



Lecture Notes:

1-13-25

Sets:

$\mathbb{N}^+ \cdot \mathbb{Z}^+ \cdot \mathbb{R}^+ \cdot \mathbb{C}^+ \cdot \mathbb{Q}^+ \cdot -$

$\mathbb{Z}[x] \cdot \mathbb{R}[z] \cdot \mathbb{C}[x, y, z] \cdot -$

$\mathbb{Z}/p \mathbb{Z}/n [\varnothing]$

continuous functions: $C(\mathbb{R}) \cdot -$

functions: $X \rightarrow Y$ nothing!

differentiable functions $\cdot -$

Smooth functions: $\cdot -$

Power Series: $\mathbb{R}[[x]] \cdot -$

Vector Spaces: $\cdot -$, scalar $\cdot$

Linear Functions: $V \rightarrow W \cdot -$

Rational Functions: $\mathbb{R}(x) \cdot +, -, \cdot$

Note.

$\mathbb{R}^+ \cdot - \cdot \cdot$

$\mathbb{R}^x = \mathbb{R}^+ = \mathbb{R} \setminus \{0\} = \mathbb{R} - \{0\} \cdot - \cdot /$

$\mathbb{Q} - \{0\} = \mathbb{Q}^+ \cdot - \cdot /$

$\mathbb{C}^+ \cdot - \cdot /$

Terminology:

Def. A composition law on a set X
is a function $m: X \times X \rightarrow X$
 $x \circ y = m(x, y)$

ex. $X = \mathbb{Q}$

$x \circ y = m(x, y) = x + y$

ex. $X = \mathbb{R}^+ [+]$

$m(x, y) = x \cdot y$

ex. $X = \mathbb{C}^+$

$m(x, y) = x - y$? Not a composition
law b/c $m(x, y)$ is not a function

Recall. X, Y are sets, then:

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

i.e. cartesian product

ex. $\{1, 2\} \times \{3, 4\} = \{(1, 3), (1, 4), (2, 3), (2, 4)\}$

ex. $\mathbb{R} \times \mathbb{R} = \mathbb{R}^2$

Note in calc III,

2 var function $f(x, y) = x^2 + \sin(y - x)$

$$f: \mathbb{R} \times \mathbb{R} \rightarrow \mathbb{R}$$

ex. f is a composition law on $\mathbb{R}$

$$f(x, y) = x^2 + \sin(y - x) = x \circ y$$

Lecture Notes:

1.15.25

A composition law on a set X :

$$m: X \times X \rightarrow X$$

i.e. $\forall x, y \in X \rightarrow m(x, y) \in X$

often written as:

$$x \circ y = m(x, y)$$

$$x \oplus y = m(x, y) \quad \text{etc}$$

$$x \odot y = m(x, y)$$

On paper. "Let $\circ$ be a composition law on X "

Ex. $\mathbb{R}$ " $-$ " $x - y$ in the usual $-$

Non Ex. $\mathbb{R}$ $x \circ y = \ln(x + y)$

doesn't always make sense

Non Ex. $\mathbb{Q}$ $x \circ y = \sqrt{x}$

not defined uniquely

Properties that composition laws might have:

(1) Associative:

$$(x \circ y) \circ z = x \circ (y \circ z) \quad \forall x, y, z$$

Ex. $+$ on $\mathbb{R}$: $(x+y)+z = x+(y+z)$

$\cdot$ on $\mathbb{R}$: $(x \cdot y) \cdot z = x \cdot (y \cdot z)$

Matrix $\cdot$: $A(BC) = (AB)C$

for any square matrices A, B, C

Non Ex. $-$ is not associative

$$(1-1)-1 \neq 1-(1-1)$$

Neither is division:

$$(1/2)/3 \neq 1/(2/3)$$

* in this class, this will always be true

(2) A composition law has a unit e

$$\begin{array}{l} x \circ e = x \quad \forall x \\ e \circ x = x \quad \forall x \end{array} \quad \begin{array}{l} \text{(must work on} \\ \text{both sides)} \end{array}$$

ex. 0 wrt $+$

$$x + 0 = 0 + x = x$$

ex. 1 wrt $\cdot$

$$x \cdot 1 = 1 \cdot x = x$$

Non Ex. $x - 0 = x$, $0 - x \neq x$

(3) Commutativity:

$$x \circ y = y \circ x \quad \forall x, y$$

Def. A group G is a set with a composition law satisfying

(1) Associative composition law

(2) The composition law must have a unit e

(3) Every x has an inverse x^{-1} st:

$$x \circ x^{-1} = x^{-1} \circ x = e$$

proves $(G, \circ)$ is a group

Ex 1. $\mathbb{Z}$ form a group w.r.t +
 $(\mathbb{Z}, +)$ is a group, + is a composition law
(1) is it associative?

$$(x+y)+z = x+(y+z) \quad \forall x, y, z \in \mathbb{Z}$$

(2) is there a unit? yes, $e=0$
 $x+0 = 0+x = x \quad \forall x \in \mathbb{Z}$

(3) is there an inverse?

$$x+(-x) = (-x)+x = 0 \quad \forall x \in \mathbb{Z}$$

$$x \circ x^{-1} = x^{-1} \circ x = e$$

Note. if + is the composition law
denote the inverse with $-x$

Terminology: if $(G, \circ)$ is a group,
a subgroup is a subset $H \subset G$ st.
 $(H, \circ)$ is a group
• must have the same unit

Ex. $(\mathbb{R}, +)$ form a group

$\mathbb{Z}$ is a subgroup of $(\mathbb{R}, +)$

$\mathbb{Z}$ is a subgroup

Ex 1. To check that $n\mathbb{Z}$ is a subgroup of $(\mathbb{Z}, +)$

S1. Check + is a comp law on $n\mathbb{Z}$

$$nx + ny = n(x+y) \in n\mathbb{Z}$$

S2. (1) associativity? (automatic)

(2) unit?

$$0 \in n\mathbb{Z} \quad \text{st.} \quad 0 = n \cdot 0$$

(3) inverse?

$$-nx = n(-x)$$

Group: Set G together with a composition law $\circ$ such that:

(1) Associative:

$$(x \circ y) \circ z = x \circ (y \circ z) \quad \forall x, y, z \in G$$

(2) Unit:

$$e \in G \text{ st. } x \circ e = e \circ x = x \quad \forall x \in G$$

(3) Inverse:

$$\forall x \in G \rightarrow \exists x^{-1} \in G \text{ st. } x \circ x^{-1} = x^{-1} \circ x = e$$

Ex. $G = \mathbb{R}^+ = \mathbb{R} - \{0\}$ with $\cdot$

(0) Check $\cdot$ is a composition law

$$\forall x, y \in \mathbb{R}^+ \text{ verify } x \cdot y \in \mathbb{R}^+$$

ie. $x, y \neq 0 \rightarrow x \cdot y \neq 0$ which is true

(1) Associative: $(xy)z = x(yz)$

(2) choose unit $e = 1$: $x \cdot 1 = 1 \cdot x = x$

(3) x^{-1} exists: given $x \in \mathbb{R}^+$

$$\text{seek } x^{-1} \in \mathbb{R}^+ \text{ st. } x \cdot x^{-1} = x^{-1} \cdot x = 1$$

$$x^{-1} = \frac{1}{x} \in \mathbb{R}^+ \text{ (well defined if } x \neq 0)$$

Def. If $(G, \circ)$ is a group

H.C. G is a subgroup which means

$(H, \circ)$ is a group

Ex. $(G, \circ)$ is a subgroup of $(G, \circ)$

Ex. $(\mathbb{Q}, +)$ form a subgroup of $(\mathbb{R}, +)$

(0) $+$ is a composition law on $\mathbb{Q}$

$$x, y \in \mathbb{Q} \rightarrow x + y \in \mathbb{Q} \checkmark$$

(1) associative: $(x + y) + z = x + (y + z) \checkmark$

(2) $0 \in \mathbb{Q}$, already know $x + 0 = 0 + x = x$

(3) $x \in \mathbb{Q} \rightarrow -x \in \mathbb{Q}$

$$x + (-x) = (-x) + x = 0$$

Aside. $(\mathbb{R}^+, \cdot)$ is a group

$(\mathbb{R}, +)$ is a group

$\mathbb{R}^+ \subset \mathbb{R}$ but NOT a subgroup

Ex. $(\mathbb{Q}, \cdot) = (\mathbb{R}^+, \cdot)$

Then $(0, \infty)$ is a subgroup. Check:

(0) The inherited operation $\cdot$ is a composition law:

$$x, y \in (0, \infty) \rightarrow x \cdot y \in (0, \infty)$$

(1) associative $\checkmark$

(2) 1 is a unit for $\cdot$

is it in the subgroup? $1 \in (0, \infty) \checkmark$

(3) $x \in (0, \infty) \rightarrow x^{-1} \in (0, \infty) \checkmark$

Ex. Group $(\mathbb{R}^+, \cdot)$

Are any of $H_1 = (2, \infty)$, $H_2 = (\frac{1}{2}, \infty)$,
or $H_3 = \{1, 2, 3, 4, \dots\} = \mathbb{Z}_{\geq 1}$?

	H_1	H_2	H_3
(0) add	$\checkmark$	$\times$	$\checkmark$
(1)	$\checkmark$	$\checkmark$	$\checkmark$
(2)	$\times$	$\checkmark$	$\checkmark$
(3) add	$\times$	$\times$	$\times$

note. the only possible unit is 1.

check it exists in each subgroup

$$0.5 + \epsilon + 0.5 + \epsilon < 0.5 + \epsilon$$

$$5^{-1} \in (2, \infty)$$

EXA these steps are most likely to fail

Ex. $(\mathbb{R}^+, \cdot)$. $H = \{1, 13\} \subset \mathbb{R}^+$

claim. H is a subgroup

$$(0) \begin{array}{c|ccc} & 4 & -1 & 1 \\ x & 1 & -1 & 1 \\ -1 & & & \\ 1 & & & \end{array} \leftarrow x \cdot y$$

composition law $\checkmark$

(1) associative $\checkmark$

(2) $1 \in H$ $\checkmark$

(3) $1^{-1} = 1$, $(-1)^{-1} = -1 \in H$

Lecture Notes:

1.22.25

Groups: $(G, \circ)$

* (1) $\circ$ is a composition law

(Auto) (1) associative (in this class, always true)

(2) unit $e \in G$ st. $x \circ e = e \circ x = x$

* (3) inverses $x \in G \rightarrow x^{-1} \in G$ st.
 $x \circ x^{-1} = x^{-1} \circ x = e$

* most frequently messed up

Sheet: if $n \in \mathbb{Z}$

- $n\mathbb{Z} = \{nx \mid x \in \mathbb{Z}\}$ is a subgroup

- $a, b \in \mathbb{Z}$

$(a, b) = \{ax + by \mid x, y \in \mathbb{Z}\}$

Theorem: every subgroup of $(\mathbb{Z}, +)$
is of the form $n\mathbb{Z}$ for some n

Challenge: to find n

Exs. $2\mathbb{Z} = \{\dots, -6, -4, -2, 0, 2, 4, 6, \dots\}$

$10\mathbb{Z} = \{\dots, -20, -10, 0, 10, 20, \dots\}$

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

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

$0\mathbb{Z} = \{0\}$ $\hookrightarrow$ only finite group

Proof. Suppose H is a subgroup of $(\mathbb{Z}, +)$

$$H \subset \mathbb{Z}$$

$(H, +)$ is a group

(0) $+$ is a composition law on H

$$x, y \in H \rightarrow x + y \in H$$

(1) $+$ is associative

$$(2) 0 \in H$$

$$(3) x \in H \rightarrow -x \in H$$

use all 6 of these properties to construct n st. $H = n\mathbb{Z}$

Case 1: $H = \{0\}$

then $n = 0$ and $H = 0\mathbb{Z}$

Case 2: $\{0\} \subsetneq H$

(means $0 \in H$ but H contains some non-zero elements)

ToDo. Seek an n

Candidates for n from $H \subset \mathbb{Z}$

* (1) $n = \text{gcd of all elements in } n\mathbb{Z}$

(2) $n = \text{first \# to the right of } 0$

* (3) $n = \text{difference b/w adjacent terms}$

* too hard

Answer. Smallest positive number greater than 0

also works: largest negative number greater than 0

$$3\mathbb{Z} = -3\mathbb{Z}, 10\mathbb{Z} = -10\mathbb{Z}$$

Given $H \subset \mathbb{Z}$ a subgroup, define:

$$n = \min \{x \in H \mid x > 0\}$$

works because integers are discrete

Caveat: $\min \{x \in \mathbb{Z} \mid \sqrt{2} < x < \sqrt{3}\}$

$\underbrace{\hspace{10em}}_{\substack{1.4 \qquad 1.7}}$

$\min \emptyset = \text{DNE!}$ $\emptyset$

ie, must make sure H contains positive #'s

Case 2: $m \in H$ st $m \neq 0$

if $m > 0$, done

if $m < 0$, $-m \in H \wedge -m > 0$, done

Claim: $H = n\mathbb{Z}$ ie $H \subset n\mathbb{Z} \leftarrow (0), (5)$
 $n\mathbb{Z} \subset H \leftarrow (0)$

Ex. $7\mathbb{Z} + 49\mathbb{Z} + 35\mathbb{Z} + 140\mathbb{Z} = d \cdot \mathbb{Z}$ for

(1) check H is a subgroup of $\mathbb{Z}$

(2) Then implies $= n\mathbb{Z} \exists n$

Lecture Notes:

1.24.25

Theorem: $H \subset (\mathbb{Z}, +) \Rightarrow H = n\mathbb{Z} \quad \exists n$

Caution: ~~A~~ an algorithm to find n

Proof: $H = \{0\} \Rightarrow H = 0 \cdot \mathbb{Z} \quad n = 0$

Else, $n =$ smallest positive in H

Caution: $2025\mathbb{Z} + 1071\mathbb{Z}$

$$= \{2025, 2025+1071, 2025 \cdot 2 + (-3) \cdot 1071, \dots\}$$

note, it is unclear what $n =$ smallest positive should be

Claim: $H = n\mathbb{Z}$

Part I: $H \supset n\mathbb{Z}$

if $n \in H$

$2n = n+n \in H$ by group prop

$3n = 2n+n \in H$

"so on"

