = \{1, 2, 3, 4\} \to$ 4 elements $= 8 : 2$

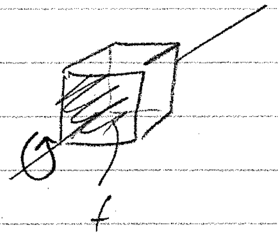
Moral → There is a bijection between elements of the orbit and cosets of the stabilizer.

$|G| = |\text{stabilizer}_G(i)|\,|\text{orbits}_G(i)|$ → ORBIT-STABILIZER THM

when $|G|$ finite → $= |\text{stab}_G(i)|\,|\text{orb}_G(i)| =$

↳ this Thm includes Lagrange's Thm...

Ex $G =$ symmetry group of a cube (rotational)



Let $X =$ set of faces of cube...

$\text{stab}_G(f) =$ 4 rotations around center of face.

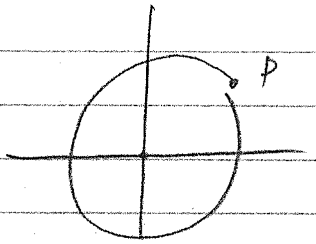
$\text{orb}_G(f) =$ 6 positions.

$\Rightarrow |G| = 24.$

Ex S_7 $X = \{1, 2, 3, 4, 5, 6, 7\}$

$\text{stab}_{S_7}(7) \cong S_6$

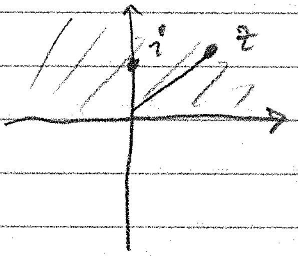
Ex $X = \mathbb{R}^2$, G = all rots around origin. $(0,0)$



$\mathrm{stab}_G(P) = \{1\}$ $\mathrm{orb}_G(P)$ = circle radius OP.

$\mathrm{stab}_G(0) = \{G\}$ $\mathrm{orb}_G(0) = \{0\}$

Ex $X = \mathbb{C}$, positive y $h \subseteq \mathbb{C}$, $h = \{x+iy \mid , y \geq 0\}$



G = 2x2 matrices w/ real entries, det 1

$$\begin{pmatrix} a & b \\ c & d \end{pmatrix} z = \frac{az+b}{cz+d}$$

$$\mathrm{stab}_G(i) = \left\{ \begin{pmatrix} \cos\theta & -\sin\theta \\ \sin\theta & \cos\theta \end{pmatrix} \right\}$$

EXTERNAL DIRECT PRODUCT

Defn Let $G_1 \dots G_n$ is a finite collection of groups. Then the direct external product

$$G_1 \oplus G_2 \oplus \dots \oplus G_n$$

is the set of all n-tuples $(g_1, g_2, \dots g_n)$ with $g_i \in G_i$ with component-wise multiplication

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

This is a group

~~$|G_1 \oplus G_2| = |G_1| \cdot |G_2|$~~ $|G_1 \oplus G_2| = |G_1| \cdot |G_2|$

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

$\mathbb{Z}_2 \oplus \mathbb{Z}_2 = \{(0,0), (0,1), (1,0), (1,1)\}$ ⇝ no generator...

↳ side note $\boxed{\text{Abelian groups of given order not cyclic}}$

Prop $\boxed{(m,n) = 1 \iff \mathbb{Z}_m \oplus \mathbb{Z}_n \text{ has generator, i.e. cyclic}}$

↳ Orders of elements in $G_1 \oplus \cdots \oplus G_n$ ...

$$\boxed{|(g_1, g_2, \ldots, g_n)| = \operatorname{lcm}(|g_1|, |g_2|, \ldots, |g_n|)}$$

For $G_1 \oplus G_2$. Let $t = |(g_1, g_2)|$, $s = \operatorname{lcm}(|g_1|, |g_2|)$

Want $t = s$, i.e. $|(g_1, g_2)| = \operatorname{lcm}(|g_1|, |g_2|)$.

Pf $(g_1, g_2)^t = (g_1^t, g_2^t) = (e, e)$ since $t = |(g_1, g_2)|$

So $\left.\begin{array}{l} g_1^t = e \\ g_1^t = e \end{array}\right\} \Rightarrow t$ = multiple of g_1 and of g_2.

$(g_1, g_2)^s = (g_1^s, g_2^s) = (e, e)$ as well since $s = \operatorname{lcm}(|g_1|, |g_2|)$

So, s must be a multiple of t, i.e. $t \leq s$. But $t \geq s$ bcz t is multiple of s.

So $\boxed{t = s}$

Thus, $\boxed{|(g_1, \ldots, g_n)| = \operatorname{lcm}(|g_1|, \ldots, |g_n|)}$

↳ Can show $\{(m,n) = 1 \iff \mathbb{Z}_m \oplus \mathbb{Z}_n$ cyclic$\}$

Ex $\mathcal{U}(8) \oplus \mathcal{U}(6)$ $\mathcal{U}(8) = \{1, 3, 5, 7\}$

$\mathcal{U}(6) = \{1, 5\}$

$\#$ elements $= 4 \cdot 2 = 8$

$(3, 1) \cdot (3, 5) = (1, 5)$

mod8 mod6

* * *

Ex ① $\mathbb{Z}_9 \oplus \mathbb{Z}_3$. How many elements of order 3?

② $\mathbb{Z}_{36} \oplus \mathbb{Z}_9$. How many cyclic subgroups of order 6 are there?

* * *

① $(a, b) \in \mathbb{Z}_9 \oplus \mathbb{Z}_3$. Know $|(a,b)| = \text{lcm}(|a|, |b|)$

Want $|(a,b)| = 3 = \text{lcm}(|a|, |b|)$

1	3
3	1
3	3

If $(|g_1|, |g_2|) = (1, 3) \Rightarrow (0,1)$ or $(0,2) \in \mathbb{Z}_9 \oplus \mathbb{Z}_3$

If $|g_1| = 3, |g_2| = 1 \Rightarrow (3,0)$ or $(6,0) \in \mathbb{Z}_9 \oplus \mathbb{Z}_3$

If $|g_1| = 3, |g_2| = 3 \Rightarrow (3,1)$ or $(3,2) \in \mathbb{Z}_9 \oplus \mathbb{Z}_3$ or $(6,1)$ or $(6,2)$

} 8

$|(a,b)| = 9$? Allowed orders in $\mathbb{Z}_9 \oplus \mathbb{Z}_3$.

$|\mathbb{Z}_9 \oplus \mathbb{Z}_3| = 27$. Allowed : 1, 3, 9, 27 ...

order 3 : 8 order 27 : 0 $(3,9) \neq 1$

order 1 : 1

$\} \Rightarrow \boxed{\text{order } 9 : 18}$

elements... $|(a,b)| = 9$ if $\underline{|a| = 9}$ and $\underline{|b| = 1, 3}$.

$|U(9)| = 6$ 3 of these.

So <u>18 elements of order 9 in</u> $\mathbb{Z}_9 \oplus \mathbb{Z}_3$.

$\mathbb{Z}_{36} \oplus \mathbb{Z}_9$. Cyclic subgroups of order 6?

<u>Hint</u> $\longrightarrow$ # elements of order 6?

$|\mathbb{Z}_{36} \oplus \mathbb{Z}_9| = 36 \times 9$

$6 = \text{lcm}(|a|, |b|) \Leftarrow |a| = 6, |b| = 1$

6 ~~elements of order 6 in $\mathbb{Z}_{36}$~~

Try $(6,0), (6,3), (6,6) \ldots$

↳ more than 2 elements of order 6. In a cyclic group of order 6, we have 2 elements of order 6. $|U(6)| = 2$.

↳ > 1 cyclic groups of order 6.

Ex Show there are <u>8</u> elements of order 6.

<u>So</u> there are $\frac{8}{2} = 4$ cyclic subgroups of order 6.

$\Rightarrow \mathbb{Z}_{36} \oplus \mathbb{Z}_9$ not cyclic...

Thm If G, H are cyclic, then

$G \oplus H$ cyclic $\Leftrightarrow (|G|, |H|) = 1$

Pf . $m = |G|$, $n = |H|$ $\langle g \rangle = G$, $\langle h \rangle = H$

If $(m, n) = 1$, then $|\langle (g, h) \rangle| = m \cdot n = |G \oplus H|$

$$\underset{\text{lcm}(m,n)}{\underbrace{|\langle (g,h)\rangle| = m\cdot n}}$$

So (g,h) generates $G \oplus H$.

If ~~G⊕H~~ cyclic. If $(m,n) = t > 1$ then

then $g^{m/t}$, $h^{m/t}$ have order t. Then

$\langle (g^{m/t}, e) \rangle$ and $\langle (e, h^{m/t}) \rangle$ are both cyclic groups of order t.

~~But H~~ $\Rightarrow$ $G \oplus H$ not cyclic (contradiction...)

---

ct 18, 2019

To day, we will "divide" by a group to get a group

Defn A subgroup H of G is a normal subgroup of G if $aH = Ha$ $\forall$ $a \in G$

Notation $H \lhd G$: H normal subgroup of G.

Thm Let $H \lhd G$, then the set

$$G/H = \{ aH \mid a \in G \}$$

is a group under the operation $(aH)(bH) = abH$.

This is called the factor group or quotient group of G by H

G/H

Pf Does $(aH)(bH) = abH$ make sense?

i.e.

if $a'H = aH$, $b'H = bH$ then we'd better have

$(a'H)(b'H) = abH = a'b'H$.

If $aH = a'H$, then $a' = ah_1$ for some $h_1 \in H$.

$bH = b'H$, then $b' = bh_2$ for some $h_2 \in H$

To show ~~(CH)~~ $a'b'H = abH$ ...

$$a'b'H = ah_1 b\underbrace{h_2 H} = ah_1 bH$$

H normal

$$= ah_1 Hb \quad (H \trianglelefteq G)$$

$$= aHb = abH \quad ✓$$

Next, show ~~(G/H)~~ G/H is group

Identity: $eH = H$ is identity

~~Ass.~~ $(aH)(bH) = abH \in G/H$ closure

Inv. $(aH)^{-1} = a^{-1}H$

Ass. follows ...