We'll prove by induction that $n \cdot k \in H \quad \forall k \geq 0$:

Base Case: $k=1 \Rightarrow n \cdot 1 \in H$

Ind Hyp: $n \cdot k \in H$

Ind Step: $n \cdot (k+1) = nk + n \in H$

because $nk \in H$ by IH and group prop

note, must use IH in inductive step

so $\{n, 2n, 3n, \dots\} \subset H$

and if $n \cdot k \in H$ then $-n \cdot k = n \cdot (-k) \in H$
and $0 \in H$ because H is a subgroup
of $(\mathbb{Z}, +)$

so $\{\dots, -3n, -2n, -n, 0, n, 2n, 3n, \dots\} \subset H$
ie. $n\mathbb{Z} \subset H$

Part 2 $H \subset n\mathbb{Z}$

We'll prove by contradiction

Suppose H contains an element $x \notin n\mathbb{Z}$

Let $x \in H$ be the smallest positive
st $x \in n\mathbb{Z}$

ie. $x \in H$ positive $x \notin n\mathbb{Z}$

x = smallest such element of H

DWR: $x = nq + r$

$r \neq 0$ because $x \notin n\mathbb{Z}$

$|r| < n$ a priori. $0 \leq r < n$

so. $x, nq \in H$

$-nq \in H$

$\Rightarrow x - nq \in H$

$\underbrace{\hspace{1cm}}$

$r \in H$

$0 < r < n$

$\Rightarrow r \notin n\mathbb{Z}$

$r \in H$

$r < n$

} contradiction since
 n = smallest pos in H

Consequences (from worksheet):

$$\begin{aligned}(1) \quad (a, b) &= a\mathbb{Z} + b\mathbb{Z} \\ &= \{ax \mid x \in \mathbb{Z}\} + \{by \mid y \in \mathbb{Z}\} \\ &= \{ax + by \mid x, y \in \mathbb{Z}\} \text{ is} \\ &\text{a subgroup of } (\mathbb{Z}, +)\end{aligned}$$

So $(a, b) = d\mathbb{Z} \exists d$
showed $d = \gcd(a, b)$

$$\begin{aligned}(2) \quad a_1\mathbb{Z} + a_2\mathbb{Z} + a_3\mathbb{Z} + \dots + a_n\mathbb{Z} \\ = \gcd(a_1, \dots, a_n) \cdot \mathbb{Z}\end{aligned}$$

We've seen: $(\mathbb{R}, +)$, $(\mathbb{R}^+, \cdot)$

$(\mathbb{Z}, +)$ and all its subgroups

Now an example from linear algebra:

$$(1) \quad G = \{X \in M_{n \times n}(\mathbb{R})\} \text{ with } +$$

(0) composition law ✓ (2) identity ✓
(1) associativity ✓ (3) inverses ✓
identity $O_n = \begin{bmatrix} 0 & 0 & \dots & 0 \\ 0 & \dots & 0 & 0 \end{bmatrix}$
inverses —

$$(2) \quad G = \{X \in M_{n \times n}(\mathbb{R}) \mid \det X \neq 0\} \text{ matrix } \bullet$$

(0) composition law (2) identity ✓ $I_n = \begin{bmatrix} 1 & & 0 \\ & \ddots & \\ 0 & & 1 \end{bmatrix}$
(1) associative ✓ (3) inverses if $\det X \neq 0$
 $(AB)C = A(BC)$ then X^{-1} exists ✓

$$\begin{aligned}&\begin{pmatrix} X & \begin{bmatrix} 1 & & 0 \\ 0 & \ddots & \\ 0 & & 1 \end{bmatrix} \end{pmatrix} \\ &\text{echelonize} \\ &\begin{pmatrix} \begin{bmatrix} 1 & & 0 \\ 0 & \ddots & \\ 0 & & 1 \end{bmatrix} & X^{-1} \end{pmatrix} \quad X^{-1} = \frac{1}{\det X} \cdot X^{\#}\end{aligned}$$

To check (c): $x, y \in G$

i.e. $x, y \in M_{n \times n}(\mathbb{R})$ st. $\det x, \det y \neq 0$

have to check $x \cdot y \in G$ st. $x \cdot y \in M_{n \times n}(\mathbb{R})$
and $\det(xy) \neq 0$

$$\det(xy) = \underbrace{\det(x)}_{\neq 0} \cdot \underbrace{\det(y)}_{\neq 0} \neq 0 \checkmark$$

This group is called $GL_n(\mathbb{R})$
(general linear)

Remark. $GL_n(\mathbb{R})$ is not commutative

$$\text{ex } n=2 \quad \begin{pmatrix} 0 & 1 \\ 1 & 0 \end{pmatrix} \cdot \begin{pmatrix} 1 & 0 \\ 0 & -1 \end{pmatrix} = \begin{pmatrix} 0 & -1 \\ 1 & 0 \end{pmatrix} \neq$$
$$\underbrace{\begin{pmatrix} 1 & 0 \\ 0 & -1 \end{pmatrix}}_B \cdot \underbrace{\begin{pmatrix} 0 & 1 \\ 1 & 0 \end{pmatrix}}_A = \begin{pmatrix} 0 & 1 \\ -1 & 0 \end{pmatrix}$$

$A, B \in GL_n(\mathbb{R})$

Lecture Notes:

1.27.25

Back to $(G, \circ)$, an abstract group
(Think $(\mathbb{Z}, +)$, $(\mathbb{R}^+, \cdot)$, $(GL_n, \cdot)$)

- $\circ$ is a composition law
- associative
- with a unit $e \in G$
- every x has an inverse $x^{-1} \in G$

Lemma 1. In a group, the unit is unique

Pf. Suppose e_1 & e_2 are both units

$$\sum x \circ e_1 = e_1 \circ x = x \quad \forall x \in G$$

$$\sum x \circ e_2 = e_2 \circ x = x \quad \forall x \in G$$

$$\text{Get } e_1 \circ x = x = e_2 \circ x$$

How to prove this is $\top \quad \forall x \in G$?

Plug in values of $x \in G$

note. only two elements in G we know are e_1 and e_2

Let's try $x = e_2$:

$$e_1 \circ e_2 = e_2 \circ e_2$$

note. by $x \circ e_2 = x$ from above:

$$e_2 \circ e_2 = e_2$$

$$e_1 \circ e_2 = e_1$$

$$\text{so } e_1 = e_2$$

$$\text{Ex. } G = \{0\}, \cdot$$

Claim. 0 is a unit

$$\text{check } x \circ 0 = 0 \circ x = x \quad \forall x \in G$$

$$\text{ie } 0 \circ 0 = 0 \circ 0 = 0$$

Lemma 2: Suppose $(G, \circ)$ is a group and $e = \text{the unique unit}$.
Then $\forall x \in G$ must have a unique inverse

Pf. Suppose $x \in G$ has two inverses A, B :

$$x \circ A = A \circ x = e \quad \text{here } x \text{ is fixed}$$

$$x \circ B = B \circ x = e$$

so must do different operations than in lemma 1:

$$B \circ (x \circ A = e)$$

$$B \circ (x \circ A) = B \circ e$$

$$(B \circ x) \circ A = B$$

$$e \circ A = B$$

$$A = B$$

not empty

Lemma 3: Suppose $(G, \circ)$ is a group and $H \subseteq G$ is a subset $\iff$

Then H is a subgroup iff:

$$\forall x, y \in H \Rightarrow x \circ y^{-1} \in H$$

Pf. " $\Rightarrow$ " Suppose $H = \text{subgroup}$

$$x, y \in H \quad \text{WTS } x \circ y^{-1} \in H$$

$$\Rightarrow y^{-1} \in H \Rightarrow x \circ (y^{-1}) \in H \quad \forall x \in H$$

" $\Leftarrow$ " Suppose we know $x \circ y^{-1} \in H$
 $\forall x, y \in H$:

WTS H is a subgroup

check:

(iv) (0) composition law:

(i) (1) associative:

$$x, y, z \in H \subset G \Rightarrow (x \circ y) \circ z = x \circ (y \circ z)$$

which is true since G is a group

(ii) (2) units:

$$\text{take } x = y \in H \Rightarrow x \circ y^{-1} = x \circ x^{-1} = e \in H$$

(iii) (3) inverses: if $y \in H$ check $y^{-1} \in H$

$$y^{-1} = e \circ y^{-1} \in H \text{ because } e, y \in H$$

* if $x, y \in H$ check $x \circ y \in H$

we know $x, y^{-1} \in H$ so $x \circ (y^{-1})^{-1} \in H$
so $x \circ y \in H$

Ex. $H = \{ax + by + cz \mid x, y, z \in \mathbb{Z}\}$
= " (a, b, c) " is a subgroup of $\mathbb{Z}$

only need to check $x, y \in H \Rightarrow x \circ y^{-1} \in H$

$$x = ax_1 + by_1 + cz_1 \in H$$

$$y = ax_2 + by_2 + cz_2 \in H$$

$$\text{check } x - y = a(x_1 - x_2) + b(y_1 - y_2) + c(z_1 - z_2) \in H$$

By Lemma H is a subgroup of $\mathbb{Z}$ (with +)

UR-EX. $G = \mathbb{R}^+$ (with $\cdot$)

$$H = \left\{ \dots, \frac{1}{8}, \frac{1}{4}, \frac{1}{2}, 1, 2, 4, 8, \dots \right\} \subset G$$
$$= \{ 2^n \mid n \in \mathbb{Z} \} = 2^{\mathbb{Z}}$$

Claim. H is a subgroup

$$x = 2^a \in H$$

$$y = 2^b \in H$$

check:

$$x \cdot y^{-1} = 2^{a-b} \in H$$

since $a-b \in \mathbb{Z}$

so H is a subgroup

Lecture Notes:

1.29.25

Suppose $(G, \circ)$ is a group

Notation. xy instead of $x \circ y$

$$x^n = \underbrace{x \circ x \circ \dots \circ x}_{n \text{ times if } n > 0}, \quad x^{-n} = (x^n)^{-1}$$

Remark. $x^n \cdot x^m = x^{n+m}$

Lemma. if G is a group

$x_1, x_2, \dots, x_n \in G$, $x_1 x_2 \dots x_n$
makes sense independent of the "order
of multiplication"

Reason. associativity

$$n \geq 3 \quad x_1 x_2 x_3 = \begin{cases} (x_1 x_2) x_3 \\ x_1 (x_2 x_3) \end{cases}$$

by induction see textbook

Lemma. if $(G, \circ)$ is a group

$$x_1, x_2, \dots, x_n \in G$$

$$(x_1 x_2 \dots x_n)^{-1} = x_n^{-1} x_{n-1}^{-1} \dots x_1^{-1}$$

recall. $(AB)^{-1} = B^{-1} A^{-1}$ for matrices

Proof. To check $x_n^{-1} x_{n-1}^{-1} \dots x_1^{-1}$ is

the inverse of $x_1 x_2 \dots x_n$

verify that both products are $= e$

$$(x_1 x_2 \dots x_n) \cdot (x_n^{-1} x_{n-1}^{-1} \dots x_1^{-1})$$

note. say "multiply" or "group multiply" instead of "composition law"

$$= x_1 x_2 \dots x_n x_n^{-1} x_{n-1}^{-1} \dots x_1^{-1}$$

$$= x_1 x_2 \dots (x_n x_n^{-1}) x_{n-1}^{-1} \dots x_1^{-1}$$

$$= x_1 \dots x_{n-1} e x_{n-1}^{-1} \dots x_1^{-1}$$

$$= x_1 \dots (x_{n-1} x_{n-1}^{-1}) \dots x_1^{-1}$$

$$= \dots = x_1 \cdot (x_2 x_2^{-1}) x_1^{-1}$$

$$= x_1 x_1^{-1} = e$$

Next Steps. see all this in action

- $(\mathbb{Z}_n, +)$
- units modulo n ,
- Permutations

Big Example #1: $\mathbb{Z}_n$

$$n \in \mathbb{Z}, n \geq 1$$

Def. $a \equiv b \pmod{n}$ if:

- a & b same remainder when dividing by n
- $n \mid a - b$
- $a - b \in n\mathbb{Z}$

Prop. (1) $a \equiv a \pmod{n}$

$$(2) a \equiv b \pmod{n} \Rightarrow b \equiv a \pmod{n}$$

(3) if $a \equiv b \pmod{n}$ and $b \equiv c \pmod{n}$
then $a \equiv c \pmod{n}$

Textbook: $\equiv \pmod{n}$ is an equivalence relation

(4) if $a \equiv b \pmod{n}$ and $a' \equiv b' \pmod{n}$
then $a + a' \equiv b + b' \pmod{n}$ and
 $a \cdot a' \equiv b \cdot b' \pmod{n}$

Pf. (1) $a - a \in n\mathbb{Z}$
 $0 \in n\mathbb{Z}$

(2) know $a - b \in n\mathbb{Z}$ WTS $b - a \in n\mathbb{Z}$
note. $b - a = -(a - b)$

$n\mathbb{Z}$ is a group so if $a - b \in n\mathbb{Z}$,
its inverse $-(a - b) \in n\mathbb{Z}$

(3) we know $a-b \in \mathbb{N}$ and $b-c \in \mathbb{N}$
 WTS $a-c \in \mathbb{N}$
 $\underbrace{a-b}_{\in \mathbb{N}} + \underbrace{b-c}_{\in \mathbb{N}} = a-c \in \mathbb{N}$

note. (1) used units
 (2) used inverses
 (3) used comp law and associativity

(4) is similar and in the textbook

Def. $\mathbb{Z}_n = \{ \bar{0}, \bar{1}, \bar{2}, \dots, \overline{(n-1)} \}$, +
 $\bar{a} + \bar{b} = \bar{c} \quad 0 \leq c \leq n-1$
 if $a+b \equiv c \pmod{n}$

eg. $\mathbb{Z}_{17}$ every $a \in \mathbb{Z}$ is congruent
 mod 17 to $\bar{0}, \bar{1}, \bar{2}, \dots, \bar{16}$
 $\bar{8} + \bar{9} = \bar{0}$

note. when we write $\bar{1}$ we really
 mean $1 \pmod{n}$.

$$\begin{aligned} \bar{7} &= 7 \pmod{17} \\ &= 7 + 17 \equiv 7 + 17 \cdot 2 \equiv 7 + 17 \cdot 3 \equiv \dots \\ &\equiv 7 - 17 \equiv 7 - 17 \cdot 2 \equiv \dots \pmod{17} \end{aligned}$$

note. no notion of odd or even here

note. $1 \equiv 3 \equiv 5 \equiv \dots \pmod{2}$
 $0 \equiv 2 \equiv 4 \equiv \dots \pmod{2}$

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

Lecture Notes:

12.31.25

$$\text{Mod } n \quad a(\text{mod } n) \equiv a + kn(\text{mod } n)$$

$\bar{a}$ = the "class" of all $b \equiv a(\text{mod } n)$

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

$$\mathbb{Z}_7 = \{ \bar{0}, \bar{1}, \bar{2}, \bar{3}, \bar{4}, \bar{5}, \bar{6} \}$$

$$= \{ \overline{-7}, \overline{15}, \overline{23}, \overline{10}, \overline{-3}, \overline{40}, \overline{13} \}$$

note, $\overline{23} = \{ \text{all } a \equiv 23 \text{ mod } 7 \}$
 $= \{ 23, 23 \pm 7, 23 \pm 2 \cdot 7, \dots \}$

Defined, $\bar{a} + \bar{b} = \overline{a+b}$

Careful. Must check that this makes sense.

Ex. in $\mathbb{Z}_7$: $\bar{2} + \bar{3} = \overline{2+3} = \bar{5} \parallel \text{mod!}$
 $\parallel \parallel$
 $\overline{23} + \overline{10} = \overline{23+10} = \overline{33}$

if $\bar{a} = \bar{a'}$ & $\bar{b} = \bar{b'}$ then $\bar{a} + \bar{b} = \overline{a'+b'}$

$$a \equiv a'(\text{mod } n), b \equiv b'(\text{mod } n)$$

$$a+b \equiv a'+b'(\text{mod } n)$$

Ex. $(\mathbb{Z}_n, +)$ is a group

commutative = abelian group

The more interesting / useful group

is $(\mathbb{Z}_n^\times, \cdot)$ ← will define next week
today background
ie. $\mathbb{U}_n$ for $\mathbb{Z}_n^\times$

GCD from groups:

$$a, b \in \mathbb{Z}$$

$$(a, b) = a\mathbb{Z} + b\mathbb{Z} = \{ax + by \mid x, y \in \mathbb{Z}\}$$

$$\text{subgroup of } \mathbb{Z}: (a, b) = d\mathbb{Z}$$

$$d = \gcd(a, b)$$

$$\text{ex. } (2025, 1071) = d\mathbb{Z}$$

$$d = \gcd(2025, 1071)$$

$$2025 = 3^4 \cdot 5^2$$

$$1071 = 3^2 \cdot 119$$

$$\begin{array}{r|l} 2025 & 5 \\ 405 & 5 \\ 81 & 3^4 \\ 1071 & 3^2 \\ 119 & \end{array}$$

$$\gcd(2025, 1071) = 3^2$$

$$\text{so } (2025, 1071) = 9\mathbb{Z}$$

This is haphazard (requires intuition)

To do gcd in general: Euclidean Alg

$$\text{if } a = bq + r \text{ DWR } 0 \leq r < b$$

$$\text{then } \gcd(a, b) = \gcd(b, r)$$

$$\text{EX. } (2025, 1071) = (1071, 954)$$

$$= (954, 117) = (117, 18)$$

$$= (18, 9) = (9, 0) = 9$$

note. dropping gcd from function

Pf. To check $\gcd(a, b) = \gcd(b, r)$

$$(a, b) = (b, r)$$

$$\gcd(a, b) \cdot \mathbb{Z} = \gcd(b, r) \cdot \mathbb{Z}$$

$$a\mathbb{Z} + b\mathbb{Z} = b\mathbb{Z} + r\mathbb{Z}$$

$$r = a - bq$$

Mon. $a\mathbb{Z} + b\mathbb{Z} = b\mathbb{Z} + (a - bq)\mathbb{Z}$

Similarly, $\text{Span}(v_1, v_2) = \text{Span}(v_1 - \alpha v_2, v_2)$

Lecture Notes:

2.3.25

$\mathbb{Z}_n$ is a group $\Leftrightarrow$ gcd and divisibility

$$(a, b) = a\mathbb{Z} + b\mathbb{Z} = \gcd(a, b)\mathbb{Z}$$

Euclid. $(a, b) = (b, r)$ when $a = bq + r$

Pf. We'll show

$$a\mathbb{Z} + b\mathbb{Z} = b\mathbb{Z} + r\mathbb{Z}$$

this gives $\gcd(a, b)\mathbb{Z} = \gcd(b, r)\mathbb{Z}$

$$\Rightarrow \gcd(a, b) = \gcd(b, r)$$

" $\supset$ " Elements of $b\mathbb{Z} + r\mathbb{Z}$ are of the form:

$$bx + ry \quad \forall x, y \in \mathbb{Z}$$

$$= bx + (a - bq)y$$

$$= ay + b(x - qy) \in a\mathbb{Z} + b\mathbb{Z}$$

" $\subset$ " Every element of $a\mathbb{Z} + b\mathbb{Z}$ looks like:

$$ax + by = (bq + r)x + by$$

$$= b(qx + y) + rx \in b\mathbb{Z} + r\mathbb{Z}$$

Group of units mod n :

From wkst. $(\mathbb{Z}_n, \cdot)$ is NOT a group if $n > 1$

Q. Which elements of $\mathbb{Z}_n$ have an inverse and which don't?

$$\mathbb{Z}_6 = \{\bar{0}, \bar{1}, \bar{2}, \bar{3}, \bar{4}, \bar{5}\}$$

note $(-\bar{1})^{-1} = -\bar{1}$ $(-\bar{2})^{-1} = -\bar{2}$

$$\mathbb{Z}_6 = \{\cancel{\bar{0}}, \pm\bar{1}, \pm\cancel{\bar{2}}, \cancel{\bar{3}}\}$$

$\bar{0}$ has no inverse

does $\bar{2}$ have an inverse?

$$\bar{2} \cdot x \equiv 1 \pmod{6} \text{ NO}$$

$$\bar{3} \cdot x \equiv 1 \pmod{6} \text{ NO}$$

only $\pm\bar{1}$ have inverses

$$\text{But in } \mathbb{Z}_5 = \{\bar{0}, \bar{1}, \bar{2}, \bar{3}, \bar{4}\}$$

$$= \{\cancel{\bar{0}}, \pm\bar{1}, \pm\bar{2}\}$$

have inverses

Calc Ex. Solve

$$x^2 - 17x + 2 = 0$$

integer solutions are divisors of 2

$$x_1, x_2, 2, -2$$

Prop. An element $\bar{a} \in \mathbb{Z}_n$ has a multiplicative inverse mod n

$$\Leftrightarrow (a, n) = 1 \quad \text{ie. coprime}$$

Def. $U_n = \{ \bar{a} \in \mathbb{Z}_n \mid (a, n) = 1 \}$

Thm. $(U_n, \cdot)$ is a group

(Beyond intro books, U_n is denoted by $\mathbb{Z}_n^\times$)

note. x means all elements with inverses

Pf.

" $\Rightarrow$ " Suppose $a \in \mathbb{Z}_n$ has an inverse x
 $ax \equiv 1 \pmod{n}$

note. $1 \equiv$ unit for $\cdot \pmod{n}$

$$\Rightarrow ax - 1 \in n\mathbb{Z} \Rightarrow ax - 1 = ny$$

$$\Rightarrow ax - ny = 1 \in (a, n)\mathbb{Z} \Rightarrow (a, n) = 1$$

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

" $\Leftarrow$ " under. Suppose $(a, n) = 1$

$$a\mathbb{Z} + n\mathbb{Z} = (a, n)\mathbb{Z} = 1 \cdot \mathbb{Z} = \mathbb{Z}$$

$$\Rightarrow ax + ny = 1 \quad \exists x, y \in \mathbb{Z} \quad 1 \in$$

called Bézout's formula

$$ax + ny = 1$$

$$ax = 1 - ny$$

$$ax \equiv 1 \pmod{n}$$

Every $(a, n) = 1$ has an inverse

$$x \equiv a^{-1} \pmod{n}$$

$$U_n = \{ \bar{a} \in \mathbb{Z}_n \mid (a, n) = 1 \}$$

we showed $\forall a \in U_n$ has an inverse mod n

Thm. $(U_n, \cdot)$ where $\bar{a} \cdot \bar{b} = \overline{a \cdot b}$ is a group

Proof.

(o) composition law.

check if $\bar{a}, \bar{b} \in U_n$ then $\overline{a \cdot b} \in U_n$

$$(a, n) = 1 \quad (b, n) = 1 \quad \stackrel{?}{\Rightarrow} \quad (ab, n) = 1$$

Lemma. Suppose $(A, B) = 1$

if $A \mid B \cdot N$ then $A \mid N$

Pf. $(A, B) = 1 \Rightarrow$ ex.

$\Rightarrow$

$$A\mathbb{Z} + B\mathbb{Z}$$

$$1 \in \mathbb{Z} = A\mathbb{Z} + B\mathbb{Z}$$

$$1 = Ax + By \quad \forall x, y \in \mathbb{Z}$$

not easy

$$A \mid BN$$

$$A \mid BNy = ByN = (1 - Ax)N$$

$$A \mid N - AxN \quad \} + \Rightarrow A \mid N$$

$$A \mid AxN$$

Say $d \mid a \cdot b$ and n

d cannot divide a because then

$$d \mid (a, n) = 1$$

so $(d, a) = 1$ by lemma $d \mid b$

but $(b, n) = 1$ so $d = 1$

$$\text{Surely } (a \cdot b)^{-1} \equiv b^{-1} a^{-1} \pmod{n}$$

$\underbrace{\quad} \underbrace{\quad}$
 $b \in U_n \quad a \in U_n$

so ab invertible mod n

so $\in U_n$

(1) associativity: similar to U_n

(2) unit: $\bar{1}$

(3) inverse: $\bar{a}$ has an inverse mod n

$$\text{Ex. } U_{15} = \{\bar{1}, \bar{2}, \bar{4}, \bar{7}, \bar{8}, \bar{11}, \bar{13}, \bar{14}\}$$

$$= -\bar{7} = -\bar{4} = -\bar{2} = -\bar{1}$$

$$A = \{\bar{1}, \bar{4}\} \quad \text{these are subgroups}$$

$$B = \{\bar{1}, \bar{4}, \bar{7}, \bar{13}\} \text{ of } U_{15}$$

Ex. xy^{-1} criteria

$$1 \cdot 1^{-1} = 1 \quad 4 \cdot 4^{-1} = 1$$

$$\rightarrow 1 \cdot 4^{-1} = 4 \quad 4 \cdot 1^{-1} = 4$$

$$\text{guessed: } 4 \cdot 4 = 16 \equiv 1 \pmod{15}$$

$$4^2 \equiv 1 \pmod{15}$$

$$4 \equiv 4^{-1}$$

B

$x \backslash y$	1	4	7	13
1	1	4	13	7
4	4	1	7	13
7	7		1	
13	13			1

$$x \cdot y^{-1} \pmod{15}$$

Note.

$$7^{-1} \pmod{15} \equiv 13 \pmod{15}$$

$$7 \cdot 2 = 14 \equiv -1 \pmod{15}$$

$$7^{-1} \equiv -2 \pmod{15}$$

$$7^{-1} \equiv 13 \pmod{15}$$

$$13^{-1} \equiv (-2)^{-1} \pmod{15}$$

$$\equiv 7 \pmod{15}$$

Remark.

$$1 = 1 = 7^0$$

$$4 \equiv (-2)^2 \pmod{15} \equiv 7^2 \pmod{15}$$

$$7 = 7$$

$$13 \equiv -2 \pmod{15} \equiv 7^3 \pmod{15}$$

$$7^2 \equiv 49 \equiv 4 \pmod{15}$$

$$7^3 \equiv 49 \cdot 7 \equiv 4 \cdot 7 \equiv 28 \equiv -2 \pmod{15}$$

$$\text{i.e. } B = \{1, 7, 7^2, 7^3\}$$

$$\text{so. } A = \{1, 4\}$$

$$B = \{1, \bar{7}, \bar{7}^2, \bar{7}^3\}$$

are subgroups of U_{15}

why no higher powers of 4?

$$4^2 \equiv 1 \pmod{15}$$

why no higher powers of 7?

$$\bar{7}^4 = (\bar{7}^2)^2 \equiv 49^2 \equiv 4^2 \equiv 16 \equiv 1 \pmod{15}$$

Def. If G is any group and $g \in G$
the cyclic group generated by g

$\langle g \rangle = \text{all powers of } g = \{g^m \mid m \in \mathbb{Z}\}$
is always a subgroup of G

$$g^a \cdot (g^b)^{-1} = g^{a-b} \in \langle g \rangle$$

(if) $g^N = e$ $N = \text{smallest such positive integer}$

$$\langle g \rangle = \{e = g^0, g, g^2, g^3, \dots, g^{N-1}\}$$

$$= g^N = g^{N+1} = g^{N+2}, \dots$$

eg. inside $G = U_{15}$

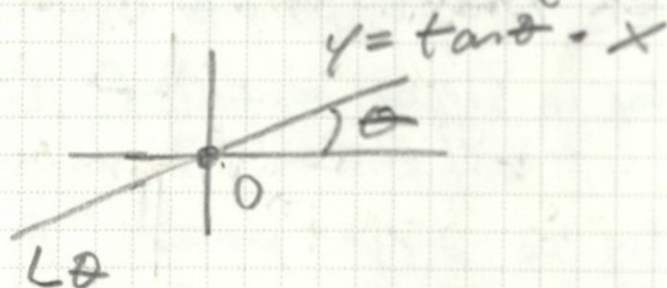
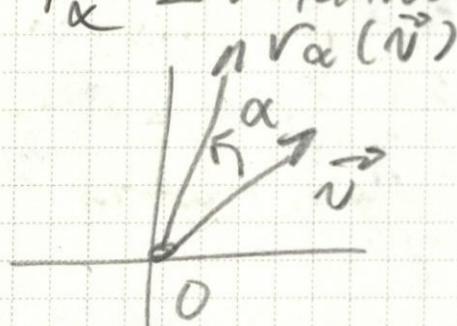
$$\langle 4 \rangle = \{1, \bar{4}\}$$

$$\langle 7 \rangle = \{1, 7, 7^2, 7^3\}$$

Reminder. $G = GL_2(\mathbb{R})$ invertible
matrices 2×2

$A \in G \iff \text{linear transformations of } \mathbb{R}^2$

$R_\alpha = \text{rotation counterclockwise by } \alpha$



$S_\theta = \text{reflection across line } L_\theta$

note: $5^{-1} \pmod{14}$

solve $5x \equiv 1 \pmod{14}$

$$5 \cdot 3 = 15 \equiv 1 \pmod{14}$$

or

5	10	15	20	25	...
1	5	9	13	17	...