$\square$

Ex $Z(G) \triangleleft G$ since $aZ = Za$. b/c if $z \in Z$ then $az = za \ \forall a \in G$.

Ex If G is abelian, then any subgroup of G is normal

Ex $\mathbb{Z}$ under $+$, $H = 4\mathbb{Z} = \{ n \in \mathbb{Z} \mid n = 4m, m \in \mathbb{Z} \}$

What is $\mathbb{Z}/4\mathbb{Z}$? $\mathbb{Z}/4\mathbb{Z} = \{ 4\mathbb{Z}, 1+4\mathbb{Z}, 2+4\mathbb{Z}, 3+4\mathbb{Z} \}$

$1+4m$ $\quad 2+4m$ $\quad 3+4m$

$aH = bH \iff a \in bH$

So $\mathbb{Z}/4\mathbb{Z} = \{ 4\mathbb{Z}, 1+4\mathbb{Z}, 2+4\mathbb{Z}, 3+4\mathbb{Z} \}$

$\hookrightarrow (aH)(bH) = (abH)$

$(a+4\mathbb{Z})+(b+4\mathbb{Z}) = (a+b+4\mathbb{Z}) =$ ~~(a+b) mod 4~~

"[illegible] "a+b" simplifies to $(a+b) \bmod 4$

So $\mathbb{Z}/4\mathbb{Z} \simeq \mathbb{Z}_4$

$$\boxed{\mathbb{Z}/n\mathbb{Z} \simeq \mathbb{Z}_n}$$

Ex $\mathbb{Z}_n/\langle k \rangle$ where $k \mid n$.

Ex $G = \mathbb{Z}_{20}$, $H = \langle 5 \rangle = \{0, 5, 10, 15\} \leq \mathbb{Z}_{20}$.

$G/H = \{ 0+H, 1+H, 2+H, 3+H, 4+H \}$

E.g. $(3+H) + (4+H) = 7+H = 2+H$

$\to \mathbb{Z}_5$.

$$\boxed{\mathbb{Z}_n/\langle k \rangle = \mathbb{Z}_k} \text{ where } k \mid n.$$

Ex $\boxed{G/Z(G) \simeq \mathrm{Inn}(G)}$

Pf Recall, $\phi_g = \phi_h \iff h^{-1}g \in Z(G)$ where $\phi_g(x) = gxg^{-1}$.

Want to find $T : G/Z(G) \longrightarrow \mathrm{Inn}(G)$ an isomorphism.

Let $T : gZ(G) \longmapsto \phi_g$. Prove T makes sense & isom

Need if $gZ(G) = hZ(G)$ then $T(g(Z(G)) = T(hZ(G))$

{ T 1-1, onto, op. preserving ....

- $gZ(G) = hZ(G) \rightarrow g = ha, \ a \in Z(G) \rightarrow h^{-1}g \in Z(G)$

$$\Updownarrow$$

$$T(gZ(G)) = T(hZ(G)) \Leftrightarrow \underbrace{\phi_g = \phi_h}$$

✓

- Op $T(gZhZ)$

$$T(gZ)T(hZ) = \phi_g \phi_h = \phi_{gh} = T(ghZ)$$

$$= T(gZhZ)$$

- 1-1 $\phi_g = \phi_h \Leftrightarrow h^{-1}g \in Z(G)$

$$\Leftrightarrow g \in hZ(G) \Leftrightarrow gZ = hZ$$

- Onto ϕ_g is image of $gZ(G)$

So $\boxed{G/Z(G) \simeq Inn(G)}$

ct 23, 2019 **Last time** Normal subgroups, factor groups ...

If $H \lhd G$, G/H is a group.

- Let $H \leq Z(G)$

then $H \lhd Z(G)$ (why?)

- Suppose G/H is cyclic. Can we deduce sth about G?

↳ G/H cyclic so it has a generator, call it gH for some $g \in G$

Let $a, b \in G$. We'll show $ab = ba$ ...

$a \in (gH)^i = g^i H$ $\qquad (g_1Hg_2H = g_1g_2H)$

$b \in (gH)^j = g^j H$

So $a = g^i x, \quad x \in H$

$b = g^j y, \quad y \in H$

$x, y \in Z(G)$

Then $ab = (g^i x)(g^j y) = g^i g^j x y$

$= g^{i+j} xy = xy\, g^{i+j}$

$= (g^j y)(g^i x) = ba$

So G is Abelian.

So $\boxed{\text{if } \cancel{H \triangleleft G}\ H \leq Z(G) \text{, then } H \triangleleft G \text{, and if } G/H \text{ cyclic then } G \text{ abelian}}$

Thm: if $H \leq Z(G)$ & G/H is cyclic then G is abelian

Suppose $|G| = pq$, p, q prime.

If $|G|$ not abelian, then $G/\cancel{Z}Z(G)$ not cyclic.

But $|G/Z(G)| = \frac{|G|}{|Z(G)|}$

But $|G| = pq$. If $|Z(G)| = p$ or q then, $\frac{|G|}{|Z|} = q$ or p.

~~But order of cyclic group must~~

But if order of group is prime it must be cyclic.

~~If G~~ G is Abelian, $Z(G) = G$.

Then $|G/Z(G)| = 1$. If G not abelian & $|G| = pq$ then $|Z| = 1$.

Thm $\boxed{\text{if } p \mid |G| \text{ and } p \text{ prime then } \exists \text{ subgroup of } G \text{ of order } p}$

↑ true in general, but we'll prove for G abelian.

Pf By induction on $|G|$. Start with $|G| = 2$. Then $|G|$ has a subgroup of order 2, i.e. G itself. $G \simeq \mathbb{Z}_2$.

Now let $\overset{p \mid n}{|G| = n}$. Assume this is true $\forall\ G'$ when $|G'| < n$

① Find an element of prime order ...

~~②~~ Suppose $x \in G$. Say $|x| = m$. If m prime, done.
If not, then $m = q \cdot d$ where q prime.

So let $z = x^d$, then $z^q = x^{qd} = e$, $|z| = q$.

② $p \mid |G|$. If $q = p$, then done. (subgroup $= \langle x^d \rangle$)

If $q \neq p$, then consider $G/\langle x^d \rangle$. G is abelian.

$$\left| G/\langle x^d \rangle \right| = \frac{|G|}{|\langle x^d \rangle|} = \frac{n}{q}$$

. Use induction to find an element of order $p \in G/\langle x^d \rangle$.

$|G/\langle x^d \rangle| < n$, Let $\overline{G} = G/\langle x^d \rangle$, then $\overline{G}$ has an element of order p.

Say $y\langle x^d \rangle$ has order p.

$(y\langle x^d \rangle)^p = y^p \langle x^d \rangle = \langle x^d \rangle$ ↗ identity in $\overline{G}$

But if $aH = H \Rightarrow a \in H$. So $y^p \in \langle x^d \rangle$, but $|\langle x^d \rangle| = q$ prime.

$y^q \neq e$

So $y^p = e$ or y^p is ~~again~~ the generator of $\langle x^d \rangle$
(done) Then $|y^p| = q$

$\hookrightarrow y^{pq} = e \Rightarrow (y^q)^p = e$

$\hookrightarrow \boxed{y^q \text{ has order } p.}$

(★) Why do we know $y^q \neq e$? $\rightarrow |y\langle z \rangle| = p$

$\hookrightarrow y^p \in \langle z \rangle,\ y \notin \langle z \rangle.$

- If $y^q = 1$, $(y\langle z \rangle)^q = y^q\langle z \rangle = \langle z \rangle$

$\Rightarrow y^q, y^p \in \langle z \rangle$

$\Rightarrow y \in \langle z \rangle$ (Bezout) $\rightarrow$ contradiction.

Defn INTERNAL DIRECT PRODUCT

If $H \triangleleft G$ and $K \triangleleft G$ and $G = HK$ and $H \cap K = \{e\}$ then we say that G is the internal direct product of H & K, denoted

$$G = H \times K$$

Note if $G = H \times K$ then $G \simeq H \oplus K$ (external direct product)

Pf If $H \triangleleft G$, $K \triangleleft G$, $G = HK$, $\forall g \in G$, $g = hk$, $h \in H$, $k \in K$.

Want $H \times K \simeq H \oplus K$

Consider $\phi : H \oplus K \longmapsto$ ~~$H \oplus K$~~ $H \times K$ if $\phi(h, k) = hk$

To show: $\phi(h, k) = hk$ is an isom.

Oct 25, 2019

GROUP HOMOMORPHISMS

Side note
$T : V \rightarrow W$ (linear)
$\ker T \leq V$
$\operatorname{Im} T \leq W$

$A\check{x} = \check{b}$
$\downarrow$
$\check{x} = \check{v}_{\text{particular}} + \{\ker A\}$

Defn A group homomorphism ϕ from G to $\overline{G}$ is a mapping from $G \to \overline{G}$ that preserves the operation.

$$\phi(ab) = \phi(a)\phi(b) \quad \text{(not necessarily an bijective map)}$$

$$\boxed{\ker \phi = \{ x \in G \mid \phi(x) = \bar{e} \in \overline{G} \}}$$

If ϕ is an isom, $\ker \phi = \{e\}$

Let $\phi : \mathbb{Z} \to \mathbb{Z}_n$ $\phi(m) = m \bmod n$.

Can check $\phi(m+n) = \phi(m)\phi(n)$ ✓

$\ker \phi = n\mathbb{Z}$. We also have $\boxed{\underset{G}{\mathbb{Z}} / \underset{\ker\phi}{n\mathbb{Z}} = \underset{\overline{G}}{\mathbb{Z}_n}}$

So $\boxed{\ker \phi \text{ is a normal subgroup...}}$

Properties...

① $\phi(e) = e$

② $\phi(g^n) = \phi^n(g)$

③ $|\phi(g)|$ divides $|g|$ (why?) $|g| = n \Rightarrow |\phi(g)|^n = e \to \dots$

④ $\phi(g) = \bar{g}$ then $\phi^{-1}(\bar{g}) = \{x \in G \mid \phi(x) = \bar{g}\} = g \ker \phi$

Show $\{\ \} \supseteq \subseteq g \ker \phi$ ...