$i=3$

also $(14, 5) = (5, 4) = (4, 1) = 1$

$$14 = 5 \cdot 2 + 4$$

$$5 = 4 \cdot 1 + 1$$

$$1 = 5 - 4 \cdot 1$$

$$1 = 5 - (14 - 5 \cdot 2) \cdot 1$$

$$1 = 14 \cdot (-1) + 5 \cdot 3 \equiv 1 \pmod{14}$$

$$1 = 0 + 5 \cdot 3 \equiv 1 \pmod{14}$$

$$3 \equiv 5^{-1}$$

Lecture Notes:

2.7.25

Linear Algebra:

$$GL_n(\mathbb{R}) = \{X = M_{n \times n}(\mathbb{R}) \mid \det X \neq 0\} \\ \Leftrightarrow X^{-1} \text{ exists}$$

$\{\text{Linear transformation } T: \mathbb{R}^n \rightarrow \mathbb{R}^n \text{ st. } T \text{ is bijective}\}$

$$\Leftrightarrow T \text{ inj and surj, } \ker T = \{0\}, \operatorname{Im} T = \mathbb{R}^n$$

How to get linear transformation from matrix?

$$T(\vec{v}) = A \cdot \vec{v}$$

If $T: \mathbb{R}^n \rightarrow \mathbb{R}^n$ then how to get matrix?

You need a basis $\mathcal{B} = \{\vec{v}_1, \vec{v}_2, \dots, \vec{v}_n\}$

typically $v_1 = e_1 = (1 \ 0 \ \dots \ 0)$

$v_2 = e_2 = (0 \ 1 \ 0 \ \dots \ 0)$

$\vdots$

$$[T]_{\mathcal{B}} = [T(\vec{v}_1) \mid T(\vec{v}_2) \mid \dots \mid T(\vec{v}_n)]$$

here write $T(\vec{v}_1) = a_{11}\vec{v}_1 + a_{12}\vec{v}_2 + \dots + a_{1n}\vec{v}_n$

$$\text{If } A, B \leftrightarrow T_A, T_B$$

$$A \cdot B \leftrightarrow T_{A \cdot B}$$

$$T_{A \cdot B}(\vec{v}) = (A \cdot B)\vec{v} = A \cdot (B\vec{v})$$

$$= A \cdot T_B(\vec{v}) = T_A(T_B(\vec{v}))$$

$$\text{ie } T_{AB} = T_A \circ T_B$$

Lets see some ex of subgroups of $GL_n(\mathbb{R})$:

$$(1) \ SL_n(\mathbb{R}) = \{X \in GL_n(\mathbb{R}) \mid \det X = 1\}$$

subgroup of $GL_n(\mathbb{R})$

$$(2) \ GL_n^+(\mathbb{R}) = \{X \in GL_n(\mathbb{R}) \mid \det X > 0\}$$

(3) Orthogonal Group:

$$O_n(\mathbb{R}) = \{X \in GL_n(\mathbb{R}) \mid X^T = X^{-1}\}$$

Prop. $O_n(\mathbb{R})$ is a subgroup of $GL_n(\mathbb{R})$

Pf. $X, Y \in O_n(\mathbb{R})$ check $XY^{-1} \in O_n(\mathbb{R})$

know $X^T = X^{-1}$ wts $(XY^{-1})^T = (XY^{-1})^{-1}$

Definitions

Work: $(XY^{-1})^T = (XY^T)^T = (Y^T)^T X^T = YX^T$

$$(XY^{-1})^{-1} = (Y^{-1})^{-1} X^{-1} = YX^{-1} \quad \parallel$$

note. $(AB)^{-1} = B^{-1}A^{-1}$

$$(AB)^T = B^T A^T$$

Remark. If $X \in O_n(\mathbb{R})$ then $\det X = \pm 1$

$$X^T = X^{-1} \Rightarrow \det(X^T) = \det(X^{-1})$$

$$\Rightarrow \det(X) = \frac{1}{\det(X)}$$

$$\Rightarrow [\det(X)]^2 = 1 \Rightarrow \det(X) = \pm 1$$

Stay. $A \in O_n(\mathbb{R})$ preserves distance

$$\| \vec{x} \|^2 = \vec{x} \text{ dot product } \vec{x}$$

$$= \vec{x}^T \cdot \vec{x}$$

$$= \square \quad \square$$

$$\| A\vec{x} \|^2 = (A\vec{x})^T \cdot A\vec{x} = \vec{x}^T A^T A \vec{x}$$

$$= \vec{x}^T A^{-1} A \vec{x} = \vec{x}^T \vec{x} = \| \vec{x} \|^2$$

Lecture Notes:

2.10.25

Subgroups $GL_n(\mathbb{R})$

eg. $SL_n(\mathbb{R})$ $\det = 1$

$GL_n(\mathbb{R})^+$ $\det > 0$

$O_n(\mathbb{R}) = \{A \in GL_n(\mathbb{R}) \mid A^T = A^{-1}\}$

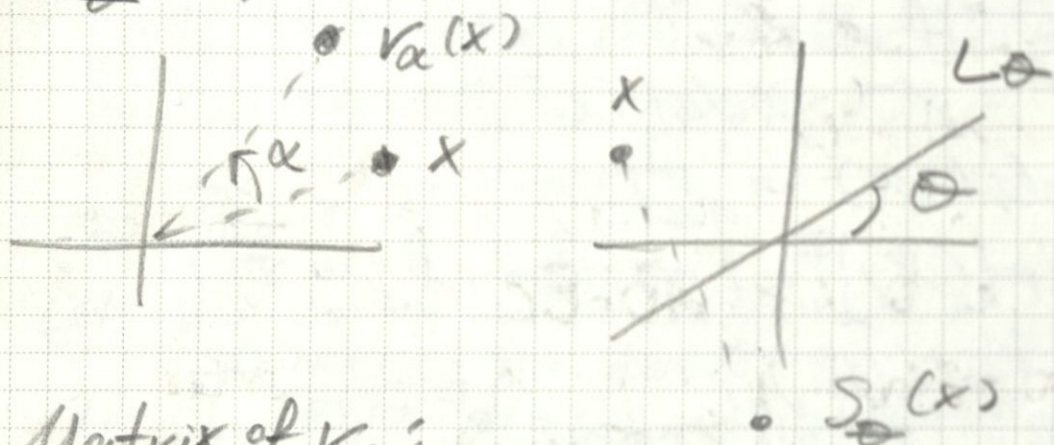
note $\|A\vec{x}\| = \|\vec{x}\|$ if $A \in O_n(\mathbb{R})$

Ex from sheet: $r_\alpha : \mathbb{R}^2 \rightarrow \mathbb{R}^2$

rotation about 0 by angle α

" $r_\alpha \in O_n(\mathbb{R})$ "

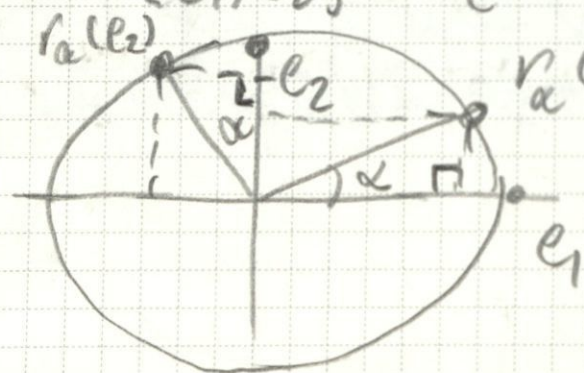
$S_\alpha : \mathbb{R}^2 \rightarrow \mathbb{R}^2$ reflection across



Matrix of r_α :

Basis e_1, e_2

$[r_\alpha]_{\{e_1, e_2\}} = [r_\alpha(e_1) \mid r_\alpha(e_2)]$



$r_\alpha = \begin{bmatrix} \cos \alpha & -\sin \alpha \\ \sin \alpha & \cos \alpha \end{bmatrix}$
 $\in O_2(\mathbb{R})$

Check. $R_\alpha^T = R_\alpha^{-1}$

$\Leftrightarrow R_\alpha^T \cdot R_\alpha = I_2$ or $R_\alpha \cdot R_\alpha^T = I_2$

$$\begin{bmatrix} \cos \alpha & \sin \alpha \\ -\sin \alpha & \cos \alpha \end{bmatrix} \begin{bmatrix} \cos \alpha & -\sin \alpha \\ \sin \alpha & \cos \alpha \end{bmatrix}$$

$$= \begin{bmatrix} \cos^2 \alpha + \sin^2 \alpha & 0 \\ 0 & \sin^2 \alpha + \cos^2 \alpha \end{bmatrix} = \begin{bmatrix} 1 & 0 \\ 0 & 1 \end{bmatrix}$$

note. $R_\alpha^{-1} = R_\alpha^T = \begin{bmatrix} \cos \alpha & \sin \alpha \\ -\sin \alpha & \cos \alpha \end{bmatrix}$

note. computers sometimes do xA instead of Ax

calculate directly:

note. $\begin{pmatrix} A & B \\ C & D \end{pmatrix}^{-1} = \frac{1}{AD-BC} \begin{pmatrix} D & -B \\ -C & A \end{pmatrix}$

$$\begin{pmatrix} \cos \alpha & -\sin \alpha \\ \sin \alpha & \cos \alpha \end{pmatrix} = \frac{1}{1} \begin{pmatrix} \cos \alpha & \sin \alpha \\ -\sin \alpha & \cos \alpha \end{pmatrix}$$

From Sheet: $R_\alpha \circ R_\beta = R_{\alpha+\beta}$

but $T_A \circ T_B = T_{A \cdot B}$

Reinterpret as Matrices: $\begin{pmatrix} \cos \alpha & -\sin \alpha \\ \sin \alpha & \cos \alpha \end{pmatrix} \begin{pmatrix} \cos \beta & -\sin \beta \\ \sin \beta & \cos \beta \end{pmatrix}$

$$= \begin{pmatrix} \cos(\alpha+\beta) & -\sin(\alpha+\beta) \\ \sin(\alpha+\beta) & \cos(\alpha+\beta) \end{pmatrix}$$

Compute $\cos(\alpha+\beta)$ term:

$$\cos(\alpha+\beta) = \cos\alpha \cos\beta - \sin\alpha \sin\beta$$

proves this identity in all forms:

$$\sin(\alpha+\beta) = \sin\alpha \cos\beta + \sin\beta \cos\alpha$$

$$\text{Ex. } R_{\frac{\pi}{2}} = \begin{pmatrix} 0 & -1 \\ 1 & 0 \end{pmatrix} \quad R_{\pi} = \begin{pmatrix} -1 & 0 \\ 0 & -1 \end{pmatrix} \quad R_{\frac{3\pi}{2}} = \begin{pmatrix} 0 & 1 \\ -1 & 0 \end{pmatrix}$$

$$\text{by inspection } R_{\frac{3\pi}{2}} = R_{\frac{\pi}{2}}^{-1}$$

$$\text{since } R_{2\pi} = I_2 = R_0, \quad R_{\alpha}^{-1} = R_{-\alpha}$$

$$R_{\alpha} \circ R_{-\alpha} = R_{\alpha+(-\alpha)} = R_0 = I_2$$

$$R_{\frac{\pi}{2}}^{-1} = R_{-\frac{\pi}{2}} = R_{-\frac{\pi}{2}} \circ I_2 = R_{-\frac{\pi}{2}} \circ R_{2\pi}$$

$$= R_{-\frac{\pi}{2} + 2\pi} = R_{\frac{3\pi}{2}}$$

Remark. $g \in G$ generates subgroup $\langle g \rangle \in G$

$$\langle R_{\frac{\pi}{2}} \rangle \subset GL_2(\mathbb{R})$$

$$= \{ R_{\frac{\pi}{2}}^n \mid n \in \mathbb{Z} \} = \{ R_{\frac{\pi}{2}}^0 = I_2$$

$$= \{ I_2, R_{\frac{\pi}{2}}, R_{\pi}, R_{\frac{3\pi}{2}} \}$$

cyclic group

order 4

$$R_{\frac{\pi}{2}}^1 = R_{\frac{\pi}{2}}$$

$$R_{\frac{\pi}{2}}^2 = R_{\pi}$$

$$R_{\frac{\pi}{2}}^3 = R_{\frac{3\pi}{2}}$$

$$R_{\frac{\pi}{2}}^4 = R_{2\pi} = I_2 \}$$

Ex. $\langle r_{10^\circ} \rangle$, note $0 = \frac{2\pi}{360}$

$$= \{ I_2, r_{10^\circ}, r_{20^\circ}, r_{30^\circ}, \dots, r_{350^\circ} \}$$

$\parallel$ $\parallel$ $\parallel$
 $r_{10^\circ}^2$ $r_{10^\circ}^3$ $r_{10^\circ}^{35}$

$r_{10^\circ}^{36} = r_{360^\circ} = r_0 = I_2$ ie. already in set
order 36

Ex. $\langle r_1 \rangle$, $1 = 1 \text{ radian} \sim 57^\circ$

$$\langle r_1 \rangle = \{ \dots, r_{-2}, r_{-1}, I_2, r_1, r_2, \dots \}$$

infinite order

$r_n \neq I_2$ since $\cos(n) \neq 1$
 means $n \notin 2\pi\mathbb{Z}$ ie. $n \notin \mathbb{Z}$