(pre-image)

Show $\phi^{-1}(\bar{g}) = g \ker \phi$.

① $\phi^{-1}(\bar{g}) \in g \ker \phi$. Let $x \in \phi^{-1}(\bar{g})$, then $\phi(x) = \bar{g}$. Look at $g^{-1}x$

$\to \phi(g^{-1}x) = \phi(g^{-1})\phi(x) = \phi(g)^{-1} \cdot \phi(x) = \bar{g}^{-1} \cdot \bar{g} = \bar{e} \Rightarrow g^{-1}x \in g \ker \phi$

$\Rightarrow x \in g \ker \phi$.

(2) $g\ker\phi \subseteq \phi^{-1}(\bar{g})$. If $x \in g\ker\phi \Rightarrow x = gh$

$$\phi(x) = \phi(g)\phi(h) = \bar{g}\cdot\bar{e} = \bar{g} \Rightarrow x \in \phi^{-1}(\bar{g}) \ldots$$

<u>more properties</u>

ϕ takes subgroups of G to subgroups of $\bar{G}$

(normal subgroups of G) → (normal subgroups of $\bar{G}$)

(Abelian/cyclic of G) → (Abelian/cyclic of $\bar{G}$)

If $|\ker\phi| = n$, then ϕ is an n-to-1 map → $|g\ker\phi| = n$ $\forall g$

Oct 28, 2019

$$\begin{tikzcd} G \arrow[r, "\phi"] & \bar{G} \\ \rotatebox{90}{$\leq$}(?) & \rotatebox{90}{$\leq$} \\ \phi^{-1}(\bar{K}) & \bar{K} \arrow[l, bend left] \end{tikzcd}$$

$\phi^{-1}(\bar{K})$: pre image of $\bar{K}$.

If $\bar{K} \leq \bar{G}$, then $\phi^{-1}(\bar{K}) \leq G$ → $\{k \in G \mid \phi(k) \in \bar{K}\}$

Pf ⊙ $e \in \phi^{-1}(\bar{e})$ since $\phi(e) = \underset{\underset{\bar{K}}{\uparrow}}{\bar{e}}$ ⇒ $\phi^{-1}(\bar{K})$ not empty.

⇒ $e \in \phi^{-1}(K)$ ✓

⊙ If $h_1, h_2 \in \phi^{-1}(\bar{K})$ then <u>WTS</u> $h_1h_2^{-1} \in \phi^{-1}(\bar{K})$

$h_1, h_2 \in \phi^{-1}(\bar{K}) \Rightarrow \phi(h_1), \phi(h_2) \in \bar{K}$. $\bar{K}$ is a group, so

$(\phi(h_2))^{-1} \in \bar{K} \Rightarrow \phi(h_2^{-1}) \in \bar{K} \Rightarrow \phi(h_1h_2^{-1}) = \phi(h_1)\phi(h_2^{-1})$

↳ ϕ is homom

$= \phi(h_1)(\phi(h_2))^{-1} \in \bar{K}$

<u>So</u> $h_1h_2^{-1} \in \phi^{-1}(\bar{K})$ ✓

□

$$\boxed{\text{If } \bar{K} \trianglelefteq \bar{G}, \text{ then } \phi^{-1}(\bar{K}) \trianglelefteq G}$$

$$\begin{tikzcd} G \arrow[r, "\phi"] & \bar{G} \\ \bigtriangledown (?) & \bigtriangledown \\ \phi^{-1}(\bar{K}) & \bar{K} \arrow[l] \end{tikzcd}$$

$\bar{K}$ → a subgroup

WTS $\forall x \in G$, $x\phi^{-1}(\bar{K})x^{-1} \in \phi^{-1}(\bar{K})$ (normal, defn)

Let $y \in \bar{K}$. WTS $\phi(x\phi^{-1}(y)x^{-1}) \in \bar{K}$

well... $\phi(x\phi^{-1}(y)x^{-1}) = \phi(x)\,\phi(\phi^{-1}(y))\,\phi(x^{-1})$

$$= \phi(x) \cdot y \cdot (\phi(x))^{-1} \ \underline{\in \bar{K}}$$

$\bar{K} \trianglelefteq \bar{G}$, ~~$= (y\,\phi(x)\,(\phi(x))^{-1} = y \in \bar{K}$~~

$y \in \bar{K}$

$\phi(x) \in \bar{G}$

So Done!

$\square$

$\boxed{\text{kernel of } \phi\,?}$ $\boxed{\ker\phi \trianglelefteq G}$ because in this case $\bar{K} = \{e\}$.

$\boxed{\text{Ex}}$ Find all homom $\mathbb{Z}_{12} \to \mathbb{Z}_{30}$. For each one, find ker, find image. $\phi(\mathbb{Z}_{12}) \leq \mathbb{Z}_{30}$. Try to notice interesting things...

$\phi(x) = x \bmod 30, 29, \ldots, 23.$

Know $\left\{ \begin{array}{l} |\phi(1)| \mid |\mathbb{Z}_{30}| \\ \\ |\phi(1)| \mid |1|_{12} \end{array} \right.$

$\Rightarrow |\phi(1)| = 1, 2, 3, 6.$

If $|\phi(1)| = 1 \Rightarrow \phi(1) = 0,$ $\Rightarrow$ $\underline{\phi(x) = \phi(1 + \cdots + 1) = 0,}$

$|1111| =$ ~~30~~, ~~15~~, 10, ⑥, ③, ②, ①

$|\phi(1)| \mid \underbrace{|111|}$ = 12

$\phi(x) = 2x$ 4x ~~6x~~ 12

- If $|\phi_0(1)| = 1 \Rightarrow \phi(1) = 0 \Rightarrow \phi(x) = 0 \quad \forall x \in \mathbb{Z}_{12}$

$\ker\phi_0 = \mathbb{Z}_{12}$, $\text{Im}\,\phi_0 = \{e\} = \{0\}$.

- If $|\phi(1)| = 2 \Rightarrow \phi(1) = 15 \to \phi(\text{odd}) = 15$
  $\phi(\text{even}) = 0$.

So $\ker\phi = \{0, 2, 4, \dots, 10\}$
$\text{Im}\,\phi = \{0, 15\} \simeq \mathbb{Z}_2 = \phi_{15}(\mathbb{Z}_{12})$

$$|\ker\phi_{15}| \cdot |\phi_{15}(\mathbb{Z}_{12})| = 6 \cdot 2 = \boxed{12}$$

Oct 30, 2014 Recall $\phi(\mathbb{Z}_{12}) \to \mathbb{Z}_{30}$. 1 generates $\mathbb{Z}_{12}$. Determining $\phi(1)$ is sufficient since $\langle 1 \rangle = \mathbb{Z}_{12}$.

$|\phi(1)| \mid 30$ & $|\phi(1)| \mid 12 \to |\phi(1)| = 1, 2, 3, 6$.

$|\phi(1)| = 1 \Rightarrow \phi(1) = 0 \Rightarrow \phi(x) = 0 \quad \ker\phi = \mathbb{Z}_{12}$, $\text{Im}\,\phi = 0$

$|\phi(1)| = 2 \to \phi(1) = 15 \Rightarrow \phi(\text{odd}) = 15 \quad \ker\phi = \{0, 2, 4, \dots, 10\}$
$\phi(\text{even}) = 0 \quad \text{Im}\,\phi = \{0, 15\}$
$(\underset{\mathbb{Z}_6}{\underset{\cong}{\ker\phi_{15}}}| = 6$, $|\underset{\mathbb{Z}_2}{\underset{\cong}{\text{Im}\,\phi_{15}}}| = 2 \to |\ker\phi_{15}||\text{Im}\,\phi_{15}| = 12$

$|\phi(1)| = 3 \to \phi(1) = 10$ or 20

$\ker\phi = \{0, 3, 6, 9\} \sim \mathbb{Z}_4 \qquad 4 \cdot 3 = 12 \dots$
$\text{Im}\,\phi = \{0, 10, 20\} \sim \mathbb{Z}_3$

$|\phi(1)| = 6 \Rightarrow \phi(1) = 5$ or 25
$\ker\phi = \{0, 6, \} \sim \mathbb{Z}_2$
$\text{Im}\,\phi = \{0, 5, 10, 15, 20, 25\} \sim \mathbb{Z}_6$.

<u>So</u> $|\ker\phi|\cdot|\text{Im}\,\phi| = |G|$ for $\phi: G \longrightarrow \bar{G}$, homom.

<u>Suppose</u> $\phi: G \longmapsto \bar{G}$ homomorphism, $\ker\phi \trianglelefteq G$

Let $\psi: \underset{\underset{G/\ker\phi}{\cap}}{g\ker\phi} \longrightarrow \phi(g)$, $g \in G$

<u>Question</u> is ψ an isomorphism?

$\boxed{\psi \text{ is an isomorphism.}}$

$\boxed{G/_{\ker G} \simeq \phi(G)}$ ⇝ First Isomorphism theorem

If $\phi: G \to \bar{G}$ is an homomorphism then $G/_{\ker\phi} \simeq \phi(G)$

<u>Pf</u> <u>Consider</u> $\psi(g\ker\phi) = \phi(g)$ is an isom

<u>Well-defined:</u> If $g\ker\phi = g'\ker\phi$ then $\phi(g) = \phi(g')$

$g\ker\phi = g'\ker\phi$ then $g^{-1}g' \in \ker\phi \Rightarrow \phi(g^{-1}g) = \bar{e}$

<u>So</u> $\phi(g^{-1})\cdot\phi(g') = \bar{e} = (\phi(g))^{-1}(\phi(g')) \Rightarrow \phi(g) = \phi(g')$ ✓

<u>1-1</u> If $\phi(g) = \phi(g')$ then $g\ker\phi = g'\ker\phi$.

$\phi(gg'^{-1}) = \bar{e} \Rightarrow gg'^{-1} \in \ker\phi \Leftrightarrow g\ker\phi = g'\ker\phi$. ✓

Onto By construction ...

Operation preservation $\psi(g\ker\phi)\psi(g'\ker\phi) = \phi(g)\phi(g')$

$$= \phi(gg')$$
$$= \psi(gg'\ker\phi)$$
$$= \psi(g\ker\phi\, g'\ker\phi)$$

✓

□

$\cancel{\psi}$

Corollary If $\phi : G \mapsto \overline{G}$ is a homomorphism, then $|\phi(G)| \,\Big|\, |G|$ and $|\overline{G}|$

Pf

$|\phi(G)| \,\Big|\, |\overline{G}|$ by Lagrange's Thm.

$$|\phi(G)| = \left|G/\ker\phi\right| = |G|/|\ker\phi| \,\Big|\, |G|$$ ✓

$\to$ $|\phi(G)| \cdot |\ker\phi| = |G|$

$$\boxed{\begin{tikzcd} G \arrow[rr, "\phi"] \arrow[dr, "\gamma"'] & & \phi(G) \\ & G/\ker\phi \arrow[ur, "\psi"'] & \end{tikzcd}}$$

"Commutative diagrams"

$\psi(g\ker\phi) = \phi(g)$

$\gamma(g) = g\ker\phi$

So $\boxed{\phi = \psi\gamma}$

Nov 1, 2019

Suppose $N \trianglelefteq G$, is there ϕ s.t $G/N \simeq \phi(G)$?

Sure $\phi(g) = gN$, ker $\phi = \{g \in G \mid \phi(g) = N\} = N$.

Ex

Normalizer

G, $H \le G$. Let $N(H) = \{x \in G \mid xHx^{-1} = H\}$

(Normalizer of H in G)

So $H \trianglelefteq N(H) \le G$

Let $C(H) = \{x \in G \mid xhx^{-1} = h \ \forall h \in H\}$

$C(G) = Z(G)$; $Z(H) \le C(H) \le G$

$\phi(h) = \phi_g(h)$

Consider $\phi : N(H) \longrightarrow \text{Aut}(H)$

$g \longrightarrow \phi_g(h) = ghg^{-1} \ \forall h \in H$

This is an homomorphism $\Rightarrow \phi(g\bar{h}) = \phi_{g\bar{h}} = \phi_g \phi_{\bar{h}}$

kernel of ϕ? ker $\phi = \{?\}$ = pre-image of identity of $\bar{e} \in \text{Aut}(H)$

$\bar{e} \in \text{Aut}(H$ is just $\phi_e \rightsquigarrow$ identity

ker $\phi = \{g \in N(H) \mid \underbrace{ghg^{-1}}_{\phi_g(h)} = h\}$ wtf?

~~[illegible]~~ If $C_{N(H)}(H) = \{x \in N(H) \mid xhx^{-1} = h, \forall h \in H\}$

$\phi : N(H) \longmapsto \text{Aut}(H)$

ker $\phi = C_{N(H)} \Rightarrow C_{N(H)} \trianglelefteq N(H)$.

CLASSIFICATION OF ABELIAN GROUP

Thm Every finite Abelian group is a direct product of cyclic groups whose order is a power of a prime.

This factorization is unique up to ordering of the factors.

i.e. $G \simeq \mathbb{Z}_{p_1^{n_1}} \oplus \mathbb{Z}_{p_2^{n_2}} \oplus \cdots \oplus \mathbb{Z}_{p_k^{n_k}}$

Ex. obs $|G| = \prod_{i=1}^{k} p_i^{n_i}$ → The p's are not necessarily distinct...

Ex

(1) Let $|G| = p^k$, p prime. If $k = 1$, then $G \simeq \mathbb{Z}_p$.

(2) If $h = 2$, $|G| = p^2$. G can be $\mathbb{Z}_{p^2}$ or $\mathbb{Z}_p \oplus \mathbb{Z}_p$

(3) If $h = 3$, $|G| = p^3$. G can be $\mathbb{Z}_{p^3}$, $\mathbb{Z}_{p^2} \oplus \mathbb{Z}_p \simeq (\mathbb{Z}_p \oplus \mathbb{Z}_{p^2})$

$\mathbb{Z}_p \oplus \mathbb{Z}_p \oplus \mathbb{Z}_p$

If $h = 4$ →
4
3 + 1
2 + 2
2 + 1 + 1
1 + 1 + 1 + 1

If $|G| = p^k$ then the isomorphism classes of G correspond 1-1 to partitions of k

$|G| = 2 \cdot 5^2 \cdot 7^3 \Rightarrow G \simeq (\mathbb{Z}_2) \oplus (\;\text{—}\;) \oplus (\;\equiv\;)$

$\mathbb{Z}_2$

$\mathbb{Z}_5 \oplus \mathbb{Z}_5$, $\mathbb{Z}_{25}$

$\mathbb{Z}_{7^3}$, $\mathbb{Z}_{7^2} \oplus \mathbb{Z}_7$, $\mathbb{Z}_7 \oplus \mathbb{Z}_7 \oplus \mathbb{Z}_7$

6 possibilities

Nov 4, 2019

$\boxed{\text{pf}}$

Lemma 1:

If $|G| = p^n m$, G abelian, p prime, $p \nmid m$ then

$$G = H \otimes K \text{ with } H = \{x \in G \mid x^{p^n} = e\}, \quad K = \{x \in G \mid x^m = e\},$$

where $|H| = p^n$ & $|K| = m$

It follows (by induction) that if $|G| = p_1^{n_1} p_2^{n_2} \cdots p_k^{n_k}$ then

$$G = G(p_1) \otimes G(p_2) \otimes \cdots \otimes G(p_n), \quad |G(p_i)| = p_i^{n_i}$$

product →

($\times$ → internal direct product)

Lemma 2

If $|G| = p^n$, p prime, G abelian, $a \in G$ has maximal order in G. Then

$$(G) = \langle a \rangle \otimes K$$

cyclic

Lemma 3

If $|G| = p^n$, G abelian, then G is an _internal_ direct product of cyclic subgroups

Lemma 4

uniqueness →

If $G = H_1 \otimes H_2 \otimes H_3 \otimes \cdots \otimes H_m$
$= K_1 \otimes K_2 \otimes \cdots \otimes K_n$

where the orders of the H_i are non decreasing
$- - - K_i - - - - - -$

then $m = n$ and $H_i = K_i$

(pf) **Lemma 1** $|G| = p^n m$, $p \nmid m$. $H, K \le G$.

For $G = H \times K$, need

$$\begin{cases} H \cap K = \{e\} \\ H, K \trianglelefteq G \\ G = HK \end{cases}$$

⑥①

H, K are normal since G abelian

<u>WTS</u> $G = HK$, $H \cap K = \{e\}$.

$\boxed{G = HK}$ Let $x \in G$, $\gcd(p^n, m) = 1$ $\exists\, s,t$ so that $sp^n + tm = 1$

$\underline{x^1 = x^{sp^n} \cdot x^{tm}}$ $\qquad (x^{tm})^{p^n} = x^{\overbrace{(mp^n)}t} = e$ since $mp^n = |G|$

$\Rightarrow x^{tm} \in H$.

Similarly, $x^{sp^n} \in K$

<u>So</u>

$G = HK$ as set.

$\boxed{H \cap K = \{e\}}$ Let $y \in H \cap K \Rightarrow |y| \mid p^n$ & $|y| \mid m \Leftrightarrow |y| = 1$.

$\Leftrightarrow e = y$.

<u>So</u> $G = H \times K$

$\boxed{\text{WTS}}$ $|H| = p^n$. $\quad |G| = |HK| = p^n m \overset{\text{thm}}{=} \dfrac{|H||K|}{\underbrace{|H \cap K|}_{\{e\}}} = |H| \cdot |K|$

<u>So</u> $p^n m = |H| \cdot |K|$. How to show $|H| = p^n$? $\rightarrow$ <u>need</u> $p \nmid |K|$

If $p \mid |K|$ then $\exists$ element of order p in K (thm)
but for $x \in K$, $|x| \mid m$ $\rightarrow$ contradiction.

<u>So</u> $|H| = p^n$, $|K| = m$.

$\boxed{1}$

$\boxed{\text{Lemma 2}}$ $|G| = p^n$. ~~G~~ G abelian, $a \in G$ has max order.

<u>Claim</u>: $G = \langle a \rangle \times K$. for some $K \trianglelefteq G$.

<u>Pf</u> Induction on power of p. (n).

$n = 0 \Rightarrow |G| = 1 = \{e\}$ $\qquad n = 1 \Rightarrow |G| = p \rightarrow$ cyclic $\Rightarrow G = \langle a \rangle$, $a \neq e$.

Assume true for $k < n$. WTS true for $k = n$. Let a have max order, $|a| = p^m$ i.e. $m \leq n$.

- If $m = n$, then $|a| = p^n \Rightarrow \langle a \rangle = G \rightarrow G = \langle a \rangle \times \langle e \rangle$
- If $m < n$, then

$$a^{p^m} = e$$

Also, since a has max order, $x^{p^m} = e \ \forall x \in G$. Find some $b \notin \langle a \rangle$ such that $|b|$ is smallest.

$$|b| = p^l \text{ for some } l \leq m.$$

$|b| = p^l \Rightarrow b^{p^l} = e = (b^p)^{\boxed{p^{l-1}}} = e \Rightarrow |b^p| = p^{l-1} < p^l$. But $|b|$ minimal, so

$$b^p \in \langle a \rangle \Rightarrow b^p = a^i \Rightarrow b^{p^m} = e = (a^i)^{p^{m-1}}$$

So

$$|a^i| = p^{m-1} \Rightarrow a^i \text{ does not generate } \langle a \rangle$$

$$\gcd(i, p^m) \neq 1 \text{. So } p \mid i \Rightarrow i = pj$$

$\langle a^i \rangle < \langle a \rangle$

Nov 6, 2014

So $b^p = a^i = a^{pj} = (a^j)^p \Rightarrow a^{-j} b = c$ satisfies $c^p = e$
(G ablian)

But because $a^{-j} b \neq e$ because $b \notin \langle a \rangle$

So $|a^{-j} b| = p = |c|$. But $b \notin \langle a \rangle$, $c \notin \langle a \rangle$, $|c| = |p|$

And so c has the smallest possible order of an element $\notin \langle a \rangle$, i.e. p.