Lecture Notes:

2.12.24

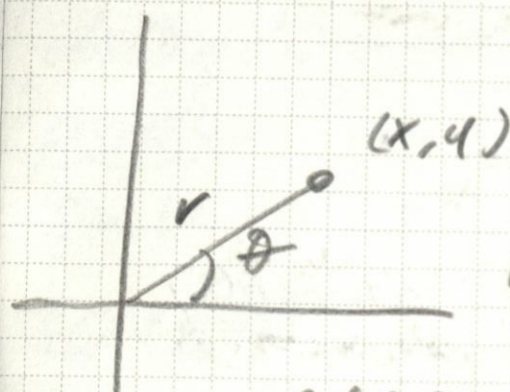
$O_2(\mathbb{R}) \subset GL_2(\mathbb{R})$ ie. subgroup of isometries, ie. preserved distance

r_α = rotation by α

s_α = reflection across L_α

$$r_\alpha = \begin{pmatrix} \cos \alpha & -\sin \alpha \\ \sin \alpha & \cos \alpha \end{pmatrix}$$

Side Remark: In polar coords



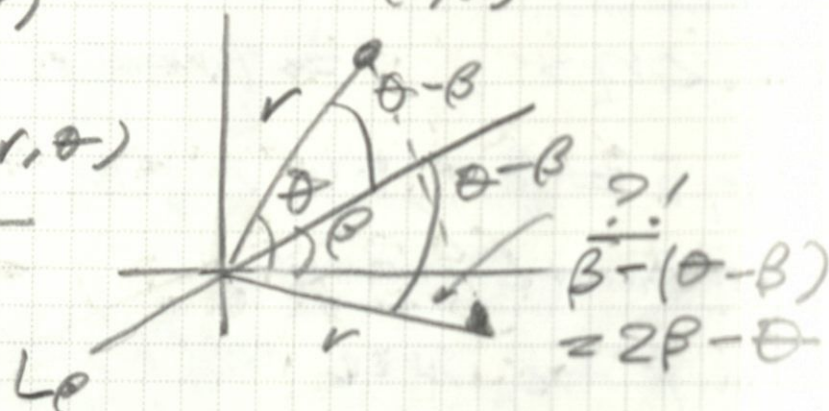
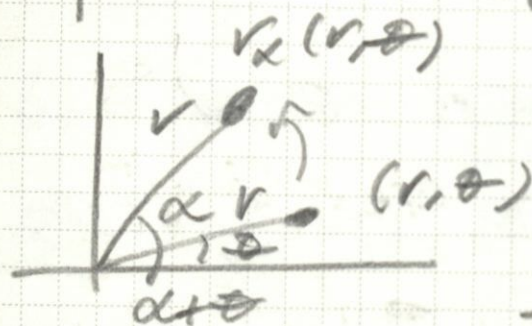
$$x = r \cos \theta$$

$$y = r \sin \theta$$

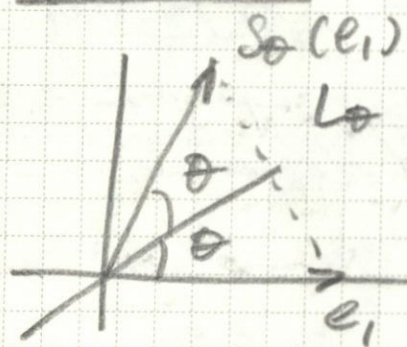
$$(x, y) \Leftrightarrow (r, \theta)$$

$$r_\alpha(r, \theta) = (r, \theta + \alpha)$$

$$s_\beta(r, \theta) = (r, 2\beta - \theta)$$



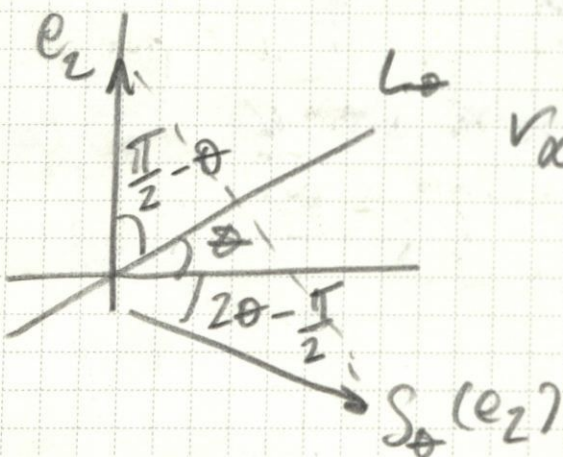
Matrix of S_θ : $S_\theta(e_1) = (\cos(2\theta), \sin(2\theta))$



$$S_\theta(e_2) = (\cos(2\theta - \frac{\pi}{2}), \sin(2\theta - \frac{\pi}{2}))$$

$$= (\sin(2\theta), -\cos(2\theta))$$

$$S_\theta = \begin{pmatrix} \cos 2\theta & \sin 2\theta \\ \sin 2\theta & -\cos 2\theta \end{pmatrix}$$



$$r_\alpha = \begin{pmatrix} \cos \alpha & -\sin \alpha \\ \sin \alpha & \cos \alpha \end{pmatrix}$$

$$S_0 = \begin{pmatrix} 1 & 0 \\ 0 & -1 \end{pmatrix}$$

Theorem: Every matrix in $O_2(\mathbb{R})$ is either V_α for some α or S_θ for some θ

Moreover, $S_\theta = V_\theta S_0 V_\theta^{-1}$

Remark. Something like this exists for $O_n(\mathbb{R})$. Gram-Schmidt decomposition

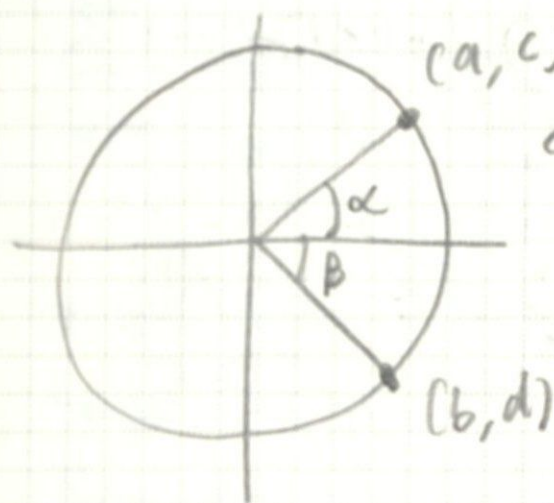
Proof. Fix $A \in O_2$ show $A = V_\alpha$ or S_θ

$$A = \left\{ \begin{pmatrix} a & b \\ c & d \end{pmatrix} \mid A^T = A^{-1} \Leftrightarrow A^T A = I_2 \right\}$$

$$A^T A = \begin{pmatrix} a & c \\ b & d \end{pmatrix} \begin{pmatrix} a & b \\ c & d \end{pmatrix} = \begin{pmatrix} 1 & 0 \\ 0 & 1 \end{pmatrix}$$

$$\Rightarrow \begin{cases} a^2 + c^2 = 1 \\ ab + cd = 0 \\ ba + dc = 0 \\ b^2 + d^2 = 1 \end{cases} =$$

Since $a^2 + c^2 = 1$, and $b^2 + d^2 = 1$
 $a = \cos \alpha$ and $c = \sin \alpha$ for some α
 $b = \cos \beta$ and $d = \sin \beta$ for some β



(a, c) also,

$$\cos \alpha \cos \beta + \sin \alpha \sin \beta = 0$$

$$\cos(\alpha - \beta) = 0$$

$$\text{so } \alpha - \beta = \pm \frac{\pi}{2}$$

$$\beta = \alpha \pm \frac{\pi}{2}$$

$$\text{so } A = \begin{pmatrix} \cos \alpha & \cos(\alpha + \frac{\pi}{2}) \\ \sin \alpha & \sin(\alpha + \frac{\pi}{2}) \end{pmatrix}$$

or

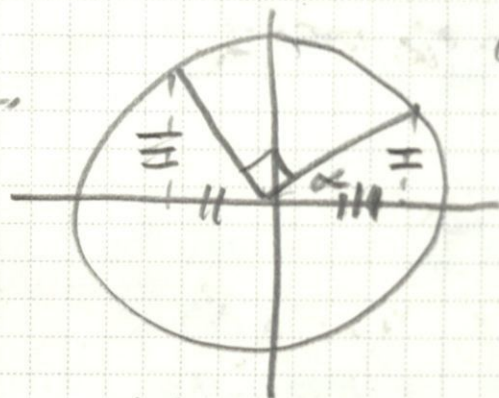
$$A = \begin{pmatrix} \cos \alpha & \cos(\alpha - \frac{\pi}{2}) \\ \sin \alpha & \sin(\alpha - \frac{\pi}{2}) \end{pmatrix}$$

$$A = \begin{pmatrix} \cos \alpha & -\sin \alpha \\ \sin \alpha & \cos \alpha \end{pmatrix} = R_\alpha$$

$\Rightarrow$ or

$$A = \begin{pmatrix} \cos \alpha & \sin \alpha \\ \sin \alpha & -\cos \alpha \end{pmatrix} = S_{\frac{\alpha}{2}}$$

note,



useful for:

$$\sin(\theta \pm \frac{\pi}{2})$$

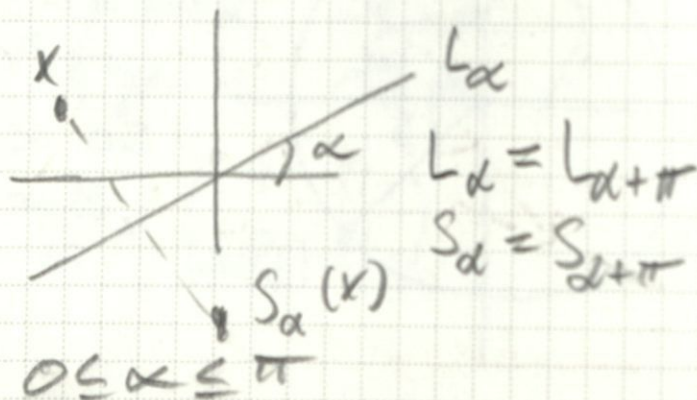
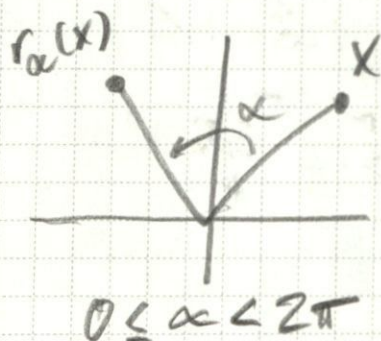
$$\cos(\theta \pm \frac{\pi}{2})$$

Lecture Notes:

2.14.25

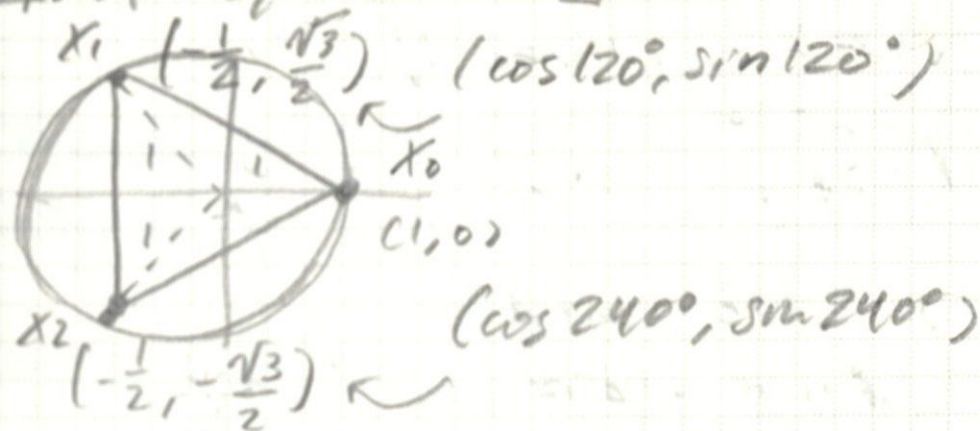
$$O_2(R) = \{ R_\alpha = \begin{pmatrix} \cos \alpha & -\sin \alpha \\ \sin \alpha & \cos \alpha \end{pmatrix} \mid \alpha \in [0, 2\pi) \}$$

$$\cup \{ S_\alpha = \begin{pmatrix} \cos \alpha & \sin \alpha \\ \sin \alpha & -\cos \alpha \end{pmatrix} \mid \alpha \in [0, \pi) \}$$



Def. Suppose $A \subset \mathbb{R}^2$ is any subset
 A symmetry of A is a matrix $g \in O_2(\mathbb{R})$
 st. $g(A) = A$

Ex. $A = \text{equilateral } \triangle \text{ with vertices}$



$g \in O_2(\mathbb{R})$ can only be r_α or s_α
 Can $r_\alpha(A) = A$?



$$\alpha = 0, \frac{2\pi}{3}, \frac{4\pi}{3}$$

$$r_\alpha(x_0) \in \{x_0, x_1, x_2\}$$

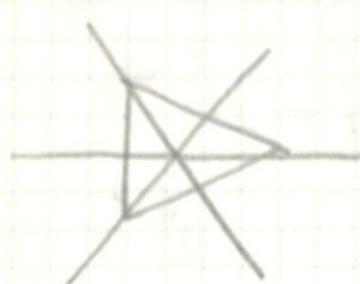
$$r_\alpha(x_0) = x_0 \Rightarrow \alpha = 0$$

$$r_\alpha(x_0) = x_1 \Rightarrow \alpha = \frac{2\pi}{3}$$

$$r_\alpha(x_0) = x_2 \Rightarrow \alpha = \frac{4\pi}{3}$$

Can $s_\alpha(A) = A$?