So $\boxed{|b| = p.}$

We have $\langle a \rangle \cap \langle b \rangle = \{e\}$ b/c if $b^j \in \langle a \rangle$ then since $|b| = p$ prime, $\langle b^j \rangle = \langle b \rangle$. So $b = (b^j)^d$ for some d
$\Rightarrow b \in \langle a \rangle$ (contradiction)

Is $\langle b \rangle$ the group K we need for this lemma...

NO → not enough elements... if $m < n-1$.

Consider $\bar{G} = G/\langle b\rangle$. $|\bar{G}| = p^n/p = p^{n-1}$

Then $|\bar{G}| = p^n/p = p^{n-1}$

$\bar{G} = \langle$ element of max order in $\bar{G}\rangle \times \bar{K}$

Use notation $x\langle b\rangle = \bar{x}$

Consider $\bar{a} = a\langle b\rangle$, a has max order in G.

<u>Claim</u> $\bar{a}$ has max order in $\bar{G}$. In fact $|\bar{a}| = |a| = p^m$.

Suppose $|\bar{a}| < p^m$ then $(\bar{a})^{p^{m-1}} = \bar{e} = \langle b\rangle$

So $(a\langle b\rangle)^{p^{m-1}} = a^{p^{m-1}}\langle b\rangle = \langle b\rangle \to a^{p^{m-1}} \in \langle b\rangle$

contradicts $\langle a\rangle \cap \langle b\rangle = \{e$

$\Rightarrow |\bar{a}| = p^m$. Why is it maximum order in $\bar{G}$?

→ because $|\bar{x}|$ divides $|x|$

By induction, $\bar{G} = \langle \bar{a}\rangle \times \bar{K}$ for some $\bar{K} \leq \bar{G}$.

What is K? → pre image of $\bar{K}$ under $\phi: G \longrightarrow \bar{G}$

So $\boxed{K = \phi^{-1}(\bar{K})}$ → proof in HW $\boxed{k}$

Lemma 3 $G \cong \langle a\rangle \times K$. So $\langle a\rangle$ has prime power order.

Continue to do the same to K

So lemma 3 follows from that.

$|G| = p^n \to G$ is a product of cyclic groups.

Lemma 4 Uniqueness (not gonna do in class).

Nov 8, 2019

RINGS

Defn a Ring $\overset{R}{\vee}$ is a set with 2 binary operations.

Addition $a+b \in R$
multiplication $ab \in R$

s.t.

- R is an abelian group under addition
- associativity of multi' $a(bc) = (ab)c$
- Distributivity $a(b+c) = ab + ac$ and $(b+c)a = ba + ca$

If multiplication is commutative, i.e $ab = ba \ \forall a,b \in R$ then R is called a commutative ring

If R has a multiplicative identity, then R is a unital ring or a ring with unity.

An element of R that has a multiplicative inverse is a unit of the ring.

Ex
rational numbers complex numbers...
matrices: $n \times n$
$\mathbb{Z}_n$ + $\cdot$ mod n
↳ set of units in $\mathbb{Z}_n$? $\boxed{U(n)}$?

Example of ring without multiplicative identity? $\boxed{2\mathbb{Z}}$

Direct sum of rings

$$R_1 \oplus R_2 \oplus \cdots \oplus R_n = \{(a_1, a_2, \ldots, a_n) \mid a_i \in R_i\}$$

+ , $\cdot$ are component wise

Properties

$a \cdot 0 = 0 \cdot a = 0$

$a(-b) = -(ab) = (-a)b$

$(-a)(-b) = ab$

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

$(b-c)a = ba - ca$

If

∃1 then $(-1)\cdot a = -a$, $(-1)(-1) = 1$

If ∃1, it is unique.

If $a \in R$ is a unit (has multiplicative inverse) → it's unique

NOT true abt rings → $\boxed{ab = ac \not\rightarrow b = c}$

Ex $\mathbb{Z}_6$: $3 \cdot 2 \equiv 0$, $3 \cdot 4 \equiv 0$

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

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

$(1,1)(0,0) = (0,0)$

Upshot → unless you really know what you're doing, don't cancel in rings (multiplicative)

SUBRING

↳ a subset S of a ring R is a subring of R if S is itself a ring with the same two operations of R

Subring conditions...

subgroup

$S \leq R$ is a subring of R if $a, b \in S \Rightarrow$ $a - b \in S$, $ab \in S$

closure under mult.

Pf | $a - b \in S \Rightarrow$ S is a subgroup by the one-step subgroup test
$ab \in S \rightarrow$ closed under multiplication...

associativity & dist. come from R.

Ex $\mathbb{Q} < \mathbb{R}$; $\{0\} \leq R$ for any R. ; $R \leq R$
$2\mathbb{Z} \leq \mathbb{Z}$

Subrings of $M_{2\times 2}(\mathbb{R})$ < diagonal / upper triangular

Question

$\{0, 2, 4\} < \mathbb{Z}_6$.

① What's the multiplicative Id in $\mathbb{Z}_6$? (1
② What's the multip Id in $\{0,2,4\}$, if there is one...

	0	2	4
0	0	0	0
2	0	4	2
4	0	2	4

② Unity: an element x s.t. $xy = yx \; \forall y \in R$.
④ is unity in $\{0, 2, 4\}$

$1 \rightarrow$ unity in $\mathbb{Z}_6$. $4 \rightarrow$ unity in $\{0, 2, 4\}$

When can we cancel in rings?

$ab = 0 \Rightarrow a = 0$ or $b = 0$

Suppose $ab = ac$ but $b \neq c$, $a \neq 0$

$ab - ac = 0$
$a(b - c) = 0$

Defn A *zero divisor* is a nonzero element $a \in R$ s.t. $\exists b \in R$, $b \neq 0$ s.t. $ab = 0$.

Def^n An *integral domain* is a commutative ring with unity and **no** zero-divi

Nov 11, 2019 When can we cancel?

Def^n An integral domain is a commutative ring with unity and no zero divisors

Def^n. Zero-divisor is a non-zero element $a \in R$ where R is a commutative ring & $\exists\, b \in R \neq 0$ s.t. $ab = 0$

Ex $\mathbb{R}$, $\mathbb{Z}$, [illegible] → integral domains.

$\mathbb{Z}_4$, $\mathbb{Z}_n$ → $\boxed{\text{not}}$ integral domains.

↳ for n not prime...

int. dom → $\mathbb{Z}[x]$ → polynomials with integer coefs...

2×2 matrices over $\mathbb{Z}$ → not int. dom e.x. $\begin{pmatrix} 0 & 1 \\ 0 & 0 \end{pmatrix}$...

Cancellation If $a, b, c \in$ integral domain, then if $a \neq 0$ and $ab = ac$, $b = c$

Pf $ab = ac \Rightarrow$ [illegible]

↳ $ab - ac = 0 \rightarrow \overset{\neq 0}{a}(b-c) = 0 \rightarrow \boxed{b = c}$

Are there rings that are also groups under ×?

$\mathbb{R}$, $\mathbb{C}$, $\mathbb{Q}$ ... → $\boxed{\text{FIELDS}}$

Def^n → a field is a commutative ring with unity in which every nonzero element ~~has~~ is a unit

i.e. field = ring R which is also an abelian group under ×.
↳ without $R \setminus \{0\}$

$\boxed{\text{Question}}$ Is a field an integral domain... $\boxed{\text{Yes}}$

~~field~~ [illegible] field is an integral domain

$\boxed{\text{An integral domain in general is not a field...}}$

Thm A <u>finite</u> integral domain is a field

(<u>Note</u>: finiteness necessary otherwise $\mathbb{Z}$ is a field)
(which it isn't.

Pf NTS: <u>any nonzero element is a unit</u>.

Suppose $a = 1$. Then $a^{-1} = 1$

Suppose $a \in$ I.D., $a \neq 0, 1$. Find inverse of a...

Idea... consider $\{a, a^2, a^3, \dots\}$. Use this to construct a^{-1}

From finiteness, $\{a, a^2, a^3, \dots\}$ is finite. For $i > j$

$$a^i = a^j \rightarrow a^i = a^{j+i-j} = a^j a^{i-j}$$

$$\Rightarrow a\, a^{i-1} = a^j a^{i-j} \qquad a^{i-j} = 1$$

$$\text{So } a\,(\underbrace{a^{i-j-1}}_{a^{-1}}) = \underline{1}$$

$\mathbb{Z}_n$ for n not prime $\longrightarrow$ not integral domain

$\mathbb{Z}_p$ for p prime $\longrightarrow$ integral domain.

Corollary $\boxed{\mathbb{Z}_p \text{ is a field } \forall\ p \text{ prime}}$

Characteristic of a ring R

Defn The characteristic of a ring R is the least positive integer n s.t. $nx = 0$ $\forall x \in R$. Write $n = \text{char } R$.

If there is no such n, we say $\text{char } R = 0$

$\text{char } \mathbb{Z} = \infty$

$\text{char } \mathbb{Z}_n = n$

Thm If R has unity 1 then:

if 1 has $\overset{\text{ord}}{\infty}$ order under $+$ then $\text{char } R = 0$

if 1 has order n under $+$ then $\text{char } R = n$

Nov 13, 2019

Pf ⓐ True by definition.

ⓑ Suppose $n \cdot 1 = 0$, n smallest integer, then

$$\forall x \in R, \quad nx = \underbrace{x + \cdots + x}_{n \text{ times}} = \underbrace{1 \cdot x + \cdots + 1 \cdot x}_{n \text{ times}}$$

$$= \underbrace{(1 + 1 + \cdots + 1)}_{n \text{ times}} x = 0x = 0$$

Thm If R is an integral domain then $\text{char } R = 0$ or prime

0	0	0	0	0
a	0	1	a	b
1	0	a	1	a
b	0	b	b	b

$nx = 0$

$x + \cdots + x = 0$

$xy = 1 \cdot x = 1 \cdot y = 0$

Pf check additive order of R.