$\Leftrightarrow L_\alpha$ is a line of symmetry for A



L_0

L_{120}

$L_{240} = L_{60}$

$S_0, S_{\frac{\pi}{3}}, S_{\frac{2\pi}{3}}$

Symmetries of A : $\{r_0, r_{\frac{2\pi}{3}}, r_{\frac{4\pi}{3}}\} \cup \{s_0, s_{\frac{\pi}{3}}, s_{\frac{2\pi}{3}}\}$

Theorem. For any $A \in \mathbb{R}^2$

$$\text{Sym}(A) = \{ \text{all the symmetries of } A \} \subset O_2(\mathbb{R})$$

i.e. $\text{Sym}(A)$ is a subgroup of $O_2(\mathbb{R})$

$$\text{Eq. } \text{Sym}(\Delta) = \left\{ r_{\frac{2\pi}{3} \cdot k} \mid k=0,1,2 \right\} \cup \left\{ s_{\frac{\pi}{3} \cdot j} \mid j=0,1,2 \right\} \quad \text{subgroup of } O_2(\mathbb{R})$$

Proof. Suppose $g, h \in \text{Sym}(A)$

i.e. $g, h \in O_2(\mathbb{R})$ st $g(A) = A$ and $h(A) = A$

Check. $gh^{-1} \in \text{Sym}(A)$

i.e. $gh^{-1} \in O_2(\mathbb{R})$ and $gh^{-1}(A) = A$

automatic
as $O_2(\mathbb{R})$ is a group

Know. $h(A) = A$

$$h^{-1}(h(A)) = h^{-1}(A)$$

$$(h^{-1}h)(A) = h^{-1}(A) \quad \text{because all these are matrix multiplications and this is associative}$$

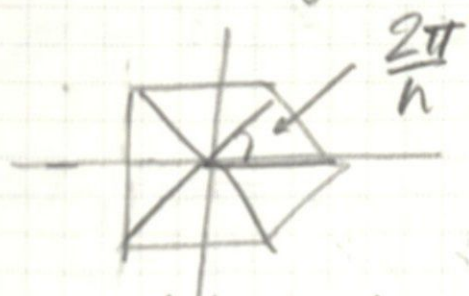
$$A = h^{-1}(A)$$

Check. $gh^{-1}(A) = A$

$$(gh^{-1})(A) = g(h^{-1}(A)) = g(A) = A$$

□

Def. P_n = regular n -gon



The dihedral group $D_n = \text{Sym}(P_n)$
 $= \{ \rho_{\frac{2\pi}{n}k} \mid 0 \leq k \leq n-1 \} \cup \{ s_{\frac{\pi}{n}j} \mid 0 \leq j \leq n-1 \}$

Lecture Notes:

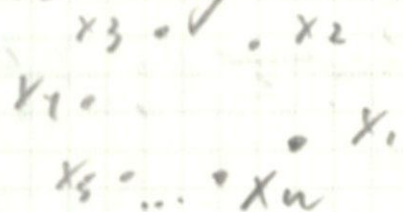
2.17.25

Symmetric Group & Permutations: J 85

$D_n \subset O_2(\mathbb{R}) \subset GL_2(\mathbb{R})$
 symmetries of P_n order $2n$ isometries in $\mathbb{R}^2$ linear transformations in $\mathbb{R}^2$

What does D_n do to P_n abstractly?

P_n = regular n -gon



$$D_6 = \{ \rho_{\frac{2\pi}{6}k} \mid 0 \leq k \leq 5 \} \cup \{ s_{\frac{\pi}{6}k} \mid 0 \leq k \leq 5 \}$$

$$= \{ e, r, r^2, r^3, r^4, r^5 \}$$

$$r = \rho_{\frac{2\pi}{6}} = \rho_{\frac{\pi}{3}} = \rho_{60^\circ}$$

$$\cup \{ s_0, r s_0, r^2 s_0, r^3 s_0, r^4 s_0, r^5 s_0 \}$$

$$\text{or } s_0, s_{\frac{\pi}{6}}, s_{\frac{2\pi}{6}}, \dots, s_{\frac{5\pi}{6}}$$

What does $g \in D_n$ do only to P_n not the whole $\mathbb{R}^2$?

$$\underline{D_6} \in (X_i) = x_i \quad \forall i$$

$$V: P_n \rightarrow P_n \quad \begin{matrix} x_1 & x_2 & x_3 & x_4 & x_5 & x_6 \\ \downarrow & \downarrow & \downarrow & \downarrow & \downarrow & \downarrow \\ x_2 & x_3 & x_4 & x_5 & x_6 & x_1 \end{matrix}$$

here notation:

$$V^2 = \begin{pmatrix} x_1 & x_2 & x_3 & x_4 & x_5 & x_6 \\ x_3 & x_4 & x_5 & x_6 & x_1 & x_2 \end{pmatrix}$$

$$S_6 = \begin{pmatrix} x_1 & x_2 & x_3 & x_4 & x_5 & x_6 \\ x_1 & x_6 & x_5 & x_4 & x_3 & x_2 \end{pmatrix}$$

Remark. $g \in D_n$ can be thought of as a permutation of vertices of P_n

Goal. Make sense of the group of permutations S_n then D_n as a subgroup of S_n

Def. $X_n = \{1, 2, \dots, n\}$

A permutation σ of X_n is a bijective function $\sigma: X_n \rightarrow X_n$

$$S_n = \{ \text{all permutations } \sigma: X_n \rightarrow X_n \}$$

Theorem. S_n is a group w.r.t composition of functions

$$\sigma, \tau: X_n \rightarrow X_n \quad \sigma \tau: X_n \rightarrow X_n$$

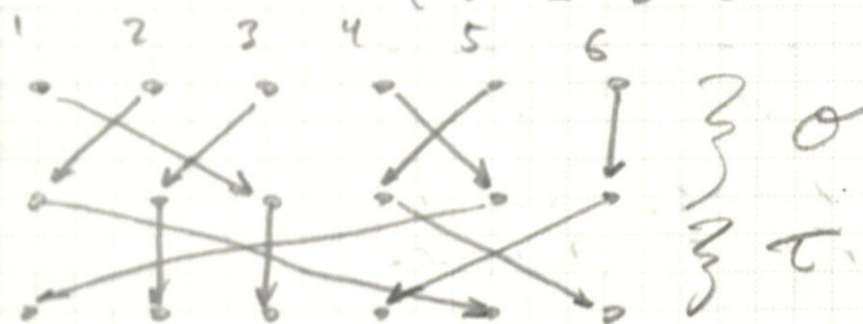
$$\sigma \tau = \sigma \circ \tau \text{ as a function}$$

Notation:

$$\sigma = (\sigma(1) \ \sigma(2) \ \sigma(3) \ \dots \ \sigma(n))$$

Ex. So $\sigma = \begin{pmatrix} 1 & 2 & 3 & 4 & 5 & 6 \\ 3 & 1 & 2 & 5 & 4 & 6 \end{pmatrix}$

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



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

($\tau \circ \sigma$)

note. $\sigma \tau = \sigma \circ \tau = \sigma(\tau(i)) \ \forall i$

note.

$$\begin{aligned} s^i r^k s^i &= r^{-k} \\ s^0 r^k s^0 &= r^k \\ s^k r^j s^k &= r^{(-1)^k \cdot j} \end{aligned}$$

$$S_n = \{ \sigma: X_n \rightarrow X_n \text{ bijective function} \}$$

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

Theorem. S_n is a group of order $n!$

PF. $|S_n| = n!$ $\sigma \in S_n$ $\sigma = \begin{pmatrix} 1 & 2 & \dots & n \\ \sigma(1) & \sigma(2) & \dots & \sigma(n) \end{pmatrix}$

Fill the bottom row one-by-one:

$$\sigma = \begin{pmatrix} 1 & 2 & 3 & \dots & n \\ \sigma(1) & \sigma(2) & \sigma(3) & \dots & \sigma(n) \end{pmatrix}$$

$\underbrace{\hspace{1cm}}_{n \text{ choices}} \quad \underbrace{\hspace{1cm}}_{n-1 \text{ choices}} \quad \underbrace{\hspace{1cm}}_{n-2 \text{ choices}} \quad \underbrace{\hspace{1cm}}_{1 \text{ choice}}$

$\sigma(2) \neq \sigma(1)$ so $n-1$ choices

$\sigma(3) \in \{1, 2, \dots, n\} - \{\sigma(1), \sigma(2)\}$
so $n-2$ choices

So total choices for $\sigma = n \cdot (n-1) \cdot \dots \cdot 1 = n!$

To check S_n is a group:

(0) composition law

$\sigma, \tau \in S_n$ verify $\sigma \circ \tau = \sigma \tau \in S_n$

(1) associativity

(2) unit

(3) inverses

(0) $\sigma, \tau : \{1, 2, \dots, n\} \rightarrow \{1, 2, \dots, n\}$ bijective
 $\sigma\tau = \sigma \circ \tau : \{1, 2, \dots, n\} \rightarrow \{1, 2, \dots, n\}$
WTS $\sigma \circ \tau$ is also bijective

Strategy. show 1-1 and onto

1-1. f is injective if $f(a) = f(b) \Rightarrow a = b$
or if $a \neq b$ then $f(a) \neq f(b)$

τ is bijective so injective
if $a \neq b$ then $\tau(a) \neq \tau(b)$

σ is bijective so injective
so $\sigma(\tau(a)) \neq \sigma(\tau(b))$

$\sigma\tau(a) \neq \sigma\tau(b) \Rightarrow \sigma\tau$ is inj

onto. f is surjective if $\forall b \exists a$ st $f(a) = b$

σ, τ surjective: to show $\sigma\tau$ is
surjective pick b and seek a
st. $\sigma\tau(a) = b$

$$\Leftrightarrow \sigma(\tau(a)) = b$$

surely can find c st $\sigma(c) = b$
because σ is surjective

if we can substitute $\tau(a) = c$
we'd be done since

$$\sigma(\tau(a)) = \sigma(c) = b$$

which of course we can do since
 τ is surjective

Aside. $X \xrightarrow{g} Y \xrightarrow{f} Z$ (different sets)
 $\text{fog} \rightarrow$

- 1) if f & g are injective so is fog
- 2) if f & g are surjective so is fog
- 3) if fog is injective then g is injective
- 4) if fog is surjective then f is surjective

Strategy 2:

A function f is bijective $\Leftrightarrow f^{-1}$ exists

σ^{-1} exists, τ^{-1} exists

Claim. $(\sigma \circ \tau)^{-1} = \tau^{-1} \circ \sigma^{-1}$
 $\sigma \circ \tau (\tau^{-1} \circ \sigma^{-1}) = \sigma \circ \tau \circ \tau^{-1} \circ \sigma^{-1}$
 $= \sigma \circ \text{id} = \sigma$

This clearly exists so $\sigma \circ \tau$ is invertible
so it is a bijection

(1) $\sigma \circ (\tau \circ \gamma) = (\sigma \circ \tau) \circ \gamma \quad \forall \sigma, \tau, \gamma \in S_n$
 $\sigma \circ (\tau \circ \gamma)(x) = \sigma(\tau(\gamma(x))) = (\sigma \circ \tau)(\gamma(x))$
 $(\sigma \circ \tau) \circ \gamma(x) = (\sigma \circ \tau)(\gamma(x)) = \sigma(\tau(\gamma(x)))$

(2) $\sigma(x) = x \quad \forall x \in \{1, 2, \dots, n\}$
so $\sigma = \text{id}$

(3) $\sigma \text{ bij} \Rightarrow \sigma^{-1} \in S_n$ st. $\sigma \circ \sigma^{-1} = \sigma^{-1} \circ \sigma = \text{id}$

Exam 4 Review:

2.20.25

Composition Law: a function m on a set X st.

$$m: X \times X \rightarrow X$$

Group: A set together with a composition law = st.

(0) Composition Law?

$$\forall x, y \in G \Rightarrow x \circ y \in G$$

(1) Associativity?

$$\forall x, y, z \in G \Rightarrow (x \circ y) \circ z = x \circ (y \circ z)$$

(2) Unit?

$$\forall x \in G \Rightarrow \exists e \in G \text{ st. } x \circ e = e \circ x = x$$

(3) Inverse?

$$\forall x \in G \Rightarrow \exists x^{-1} \in G \text{ st. } x \circ x^{-1} = x^{-1} \circ x = e$$

Theorem. every subgroup of $\mathbb{Z}, +$ is of the form $n\mathbb{Z}$ for some $n \in \mathbb{Z}$
 n = smallest positive # > 0

Consequence.

$$(a_1, a_2, \dots, a_n) = a_1\mathbb{Z} + a_2\mathbb{Z} + \dots + a_n\mathbb{Z} = d\mathbb{Z}$$

where $d = \gcd(a_1, a_2, \dots, a_n)$

Lemma. The unit and inverse of a group is unique

Theorem. H is a subgroup of G if

$$\forall x, y \in H \Rightarrow xy^{-1} \in H$$

Lemma. $\forall x_1, x_2, \dots, x_n \in G$

$$(x_1 x_2 \dots x_n)^{-1} = x_n^{-1} x_{n-1}^{-1} \dots x_1^{-1}$$

Def. $a \equiv b \pmod{n} \Rightarrow a - b \in n\mathbb{Z}$
ie. $n \mid a - b$

Prop. (1) $a \equiv a \pmod{n}$

$$(2) a \equiv b \pmod{n} \Rightarrow b \equiv a \pmod{n}$$

(3) if $a \equiv b \pmod{n}$ and $b \equiv c \pmod{n}$
then $a \equiv c \pmod{n}$

(4) if $a \equiv b \pmod{n}$ and $a' \equiv b' \pmod{n}$:
 $a + a' \equiv b + b' \pmod{n}$
 $a \cdot a' \equiv b \cdot b' \pmod{n}$

Def. $\mathbb{Z}_n = \{\bar{0}, \bar{1}, \bar{2}, \dots, \overline{(n-1)}\}$, +
note. $\bar{k} = k \pmod{n}$

Euclidean Alg. : if $a = dq + r$ then
 $\gcd(a, d) = \gcd(d, r) = (n, 0) = n$

Def. $U_n = \mathbb{Z}_n^\times = \{\bar{a} \in \mathbb{Z}_n \mid (a, n) = 1\}$

Thm. $(U_n, \cdot)$ is a group where $\bar{a} \cdot \bar{b} = \overline{a \cdot b}$

Def. $\forall \bar{a} \in \mathbb{Z}_n^\times \Rightarrow \exists x = a^{-1}$ st.
 $ax \equiv 1 \pmod{n}$

Def. Cyclic group generated by a $g \in G$ st.:

$\langle g \rangle = \{g^m \mid m \in \mathbb{Z}\}$ which is always a subgroup of G

if $g^N = e$ where N is the smallest such pos #,
order of $\langle g \rangle = N$

note. $g^a (g^b)^{-1} = g^{a-b} \in \langle g \rangle$

$$\text{def. } GL_n(\mathbb{R}) = \{X = \text{Matrix}(\mathbb{R}) \mid \det X \neq 0\} \\ \Leftrightarrow X^{-1} \text{ exists} \\ = \{T: \mathbb{R}^n \rightarrow \mathbb{R}^n \mid T \text{ bijective}\}$$

Matrix of T: need basis $\mathcal{B} = \{\vec{v}_1, \vec{v}_2, \dots, \vec{v}_n\}$

$$[T]_{\mathcal{B}} = [T(\vec{v}_1) \mid T(\vec{v}_2) \mid \dots \mid T(\vec{v}_n)]$$

note. $T_{AB} = T_A \circ T_B$

Def. $O_n(\mathbb{R}) = \{X \in GL_n(\mathbb{R}) \mid X^T = X^{-1}\}$
subgroup of $GL_n(\mathbb{R}) \Leftrightarrow X^T X = I_n$

note. $\det(X^{-1}) = \frac{1}{\det(X)}$

note. $(AB)^{-1} = B^{-1}A^{-1}$, $(AB)^T = B^T A^T$

Theorem. Every matrix in $O_2(\mathbb{R})$ is either R_α or S_α

Moreover, $S_\alpha = R_\alpha S_0 R_\alpha^{-1}$

$$O_2(\mathbb{R}) = \{R_\alpha = \begin{pmatrix} \cos \alpha & -\sin \alpha \\ \sin \alpha & \cos \alpha \end{pmatrix} \mid \alpha \in [0, 2\pi)\} \\ \cup \{S_\alpha = \begin{pmatrix} \cos \alpha & \sin \alpha \\ \sin \alpha & -\cos \alpha \end{pmatrix} \mid \alpha \in [0, \pi)\}$$

Def. A symmetry of A is a matrix $g \in O_2(\mathbb{R})$ st. $g(A) = A$

$\text{Sym}(A) = \{\text{all symmetries of } A\} \subset O_2(\mathbb{R})$
subgroup of $O_2(\mathbb{R})$

Def. Dihedral group $D_n = \text{Sym}(P_n)$

$$= \left\{ R_{\frac{2\pi k}{n}} \mid 0 \leq k \leq n-1 \right\} \cup \left\{ S_{\frac{\pi j}{n}} \mid 0 \leq j \leq n-1 \right\}$$

Lecture Notes:

2.24.25

Recall: $S_n = \{ \text{all permutations} \}$

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

$(S_n, \text{composition of functions}) = \text{group of order } n!$

$n=1$: $S_1 = \{ \sigma: \{1\} \rightarrow \{1\} \} = \{e\}, |S_1| = 1!$

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

$n=2$: $S_2 = \{ \sigma: \{1, 2\} \rightarrow \{1, 2\} \text{ bijective} \}$
 $|S_2| = 2! = 2$

enumerate: $\begin{pmatrix} 1 & 2 \\ 1 & 2 \end{pmatrix}, \begin{pmatrix} 1 & 2 \\ 2 & 1 \end{pmatrix}$

$n=3$: $|S_3| = 3! = 6$, enumerate

$\begin{pmatrix} 1 & 2 & 3 \\ 1 & 2 & 3 \end{pmatrix}, \begin{pmatrix} 1 & 2 & 3 \\ 2 & 1 & 3 \end{pmatrix}, \begin{pmatrix} 1 & 2 & 3 \\ 1 & 3 & 2 \end{pmatrix}, \begin{pmatrix} 1 & 2 & 3 \\ 2 & 3 & 1 \end{pmatrix},$
 $\begin{pmatrix} 1 & 2 & 3 \\ 3 & 1 & 2 \end{pmatrix}, \begin{pmatrix} 1 & 2 & 3 \\ 3 & 2 & 1 \end{pmatrix}$

Worksheet: Enumerate S_4

* transpositions: 1 of the elements stay intact
* more complicated

Multiplication: $\sigma = \begin{pmatrix} 1 & 2 & 3 \\ 2 & 3 & 1 \end{pmatrix}$

$$\sigma^2 = \sigma \circ \sigma = \begin{pmatrix} 1 & 2 & 3 \\ \sigma(\sigma(1)) & \sigma(\sigma(2)) & \sigma(\sigma(3)) \end{pmatrix}$$
$$= \begin{pmatrix} 1 & 2 & 3 \\ 3 & 1 & 2 \end{pmatrix}$$

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

$$\underline{S_6}: \begin{pmatrix} 1 & 2 & 3 & 4 & 5 & 6 \\ 5 & 3 & 1 & 2 & 6 & 4 \end{pmatrix} \circ \begin{pmatrix} 1 & 2 & 3 & 4 & 5 & 6 \\ 3 & 1 & 6 & 2 & 5 & 4 \end{pmatrix} \\ = \begin{pmatrix} 1 & 2 & 3 & 4 & 5 & 6 \\ 1 & 5 & 4 & 3 & 6 & 2 \end{pmatrix}$$

note. $\sigma \circ \tau(k) = \sigma(\tau(k))$

↑ reorder
columns

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

* dangerous, not real math *

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

How to list $\langle \sigma \rangle = \{e, \sigma, \sigma^2, \dots, \sigma^{N-1}\}$
 where $\sigma^N = e$

$$\sigma^2 = \begin{pmatrix} 1 & 2 & 3 & 4 & 5 & 6 \\ 6 & 1 & 5 & 3 & 4 & 2 \end{pmatrix}$$

$$\sigma^3 = \sigma^2 \circ \sigma = \begin{pmatrix} 1 & 2 & 3 & 4 & 5 & 6 \\ 4 & 5 & 6 & 1 & 2 & 3 \end{pmatrix}$$

$$\sigma^4 = \sigma^3 \circ \sigma = \begin{pmatrix} 1 & 2 & 3 & 4 & 5 & 6 \\ 2 & 6 & 4 & 5 & 3 & 1 \end{pmatrix}$$

$$\sigma^5 = \sigma^4 \circ \sigma = \begin{pmatrix} 1 & 2 & 3 & 4 & 5 & 6 \\ 3 & 4 & 2 & 6 & 1 & 5 \end{pmatrix}$$

$$\sigma^6 = \sigma^5 \circ \sigma = \begin{pmatrix} 1 & 2 & 3 & 4 & 5 & 6 \\ 1 & 2 & 3 & 4 & 5 & 6 \end{pmatrix} = e$$

so $\langle \sigma \rangle = \{e, \sigma, \sigma^2, \sigma^3, \sigma^4, \sigma^5\}$
 since $\sigma^6 = e$

Easier way to compute $\sigma^N = e$ ($N = \text{order}$)
 Keep track of each element and determine
 how soon it goes back to start

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

of
times
we apply

	1	2	3	4	5	6
3	3	1	6	2		
6	6	3	4	1		
4	4	6	2	3		
2	2	4	1	6		
1	1	2	3	4		

seek
 $\tau^5 = e$

Ex.

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

Keep track how many times we apply
 γ to go back to start

k	1	2	3	4	5	6
# times	3	2	1	2	3	3

$\gamma^m(k) = k$

order of $\langle \gamma \rangle = \text{LCM of these}$
 $= \text{LCM}(3, 2, 1, 2, 3, 3) = 6$

Lecture Notes:

2.26.25

Goal. understand the structure of groups

eg. what are their subgroups?

Are there relations between groups? $\leftarrow$ now

Later

eg. $n\mathbb{Z}$ subgroup of $\mathbb{Z}$

$$\langle r \rangle \subset D_n$$

$$\langle g \rangle \subset G$$

} all ad-hoc
not real abstract
theory

Today. understand cyclic groups

if $G = \text{any group}$, $g \in G$

$\langle g \rangle = \{g^x \mid x \in \mathbb{Z}\}$ is a subgroup of G

Eg. $n \in (\mathbb{Z}, +)$

$$\langle n \rangle = \{n \cdot x \mid x \in \mathbb{Z}\} = n\mathbb{Z}$$

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

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

note. $\langle e \rangle = \{e^x \mid x \in \mathbb{Z}\} = \{e\}$

Eg. $(\mathbb{Z}_n, +)$

if $2 \in \mathbb{Z}_{10}$

$$\langle 2 \rangle = \{2x \mid x \in \mathbb{Z}\}$$

$$= \{\bar{0}, \bar{2}, \bar{4}, \bar{6}, \bar{8}\} \subset \mathbb{Z}_{10}$$

order of $\bar{2}$ is 5

Eg. $(U_n, \cdot)$

$2 \in (U_{15}, \cdot)$

$$\langle 2 \rangle = \{ 2^x \mid x \in \mathbb{Z} \}$$

$$= \{ 1, 2, 4, 8 \}$$

$2^4 = 16 \equiv 1 \pmod{15}$ so stop

2 has order 4

Eg. $2 \in (\mathbb{R}^+, \cdot)$

$$\langle 2 \rangle = \{ 2^x \mid x \in \mathbb{Z} \}$$

$$= \{ \dots, \frac{1}{8}, \frac{1}{4}, \frac{1}{2}, 1, 2, 4, 8, \dots \}$$

Strategy. Understand cyclic groups and their subgroups

Eg. $D_n = \{ e, r, r^2, \dots, r^{n-1} \}$
 $\cup \{ s, rs, \dots, r^{n-1}s \}$

$r = r_{\frac{2\pi}{n}}$ $s = s_0$

$$\langle r \rangle = \{ e, r, \dots, r^{n-1} \} \subset D_n$$

$$\langle s \rangle = \langle s_0 \rangle = \{ e, s \}$$

$$\langle rs \rangle = \langle s_{\frac{\pi}{n}} \rangle = \{ e, rs \}$$

$$\vdots$$

$$\langle r^k s \rangle = \langle s_{\frac{k\pi}{n}} \rangle = \{ e, r^k s \}$$

Recall. $(G, \cdot)$ is a group. $g \in G$

$H = \{n \mid g^n = e\} \subset (\mathbb{Z}, +)$ is a subgroup

check xy^t criteria:

for $(\mathbb{Z}, +)$, it is really $x + (-y)$ criteria

note § 4.1 in textbook

Know every subgroup of $\mathbb{Z}$ is $N \cdot \mathbb{Z}$

$$\{n \mid g^n = e\} = N \cdot \mathbb{Z}$$

Case 1. $\{m \mid g^m = e\} = 0 \cdot \mathbb{Z} = \{0\} = H_g$

means $g^0 = e$ & no other $g^m = e$

eg. $\langle g \rangle = g\mathbb{Z} \subset \mathbb{Z}$

$$H = \{m \mid g^m = 0\} = \begin{cases} \mathbb{Z} & \text{if } g = 0 \\ \{0\} & \text{if } g \neq 0 \end{cases}$$

note. $H_e = \mathbb{Z}$

eg. $\mathbb{Z} \in (\mathbb{R}^+, \cdot)$

$$H_2 = \{m \mid 2^m = 1\} = \{0\}$$

Case 2. $H_g = \{m \in \mathbb{Z} \mid g^m = e\} = N\mathbb{Z}$

$N =$ smallest possible entry with H_g if $N > 0$

Corollary - if there is an exponent $N > 0$

st $g^N = e$ & $N =$ smallest such exponent

then $g^m = e \iff N \mid m$

$$g^x = g^y \iff x \equiv y \pmod{N}$$

Pf. if $N = \text{smallest } > 0 \text{ st } g^N = e$

then $H_g = \{ m \text{ st } g^m = e \} = N \cdot \mathbb{Z}$

$$\Leftrightarrow \{ n \text{ st } g^n = e \} = \{ m \text{ st } N | m \}$$

$$\text{since } g^m = e \Leftrightarrow N | m$$

note $g^x = g^y \Leftrightarrow g^{x-y} = e$

$$\Leftrightarrow N | x - y \Leftrightarrow x \equiv y \pmod{N}$$

Def. if $g^m = e \Leftrightarrow m = 0$ say $\text{ord}(g) = \infty$

if $g^N = e$ & $N > 0$ smallest exponent $\text{ord}(g) = N$

Corollary. if $\text{ord}(g) < \infty$

$$g^x = g^y \Leftrightarrow x \equiv y \pmod{\text{ord}(g)}$$

Theorem 1: if $g \in G$

then $\langle g \rangle$ has order $= \text{ord}(g)$

Theorem 2: Every subgroup of a cyclic group is also cyclic

Moreover, we can relate their orders

$$\begin{array}{ccc} \text{wte. generators } \mathbb{Z} & = & n\mathbb{Z} \\ \text{cyclic } \langle 1 \rangle & & \text{cyclic } \langle n \rangle \end{array}$$

Exam. 38/50

$$\geq 36 \quad B$$

$$\geq 43 \quad A$$

Lecture Notes:

2.28.25

$g \in G$, $H_g = \{n \in \mathbb{Z} \text{ st } g^n = e\}$
 $0 \in H_g$ since $g^0 = e$
subgroup of $\mathbb{Z}$

(1) $H_g = \{0\}$

$g^n \neq e$ if $n \neq 0$ so $\text{ord}(g) = \infty$

(2) $H_g = N \cdot \mathbb{Z}$

$N > 0$ smallest st. $g^N = e \Rightarrow \text{ord}(g) = N$

Theorem 1. $\langle g \rangle \subset G$

this has order $\text{ord}(g)$

Pf. if $g^N = e$ for $N > 0$ where N is smallest

On HW we showed,

$$\langle g \rangle = \{e, g, g^2, \dots, g^{N-1}\}$$

$v \in$ distinct

$$g^h = g^{Nq+r} \text{ where } h = Nq + r$$

$$= (g^N)^q \cdot g^r = \underbrace{e}_e \cdot g^r = g^r$$

$$|\langle g \rangle| = N = \text{ord}(g)$$

$$\text{Pr. } \text{ord}(g) = \infty$$

Claim. $\langle g \rangle = \{ \dots, g^{-2}, g^{-1}, e, g, g^2, \dots \}$
and all these are distinct ($\neq$)

$$\Rightarrow |\langle g \rangle| = \infty$$

By contradiction. $\exists a \neq b$ st. $g^a = g^b$

note $2^a = 2^b \Rightarrow 2^{a-b} = 1$

$$\text{so } g^{a-b} = e$$

which implies $a-b \in H_g$ which is impossible since $H_g = \{0\}$ and $a \neq b$