Suppose $n \cdot 1 = 0$ and n is the smallest such number.
If n not prime i.e. $n = st$ then $n \cdot 1 = (s \cdot t) 1 = 0$

$(s \cdot 1)(t \cdot 1) = 0$

So $s \cdot 1$ or $t \cdot 1 = 0$ since R is I.D. ~~[illegible]~~
Both $s, t < n \Rightarrow$ contradiction.

Is converse true? → FALSE $R: \mathbb{Z}_2 \oplus \mathbb{Z}_2$ under $+$, define all products to be $0 \Rightarrow R$ fails to be I.D. (R w/o unity), char $R = 2$ prime.

Back to non-integral domains

Other than cancellation, what else can go wrong?

Consider

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

Roots are 3 & 1 ⇝ all solutions in $\mathbb{R}$.

What if I want to find all solutions in $\mathbb{Z}_6$?

i.e. all $x \in \mathbb{Z}_6$ s.t. $x^2-4x+3 \equiv_6 0$.

$$(x^2-4x+3) = (x-3)(x-1) \equiv_6 0$$

$x = 1, 3$ are still solutions

Also, ~~that~~ we can have $x-3 \equiv 2$ & $x-1 \equiv 3$ ✗

or $x-3 \equiv 3$ & $x-1 \equiv 2$ ✗

$6 \equiv 2 \cdot 3 \equiv 3 \cdot 4$ or $x-3 \equiv 4$ & $x-1 \equiv 3$ ✗

or $x-3 = 3$ & $x-1 \equiv 4$ ✗

What about $\mathbb{Z}_{12}$? $12 \equiv 3\cdot4 \equiv 2\cdot6 \equiv 4\cdot6 \equiv 6\cdot6 \equiv 6\cdot8$
$\equiv 3\cdot8 \equiv$ ----

$\mathbb{Z}_{12} = \{0, \underset{\smile}{1}, 2, \underset{\smile}{3}, 4, 5, 6, \underset{\smile}{7}, 8, \underset{\smile}{9}, 10, 11\}$

no yes no yes no no no yes no yes no no

In $\mathbb{Z}_p$ for p prime → only have 3 & 1 since this is an integral domain.

Next?

10.8 Quotients of rings, "Normal" subrings

9.7 Iso & homom, products ...

8.

7.5

4 -

Nov 15, 2019

Chap 16: Analogy of normal subgroups is "Ideals" in rings.

Def^n A subring A of a ring R is a two-sided ideal of R if $\forall r \in R$ $\forall a \in A$, $ar \in A$ and $ra \in A$

Normal $gHg^{-1} \subseteq H$

Here $\rightarrow$ $Ar \subseteq A$, $rA \subseteq A$

Def^n An ideal A is a proper ideal if A is a proper subset of R.

Testing a subset to see if it is an ideal...

$$\left\{ \begin{array}{ll} \cdot\ a-b \in A \text{ if } a,b \in A & \longrightarrow \text{subgroup } (+) \\ \cdot\ ra, ar \in A \text{ when } a \in A,\ r \in R. & \longrightarrow \text{closure...} \end{array} \right\}$$

E.g. Find an ideal in $\mathbb{Z}$. $\rightsquigarrow$ $\{n\mathbb{Z}\ \forall n \in \mathbb{Z}.\}$

Principal Ideal

For R commutative w/ 1, if $a \in R$

$$\langle a \rangle = \{ra \mid r \in R\}$$

is an ideal called principal ideal generated by a.

E.g. $R = \mathbb{R}[x]$ all polynomials with real coefs...

Ideal: A all polys with no constant terms...

$$= \{c_1x + c_2x^2 + \dots + c_kx^k \mid c_i \in \mathbb{R}\}$$

Question is A a principal ideal? $\boxed{A = \langle x \rangle}$

Yes

If R is commutative w/ 1, if $a_1, a_2, \dots, a_n \in R$ then

$$I = \langle a_1, a_2, \dots, a_n \rangle = \{ ra_1 + r_2a_2 + \dots + r_na_n \mid r_i \in R \}$$

is the ideal generated by a_i's.

If A is an ideal in R then cosets of A, $\{r+A \mid, r \in R\}$ form a ring..

Thm

Suppose R is a ring and A is an ~~[illegible]~~ subring in R, then the set of cosets of A in R is a ring under the operations

ormality" →

$$(s+A)+(t+A) = (s+t)+A$$
$$(s+A)(t+A) = st+A$$

iff

A is an ideal of R

Pf A is an ideal, then (+) works... Under (+), clear from prior experience. Look at multiplication... Need to check if mult. is well-defined, associative, distributive...

☒ Well-defined... Suppose we have $s+A = s'+A$ and $t+A = t'+A$

Want $st+A$ to be the same coset as $s't'+A$

$s+A = s'+A \to s = s'+a$, $a \in A$

$t+A = t'+A \to t = t'+b$, $b \in A$

so $st = (s'+a)(t'+b) = s't' + at' + s'b + ab$

$$st + A = s't' + \underbrace{at' + s'b + ab}_{\in A} + A = s't' + A. \quad \checkmark$$

→ well-defined.

__Next__ if A not ideal, then product is not well-defined.

$\Rightarrow$ cosets do not form a ring.

Nov 18, 2019

$\Downarrow$

__Pf__ __Suppose__ A is a subring of R but is not an ideal, then $\exists\ r \in R,\ a \in A$ such that ~~[illegible]~~
s.t. $ar \notin A$.

__Now, look at...__

$(a+A)(r+A)$ products should be the same since
$(0+A)(r+A)$ $(a+A) = (0+A)$.

$(a+A)(r+A) = ar + A \neq A$ b/c $ar \notin A$
$(0+A)(r+A) = 0r + A = A$ b/c $0r = 0 \in A$

$\Rightarrow (a+A)(r+A) \neq (0+A)(r+A)$.
So this multiplication is not well defined, when A ideal $\boxed{\Leftarrow}$

__Types of Ideals__ $\rightarrow$ __Principle ideal__ $\langle a \rangle$
$\rightarrow$ __Prime ideal__
$\rightarrow$ __Maximal Ideal__

__Def^n__ $\boxed{\text{Prime ideals}}$ $\rightarrow$ a proper ideal of a commutative ring such that if $a, b \in R$, $ab \in A$ then $a \in A$ or $b \in A$

__Q__: for ~~[illegible]~~ which n is $n\mathbb{Z} \subseteq \mathbb{Z}$ a prime ideal?

$\Rightarrow$ __Answer__: $\boxed{n\mathbb{Z} \subset \mathbb{Z} \text{ is a prime ideal} \Leftrightarrow n \text{ prime}}$

Pf $\searrow$

$a, b \in R$
$ab \mid n \Rightarrow a \mid n$ or $b \mid n$

PC If $n\mathbb{Z}$ prime ideal, then let ~~$x \in n\mathbb{Z} \Rightarrow x = nk$ for some~~
$x, y \in \mathbb{Z}$ and $xy = nk$ for some k.

$\Rightarrow x \in n\mathbb{Z}$ or $y \in n\mathbb{Z}$ ✗(Suppose n not prime, then

$n = zw$ & $z, w \in \mathbb{Z}$, $z, w < n \notin n\mathbb{Z}$)✗

If p prime, then if $x, y \in p\mathbb{Z}$, then $xy = pk$, some k

$p / xy \Rightarrow p/x$ or p/y (Euclid's lemma)

$\Rightarrow x \in p\mathbb{Z}$ or $y \in p\mathbb{Z}$ ... so $p\mathbb{Z}$ prime.

Thm $\boxed{R/A \text{ is an integral domain. (I.D.)} \iff A \text{ is a prime ideal}}$ → R commutative w/ unity

($\Leftarrow$) If A prime ideal. Let $(a+A)(b+A) = A = ab + A$ (hyp)
Then $ab \in A \Rightarrow a \in A$ or $b \in A$.

$\Rightarrow a + A = A$ or $b + A = A$

Since A is zero of R/A, it follows that R/A is I.D.

□

($\Rightarrow$) If R/A is I.D., then supp. ~~R/A~~ $(a+A)(b+A) = A \to 0$ in R/A
then $a + A = A$ or $b + A = A$ (by I.D. prop)

$\Rightarrow a \in A$ or $b \in A$

Also, $(a+A)(b+A) = ab + A = A \Rightarrow ab \in A$

$\Big\}$ $\Rightarrow A$ is prime ideal.

Thm $\boxed{R/A \text{ is a field} \iff A \text{ is Maximal}}$

Suppose R/A is a field, $\Rightarrow R/A$ has unity, called $1 + A$

Suppose $b + A$ is not zero in R/A, i.e. $b \notin A$ then

$(b+A)$ has multiplicative inverse, say $(c+A)$

$\rightarrow (b+A)(c+A) = bc + A = 1 + A$.

By properties of cosets $1 - bc \in A$.

Next, try to construct an ideal that contains both A & $b \notin A$.

Suppose B is an ideal containing A & $b \in A$. Then
B contains (bc) since $b \in B$ an ideal
and $(1-bc)$ since $1-bc \in A \subseteq B$.

So B contains 1 (HW: if ideal contains 1 then ideal $= R$)

So There is no ~~proper~~ ideal B containing A except all R.
$\Leftrightarrow$ no proper ideal B containing R.

$\rightarrow$ A maximal

Def^n A maximal ideal of a commutative ring R is a proper ideal A s.t.
if B is also an ideal, $A \subseteq B \subseteq R$
then $B = A$ or $B = R$

A maximal then A prime

$(\Leftarrow)$ Before proving $(\Leftarrow)$, we look at an example ...

Ex $\langle x^2+1 \rangle$ is maximal in $R[x]$
why?
Suppose $\langle x^2+1 \rangle \subseteq B \subseteq R[x]$, B is an ideal ...
Suppose $f(x) \in B$ and $f(x)$ is not generated by $\langle x^2+1 \rangle$

Then $f(x) = q(x)(x^2+1) + r(x)$, $r(x) \neq 0$

and

$\deg(r(x)) \leq 1$.

So $r(x) = ax+b \neq 0$. Now,

$$ax+b = \underset{\substack{\cap \\ B}}{f(x)} - \underset{\substack{\cap \\ \langle x^2+1\rangle \\ \cap \\ B}}{q(x)(x^2+1)} \in B$$

Next, manipulation to get $1 \in B$, from which it will follow that $B = \mathbb{R}[x]$.

$(ax+b)(ax-b) = a^2x^2 - b^2 \in B$ since B is an ideal that contains $ax+b$. Also, $a^2(x^2+1) \in B$. So,

$$a^2(x^2+1) - (a^2x^2-b^2) = \overbrace{b^2+a^2}^{\neq 0} \in B. \quad (\neq 0 \text{ since } r(x) \neq 0)$$

And so,

$$1 = \frac{1}{a^2+b^2}(a^2+b^2) \in B.$$ So unity of R is in B

So, by HW, $B = \mathbb{R}[x]$.

$\boxed{\text{commutative ring with unity}}$

Now, back to proof Suppose A maximal $\Rightarrow R/A$ field...

Let $b \in R$, and suppose $b \notin A$ so that $\underset{(\neq A)}{b + A}$ is non zero in R/A

We want to find multiplicative inverse for $b + A$.
The idea now is to construct $B \supseteq A$, then $B = R$ (since A maximal, $1 \in B$, then manipulate...)

$$\text{Let } B = \left\{ a + br \;\middle|\; \begin{matrix} a \in A,\ r, b \in R \\ b \notin A \end{matrix} \right\} \supseteq A$$

B contains A

$\Rightarrow$ B larger than A because $b \in B$, $b \notin A$.

$\Rightarrow$ B is all of R because A maximal.

So, $1 \in B \Rightarrow 1 = a + bc$ for some $a, c \in R$. In particular,

$$1 + A = (a + bc) + A = bc + (a + A) = bc + A \qquad (a \in A)$$
$$= (b+A)(c+A)$$

unity in R/A

And so $(c+A)$ is the multiplicative inverse of $(b+A) \in R/A$. This makes R/A a field.

$\square$

$\boxed{Ex}$ We showed that $\langle x^2+1 \rangle$ is maximal in $\mathbb{R}[x]$, and so $\langle x^2+1 \rangle$ is prime in $\mathbb{R}[x]$.

But $\langle x^2+1 \rangle$ is not prime in $\mathbb{Z}_2[x]$.

Take $\langle x \rangle$ in $\mathbb{Z}[x]$: is it prime? is it maximal?

$(x+1)^2 = x^2+1 \in \mathbb{Z}_2[x]$ and $x+1 \notin \langle x^2+1 \rangle$

So $\langle x^2+1 \rangle$ not prime.

$\mathbb{Z}_2[x] / \langle x^2+1 \rangle$

$f(x)(x^2+1) = 0$

$g(x)(x^2+1)$

$\langle x \rangle = \{ a_1 x + \dots + a_n x^n \} \rightarrow$ polys w/o constant terms ...

$= \{ f(x) \in \mathbb{Z}[x] \mid f(0) = 0 \}$ I.D

If $f(x)g(x) \in \langle x \rangle$, then $f(0)g(0) = 0 \rightarrow f(0) = 0$ or $g(0) = 0$

$\Rightarrow f \in \langle x \rangle$ or $g \in \langle x \rangle \rightarrow \langle x \rangle$ prime.

$(x+1) = x^2+1$

But $\langle x \rangle$ not maximal... Call $B = \{ f \in \mathbb{Z}[x] \mid f(0) \text{ even} \}$

Check that $\langle x \rangle \subseteq B \subseteq \mathbb{Z}[x]$

Nov 22, 2014

RING HOMOMORPHISMS

$\phi: R \to S$ that preserves both operations

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

Ex $\phi: \mathbb{Z} \to \mathbb{Z}_n$. $\phi(k) = k \bmod n$.

Recall: group homomorphisms $\mathbb{Z}_{12} \mapsto \mathbb{Z}_{30}$

Generators of $\mathbb{Z}_{12}$: 1, 5, ...
Can pick

$$1 \mapsto \overset{\checkmark}{0}, 5, \overset{\checkmark}{10}, \overset{\checkmark}{15}, 20, \overset{\times}{25} \ldots$$

Which of these is also a ring homom ...

need to check : $\boxed{\phi(1) = \phi(1)\phi(1)} \to 0, 10, 15, 25$

Properties

① $\forall n \in \mathbb{Z}_+$, $\forall r \in R$

$\phi(nr) = n\phi(r)$, $\phi(r^n) = (\phi(r))^n$

② ϕ (subring of R) : subring of S

③ ϕ (ideal of R) : ideal of S

④ $\phi: R \longrightarrow S \supseteq B$ ideal $\Rightarrow \phi^{-1}(B)$ ideal of R

⑤ If R has unity then if ϕ onto, then $\phi(1)$ is unity of S. (unless $S = \{0\}$).

⑥ ϕ isomorphism $\Longleftrightarrow$ ϕ onto and $\ker(\phi) = \{0\}$

⑦ $\ker \phi$ is an ideal of R.

Pf of 7 $\phi(ra) = \phi(r)\phi(a) = 0 \to ra \in R \ \forall r \in R, a \in \ker\phi$

(8) Every Ideal of R is kernel of some ϕ:

$\phi(r) = r + A$ where A is ideal in R.

$R \longrightarrow R/A$ ...

(9) $\boxed{R/\ker\phi \approx \phi(R)}$ $\rightsquigarrow$ first isom thm for rings...

↳ isomorphism is $\psi(r + \ker\phi) = \phi(r)$ ...

QUOTIENT FIELD

Inspired by $\mathbb{Q} = \{ \frac{a}{b} \mid a, b \in \mathbb{Z}, b \neq 0 \}$

note $\mathbb{Z}$ is an integral domain, $\mathbb{Q}$ is a field...

Thm Let D be an integral domain, then $\exists$ a field F that contains a subring isomorphic to D.

F is called "field of quotients of D"

subring $\{ \frac{a}{1}, a \in \mathbb{Z} \} \approx \mathbb{Z}$

pf $S = \{$ all formal symbols $a/b \mid a, b \in D, b \neq 0 \}$

We say that $\frac{a}{b} = \frac{a'}{b'}$ if $ab' = a'b$ (well-defined)

Look at equivalence classes. Let $\left[\frac{x}{y}\right]$ be the set of all fractions equal to $\frac{x}{y}$

Claim If F is all the different $[x/y]$ then it's a field.

↳ Thm ⟶

Equiv. class.

Nov 25, 2019

Thm

$$\boxed{\begin{array}{l} F = \left\{ [x/y] \mid x, y \in D \text{, an integral domain, } y \neq 0 \right\} \\ \quad \text{is a field} \end{array}}$$

Recall

$$[a/b] = [a'/b'] \iff ab' = a'b$$

need to define (+) and $\cdot$ on F.

Def

$$\left[\frac{a}{b}\right] + \left[\frac{c}{d}\right] = \left[\frac{ad+cb}{bd}\right]$$

$$\left[\frac{a}{b}\right]\left[\frac{c}{d}\right] = \left[\frac{ac}{bd}\right]$$

Are these operations well-defined? i.e.

(+) If $[a'/b'] = [a/b]$ and $[c'/d'] = [c/d]$ then want

$$[a'/b'] + [c'/d'] = [ad+cb/bd] \ldots$$

i.e. $$\left[\frac{a'd' + c'b'}{b'd'}\right] = \left[\frac{ad+cb}{bd}\right]$$

i.e.

$$(a'd' + c'b')bd = (ad+cb)b'd'$$

given

$$ab' = a'b, \quad cd' = c'd,$$

$$a'd'bd + c'b'bd = adb'd' + cbb'd'$$

$$(ab')d'd + (cd')b'b = ab'dd' + cd'bb' \quad ✓$$

So $$[a'/b'] + [c'/d'] = \left[\frac{ad+cb}{bd}\right] \quad ✓$$

→ addition is well-defn ...

(x) <u>Want</u> $\left[\frac{a'}{b'}\right]\left[\frac{c'}{d'}\right] = \left[\frac{ac}{bd}\right]$

i.e.

$$\left[\frac{a'c'}{b'd'}\right] = \left[\frac{ac}{bd}\right] \Leftrightarrow a'c'bd = acb'd' \Leftrightarrow b'c'ad = bc'ad \quad ✓$$

$\to$ (x) is well-defined ...

<u>To show:</u> F is a field

- F has a unit $[1/1]$ where $1 \in D$
- multiplicative inverse of $[a/b]$ is $[b/a]$ for $a \neq 0$

  If $a \neq 0$ then $\left[\frac{0}{b}\right] = [0]$ is the 0 element.
- Is F a group under (+) ?..

  $$[a/b] + [-a/b] = \frac{ab - ab}{b^2} = 0.$$
- F also contains a subring isomorphic to D

  $\hookrightarrow \{[\frac{x}{1}]\} \simeq D$

$\boxed{\text{Chap. 24: SYLOW's Thm}}$

<u>Thm</u> If G is finite group & p prime then if $p^k \,|\, |G|$ then G has at least 1 subgroup of order p^k

$\boxed{\text{Conjugacy classes}}$ $\rightsquigarrow$ give a new way to partition group...

<u>Defn</u> $\rightsquigarrow$

Def^n

$$\boxed{\begin{array}{l}\text{Let } a, b \in G. \text{ Then } a, b \text{ are conjugates in } G \text{ iff } \exists x \\ \text{s.t. } xax^{-1} = b. \text{ The } \underline{\text{conjugacy class}} \text{ of } a \text{ is} \\ \qquad cl(a) = \{ xax^{-1} \mid x \in G \}\end{array}}$$

<u>Are these groups?</u> $\boxed{\text{No}}$ only a group when $\boxed{e \in Cl(a)}$

<u>Ex</u> Find all conjugacy class? $S_3 = \{ (1), (12), (13), (23), (123), (13$

$cl(1) = \{(1)\}$

$cl((12)) = \{ (12), \underbrace{(13)(12)(31)}_{(23)}, \cancel{\underbrace{(23)(12)(32)}_{(12)}}, \underset{(23)}{\cancel{(123)(12)}(132)}, \underset{(13)}{(132)(12)(123)}$

$= \{ (12), (23), (13) \} = cl((13)) = cl(23)$

$ce((123)) = cl((132)) = \{ ~~(123), (132)~~ \}$

$\{ (13), (12), (32) \}$

$cl((12)) = cl((13)) = cl((23)) = cl(123) = cl(132)$

Thm $\boxed{|Cl(a)| = |G : C(a)|, \quad C(a) = \{ x \in G \mid xa = ax \}}$

$p^h = p^{k-n} + ?$

$p^h - p^{h-n} = ?$

$p^{h-n}(p^n - 1)$

$y \in xC(a)$

$xC(a) = yC(a)$

$xax^{-1} = yay^{-1}$

$y^{-1}x a = a y^{-1} x$

$y^{-1}x \in C(a)$

~~(123)(12)(132)~~

$(13)(123)(13) \quad (23)$

$(12)(123)(21)$

$a(a^{-1} \cdots) a^{-1}$

$a^{-1} x a x^{-1} y a y^{-1} a$

$a(a^{-1} x a x^{-1} y a y^{-1} a) a^{-1}$

$(xax^{-1} yay^{-1})$

Dec 2, 2019

Note Conjugacy class is an equivalence relation.

Thm $\boxed{\text{The equivalence classes of an equivalence relation on a set } S \text{ constitute a partition of } S}$

So conjugacy classes partition G.

So $|G| = \sum\limits_{\substack{\text{distinct}\\ \text{conj classes}}} |cl(a)|$

centralizer of a...

Thm $\boxed{|cl(a)| = |G : C(a)| \text{, where } \underset{\hat{G}}{C(a)} = \{x \in G \mid xa = ax\}}$

Pf in $cl(a)$ we have xax^{-1}

in $G : C(a)$ we have $xC(a)$, cosets.

Let $\alpha : G : C(a) \longrightarrow cl(a)$ defined by

$\alpha(xC(a)) = xax^{-1}$.

WTS α is well-defined, 1-1, onto.

Well-defined: if $xC(a) = yC(a)$, then $y \in xC(a)$

so $yay^{-1} = \underset{\overset{\uparrow}{z \in C(a)}}{xzaz^{-1}x^{-1}} = xax^{-1}$

Converse is true → 1-1. Onto by defn.

$\Rightarrow \boxed{\alpha \text{ is a bijection}}$

CLASS EQN

So, $|cl(a)| = |G : C(a)| \Rightarrow \boxed{|G| = \sum\limits_{\substack{\text{over one element}\\ \text{from each conj class}}} |G : C(a)|}$

Note For some $a \in G$, $|cl(a)| = 1$ whenever $a \in Z(G)$.

So, rewrite class eqn:

$$\boxed{|G| = \underset{\substack{\text{sum over}\\ \text{one elmt}\\ \text{from each}\\ \text{conj class}}}{\sum} |G : C(a)| = |Z(G)| + \underset{\substack{\text{over all}\\ \text{conj classes}\\ \text{w/ } >1 \text{ element}}}{\sum} |G : C(a)|}$$

If $|G| = \overset{\text{prime}}{p}^k$. What can we say about $Z(G)$?

Well: $|Z(G)| = |G| - \sum |G|/|C(a)|$

$= p^k - \sum p^k/p^l \quad (l < k \text{ or else } a \in C(a))$

So $p \mid |Z(G)|$ so $\boxed{|Z(G)| \neq 1}$

Thm $\boxed{\text{If } |G| = p^k,\ p \text{ prime, then } |Z(G)| \geq p \text{ and } |Z(G)| \mid p^k \text{ as already known}}$

ec 4, 2019

Corollary $\boxed{\text{If } |G| = p^2,\ p \text{ prime. then } G \text{ abelian}}$

Pf If $|Z(G)| = p^2$, then $Z(G) = G$, so G is abelian
If $|Z(G)| = p$, then $|G/Z(G)| = p$ so it is cyclic

This implies G is abelian. ☐

(1^{st})

Sylow Thm Let G be a finite group and let p be prime. If $p^k \mid |G|$ then G has at least one subgroup of order p^k

Pf Induction on $|G|$. If $|G| = 1$ then obvious.
Assume true for groups of order $< |G|$

Case 1: Suppose G has a subgroup H for which $p^k \| |H|$.

Since $|H| < |G|$, by induction, $\exists\ L \leq H$ s.t. $|L| = p^k$. So, $K < G$, we're done.

Case 2 Suppose G has no proper subgroup H for which $p^k \mid |H|$.

In particular, $p^k \nmid |C(a)| \quad \forall\, a \notin Z(G)$

Class eqn says $|G| = |Z(G)| + \underset{\substack{\text{over conj cl} \\ \text{w/ > 1 element}}}{\sum} |G : C(a)|$

(note: if $a \in Z(G)$ then $C(a) = G$ and $cl(a) = \{a\}$)

now, $|G| = |G : C(a)| \cdot |C(a)|$

$p^k \mid |G|,\ p^k \nmid |C(a)| \Rightarrow p \mid |G : C(a)|$

By class eqn: $p \mid |Z(G)| \Rightarrow Z(G)$ contains an element of order p. (Z abelian)

Let $x \in Z(G)$, $|x| = p$.

So $\langle x \rangle \leq Z(G)$, $Z(G)$ abelian. So $\langle x \rangle \trianglelefteq Z(G)$

So

$G/\langle x \rangle$ is a group and $p^{k-1} \mid |G/\langle x \rangle|$

So $G/\langle x \rangle$ has a subgroup of order p^{k-1} by induction.

Call this subgroup $\bar{H} \leq G/\langle x \rangle$. If we show that $\bar{H} \simeq H/\langle x \rangle$ where $H \leq G$ then we have what we're looking for...

Lemma If $N \trianglelefteq G$, then every subgroup of G/N has the form H/N for some $H \leq G$.

Pf. Let $\phi : G \longmapsto G/N$ be the natural homomorphism $\phi(a) = aN$.

Let $\bar{H} \leq G/N$. Let $\phi^{-1}(\bar{H}) = H \leq G$ b/c ϕ takes subgroups to subgroups

Then $H/N = \phi(H) = \phi(\phi^{-1}(\bar{H})) = \bar{H}$. $\square$

Let $\langle x \rangle = N$, then this H is what we needed. $\square$

Def^n If p is prime and $p \mid |G|$ then if $p^k \mid |G|$ but $p^{k+1} \nmid |G|$, then any subgroup of G of order p^k is a Sylow p-subgroup of G

Corollary If $p \mid |G|$ then G has an element of order p

Dec 5, 2019

Sylow's 2nd Thm If $H \leq G$ and $|H| = p^k$ for some k then $H \leq$ some Sylow subgroup of G

Sylow's 3rd Thm ① any 2 Sylow p group are conjugate

i.e. $\exists x \in G$ s.t. $xAx^{-1} = B$

② The number of Sylow p-groups of G is $\equiv 1 \bmod p$ and divides $|G|$.

Corollary A Sylow p-group is normal $\Leftrightarrow$ it is unique

Ex $|G| = 40$. What orders of subgroups are we guaranteed by 2nd thm? How many might we have for all relevant p?

1, 2, 4, 5, 8, 10, 20, 40

$40 = 2^3 \cdot 5$ $\quad |H| = 1, 2, 4, 8, 5$

$\#$ Sylow p-group.

$\boxed{p = 5 \text{ - is normal}}$

$\begin{cases} n \equiv 1 \bmod p \\ n \mid |G| \end{cases}$ $\begin{cases} p = 5 \rightarrow \boxed{n = 1,} \rightarrow \text{normal.} \\ p = 2 \rightarrow n = 1 \text{ or } 5, \rightarrow \text{possibly normal} \end{cases}$

Sylow p-sg's

Pf of 2nd Let K be a "pyllow". Let $C = \{K_1, K_2, \ldots, K_n\}$ be all conjugates of K, with $K_1 = K$

<u>Lemma</u> Let $\overset{x \in G}{\phi_x} : G \to G$ given by $\phi_x(g) = xgx^{-1}$. Then ϕ_x is an automorphism of G.

1-1: $xgx^{-1} = xg'x^{-1}$, then $g = g'$ by cancellation...

- Onto: for $y \in G$, then $\phi_x(\underbrace{x^{-1}yx}_{\in G}) = y$.
- Op-preserving: $\phi_x(g)\phi_x(h) = \phi_x(gh)$ (easy)

Now, $K_i = xK_1x^{-1}$ for some x. Since ϕ_x 1-1 & onto $\forall x$, $|K_i| = |K|$
So, all K_i are pyllows.

Let S_C be group of permutations of C, the set. For each $g \in G$
Def: $\phi_g : C \to C$ by $\phi_g(K_i) = gK_ig^{-1} = K_j$ for some j.

So, $\phi_g \in S_C$.

Also, consider $T : G \to S_C$ given by $T(g) = \phi_g$. T is a homomorphism:

$$
\begin{aligned}
T(gh)(K_i) &= (gh)K_i(gh)^{-1} \\
&= ghK_ih^{-1}g^{-1} = gT(h)(K_i)g^{-1} \\
&= T(g)T(h)(K_i) \quad \checkmark
\end{aligned}
$$

Here $H \leq G$, so $T(H) \leq S_C$. Also, $|H|$ = power of p.

$T|H| \mid |H| \Rightarrow T(H)$ is also a power of p.

O-S Thm If Q is a finite group of permutation of set S then
$|Q| = |\text{stab } i||\text{orb } i|$, $i \in Q$.

Let $Q = T(H)$. $S = S_C$, then $|T(H)| = |\text{orb } K_i| \cdot |\text{stab } K_i|$

Suppose for some i, $|\mathrm{orb}_{T(H)}(k_i)| = 1$ (later: show there is such an i)

Then $\phi_h(k_i) = hK_i h^{-1} = k_i \;\forall h \in H$ ↳ need to show this...

So $H \leq N(k_i)$ (normalizer)

K_i is a p-syllow

$H \leq K_i$ $\square$