Back to A.

$$\begin{aligned} \langle g \rangle &= \{ g^n \mid n \in \mathbb{Z} \} \\ &= \{ g^0, g^1, g^2, \dots, g^{N-1} \} \end{aligned}$$

eg. $N=3$ we need

$$\{ g^n \mid n \in \mathbb{Z} \} = \{ e, g, g^2 \}$$

show $g^{-1} \in \{ e, g, g^2 \}$ & $g^3 = e$

$$g^{-1} = g^{-1} \cdot g^3 = g^2$$

$$\text{or } -1 = 3 \cdot (-3) + 2$$

$$g^{-1} = g^{3 \cdot (-3) + 2} = (g^3)^{-3} \cdot g^2 = g^2$$

Consequences:

- If $g \in G$ has $\text{ord}(g) = |G|$ then automatically G is cyclic

Reason - if $|G| = n = \text{ord}(g)$

$\langle g \rangle \subset G$ so $\langle g \rangle = G$
n elements n elements
by thm by def

- If there is no $g \in G$ of order n , then G is not cyclic

Theorem. If G is a cyclic group, every subgroup H of G is also cyclic

Recall. $G = \mathbb{Z} = \langle 1 \rangle$

$H \subset G$ is of the form $H = N \cdot \mathbb{Z} = \langle N \rangle$

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

$P_{H,g} = \{n \in \mathbb{Z} \mid g^n \in H\}$

note. $H_g = \{n \text{ st } g^n = e\}$

$P_{\{e\},g} = \{n \text{ st } g^n \in \{e\}\}$

Claim. $P_{H,g} \subset \mathbb{Z}$ is a subgroup

Subgroup Criteria. $\forall x, y \in H \Rightarrow xy^{-1} \in H$

Check. $m, n \in P_{H,g} \subset (\mathbb{Z}, +)$ show
 $m - n \in P_{H,g}$

START. with the definition

$$\text{know } \begin{cases} m \in P_H, g \longleftrightarrow g^m \in H \\ n \in P_H, g \longleftrightarrow g^n \in H \end{cases}$$

$$\text{WTS } \{m-n \in P_H, g \longleftrightarrow \underbrace{g^{m-n}}_{\text{clearer}} \in H\}$$

H is a group:

$$\begin{aligned} &\Rightarrow g^{-n} \in H \text{ by inverse property} \\ &\Rightarrow \underbrace{g^m}_{\in H} \cdot \underbrace{g^{-n}}_{\in H} = g^{m-n} \in H \end{aligned}$$

note. every $g \in H$ forms a cyclic group regardless of G , but $\langle g \rangle$ may

- have nothing to do w/ G
- may be $= G$

ex. S_n has order $n! \sim \left(\frac{n}{e}\right)^n$

largest cyclic subgroup $\sim e^{\sqrt{n \log n}} \ll \left(\frac{n}{e}\right)^n$
much smaller

Lecture Notes:

3.3.25

Theorem. Every subgroup of a cyclic group is cyclic

Pf. $H \leq G = \langle g \rangle = \{g^n \mid n \in \mathbb{Z}\}$
 $\uparrow$ generator

Caution. A cyclic group has more than one generators

$$\mathbb{Z} = \langle 1 \rangle = \langle -1 \rangle$$

Aim. Show H is also cyclic

i.e. $H = \langle h \rangle$ for some $h \in H \leq G$
so $h = g^m$ for some m

Aim. seek exponent $m \in \mathbb{Z}$ st.

$$H = \underbrace{\langle g^m \rangle}_h = \{ (g^m)^x \mid x \in \mathbb{Z} \}$$

Strategy. focus only on exponent

Define. $P_{H,g} = \{ n \in \mathbb{Z} \mid \text{st } \underbrace{g^n}_{\text{always in } G} \in H \}$

Claim. $P_{H,g} \subset \mathbb{Z}$ is a subgroup

if so $P_{H,g} = m\mathbb{Z}$ for some m no idea what this is...

Then we're done:

$$H = \{ g^x \in H \}$$

$$= \{ g^x \mid x \in P_{H,g} \}$$

$$= \{ g^{my} \mid y \in \mathbb{Z} \} = \{ (g^m)^y \mid y \in \mathbb{Z} \}$$

$$= \langle g^m \rangle. \quad \square$$

Pt of Claims.

Pick $x, y \in P_{H,g}$ show $x-y \in P_{H,g}$

$$\begin{array}{ccc} \downarrow & & \downarrow \\ g^x, g^y \in H & \text{show} & g^{x-y} \in H \\ & & g^{x-u} \cdot (g^y)^{-1} \end{array}$$

Ex. $H = G$, $m = 1$

$H = \{e\}$, $m = 0$?

Eg. $G = \langle g \rangle$, $H = \{e\} \subset G$

$$P_{H,g} = \{n \in \mathbb{Z} \mid g^n \in \{e\}\}$$

$$= \{n \mid g^n = e\}$$

$$= \text{Hq subgroup of } \mathbb{Z} = N \cdot \mathbb{Z}$$

where $N = \text{ord}(g) \neq 0$

$$g^N = e, H = \langle g^N \rangle = \{e\}$$

Eg. $G = (\mathbb{Z}_{10}, +)$

$H = \langle a \rangle$ for some $a \in \mathbb{Z}_{10} = \langle 1 \rangle$

a	$\langle a \rangle$
-----	---------------------

0	0
---	---

1	$\mathbb{Z}_{10}$
---	-------------------

2	$\{0, 2, 4, 6, 8\}$
---	---------------------

3	$\{0, 3, 6, 9, 2, 5, 8, 1, 4, 7\} = \mathbb{Z}_{10}$
---	--

4	$\{0, 4, 8, 2, 6\}$
---	---------------------

5	$\{0, 5\}$
---	------------

6	$\{0, 6, 2, 8, 4\}$
---	---------------------

7	$\mathbb{Z}_{10}$
---	-------------------

8	$\{0, 2, 4, 6, 8\}$
---	---------------------

9	$\mathbb{Z}_{10}$
---	-------------------

Observations:

- (1) if coprime, generate entire group
- (2) seems to depend on $\gcd(a, 10)$
- (3) orders $\mid 10$
- (4) How many times does each size appear?

Aside. finding divisors.

$$\text{if } N = p_1^{m_1} \dots p_k^{m_k}$$

$d \mid N$ means

$$d = p_1^{l_1} \dots p_k^{l_k} \text{ for } 0 \leq l_1 \leq m_1, \dots, 0 \leq l_k \leq m_k$$

divisors

$$= (m_1 + 1) \cdot (m_2 + 1) \cdot \dots \cdot (m_k + 1)$$

Ex. divisors of $24 = 2^3 \cdot 3$

$$d = 2^0, 1, 2, 0 \cdot 3^0, 0 \cdot 3^1$$

so 8 possibilities

Return to (4):

order	# times
1	1 = $\phi(1)$
2	1 = $\phi(2)$
5	4 = $\phi(5)$
10	4 = $\phi(10)$
10	

note $\phi(n) = |\phi_n|$

Lecture Notes:

3.5.25

Prop. G group w/ $g \in G$

If $\text{ord}(g) = \infty$ then $\text{ord}(g^m) = \infty$ if $m \neq 0$

If $\text{ord}(g) = N$ then $\text{ord}(g^m) = \frac{N}{(m, N)}$

Corollary. Suppose $\text{ord}(g) = N$, $G = \langle g \rangle$
then every element of G has order $|N$
and if $n | N$ then there are exactly
 $\phi(n)$ elements of order n

Proof of Corollary.

An element of G is of the form g^m

$n = \text{ord}(g^m) = \frac{N}{(m, N)}$ by Thm so $n | N$

eg. when $N = 10$

$(m, 10) = 1, 2, 5, \text{ or } 10$

order = 10, 5, 2, or 1

Suppose. $n | N$ let's count how many
of the $g^m \in G$ have order n .

Solve $\text{ord}(g^m) = n$ for m

Solve $\frac{N}{(m, N)} = n$ for m

$$(m, N) = \frac{N}{n}$$

Ex. Solve for $m = 0, 1, 2, \dots, 9$

$$N=10 \quad \text{st } (m, 10) = \frac{10}{5} = 2$$

$$n=5 \quad m = 2M \quad \text{because } 2|m$$

answer $(2M, 10) = 2$

$$\begin{array}{l} 2, 4 \\ 6, 8 \end{array} \quad (M, 5) = 1 \Rightarrow M = 0, 1, 2, 3, 4$$

of such M
is $\phi(5)$

$$\Leftrightarrow M \in U_5$$

In general, $D = \frac{N}{n}$

count m st. $(m, N) = D$

since $D|m$, $m = D \cdot M < N$

so $(D \cdot M, N) = D \quad 0 \leq M < n$

$$D \cdot (M, \frac{N}{D}) = D \quad \text{here } \frac{N}{D} = n$$

$$(M, n) = 1$$

so $M \in U_n$

Ex. $G = \langle g \rangle$ $\text{ord}(g) = 30 = 2 \cdot 3 \cdot 5$

What can the orders of elements of G be?

$$\text{ord}(x \in G) \mid 30$$

n	u	$\ell(u) = U_n $
$2^0 \cdot 3^0 \cdot 5^0$	1	1
$2^1 \cdot 3^0 \cdot 5^0$	2	1
$2^0 \cdot 3^1 \cdot 5^0$	3	2
$2^0 \cdot 3^0 \cdot 5^1$	5	2
$2^1 \cdot 3^1 \cdot 5^0$	6	4
$2^1 \cdot 3^0 \cdot 5^1$	10	4
$2^0 \cdot 3^1 \cdot 5^1$	15	8
$2^1 \cdot 3^1 \cdot 5^1$	30	8

we'll have a formula for $\ell(u)$ soon

Which elements have order 15?

$$u = 15 \quad \text{ord}(g^u) = 15$$

$$(u, 30) = D = \frac{30}{15} = 2$$

$$m = 2M \quad (M, 15) = 1$$

$$U_{15} = \{ \cancel{1}, \textcircled{2}, \cancel{3}, \textcircled{4}, \cancel{5}, \textcircled{6}, \cancel{7}, \textcircled{8}, \cancel{9}, \textcircled{10}, \cancel{11}, \textcircled{12}, \textcircled{13}, \textcircled{14} \}$$

$$\{ g^u \in G \text{ st. } \text{ord}(g^u) = 15 \}$$

$$= \{ 2 \cdot M \mid M \in U_{15} \}$$

$$= \{ 2 \cdot 1, 2 \cdot 2, 2 \cdot 4, 2 \cdot 7, 2 \cdot 8, 2 \cdot 11, 2 \cdot 13, 2 \cdot 14 \}$$

Consequences from cyclic groups and orders:

From wk st. if G = abelian group
of order N , then $a^N = e \forall a \in G$
and $\text{ord}(a) \mid N$

Ex. $G = U_n$ Euler's Theorem.

$$|G| = N = |U_n| = \varphi(n)$$

$$\forall a \in U_n, \text{ i.e., } (a, n) = 1 \text{ then } a^{\varphi(n)} \equiv 1 \pmod{n}$$

wk.

$$a^8 \equiv 1 \pmod{15} \forall a \in U_{15} \Rightarrow \varphi(15) = 8$$

$$a^6 \equiv 1 \pmod{14} \forall a \in U_{14} \Rightarrow \varphi(14) = 6$$

If $n = p$ is a prime number

$$U_p = \{0, 1, 2, \dots, p-1\}$$

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

Fermat's Little Theorem:

if $a \not\equiv 0 \pmod{p}$ then

$$a^{p-1} \equiv 1 \pmod{p}$$

Lecture Notes:

3.7.25

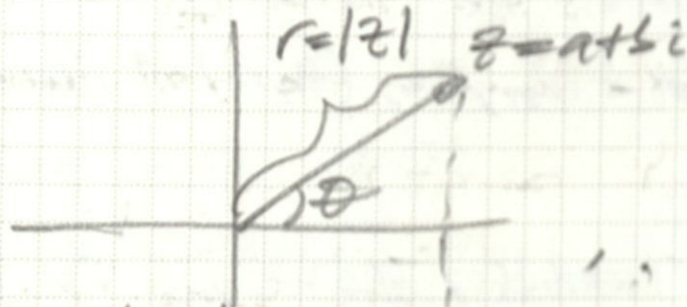
$$\mathbb{C} = \{z = a+bi \mid a, b \in \mathbb{R}\}$$

$$i = \sqrt{-1}, i^2 = -1, e^{\pi i} = -1$$

$$\text{if } z = a+bi \text{ then } \bar{z} = a-bi$$

$$|z| = \text{distance to the origin} = \sqrt{a^2+b^2}$$

$$|z|^2 = a^2 + b^2$$



Note, $\text{Re } z = a$ real part

$\text{Im } z = b$ imaginary part

$$\arg z = \theta$$

We can also: $z \cdot w \in \mathbb{C}$

$$z = a+bi \quad z \cdot w = (a+bi)(A+Bi)$$

$$w = A+Bi \quad = aA + aBi + Abi + bBi^2$$

$$= (aA - bB) + (aB + Ab)i$$

$$\in \mathbb{C}$$

R. you can multiply complex numbers!
you cannot multiply vectors

Properties

$$(1) |z|^2 = z \cdot \overline{z} \quad \text{complex conjugate}$$

$$(2) \overline{z \cdot w} = \overline{z} \cdot \overline{w}$$

$$\overline{z+w} = \overline{z} + \overline{w}$$

$$(3) |z \cdot w| = |z| \cdot |w|$$

$$(4) \text{ if } z \neq 0 \text{ then } \frac{1}{z} \in \mathbb{C}$$

complex numbers are both numbers and vectors

Pf. If $z = a + bi$

$$\begin{aligned} \frac{1}{z} &= \frac{1}{a+bi} = \frac{a-bi}{(a+bi)(a-bi)} = \frac{a-bi}{a^2+b^2} \\ &= \left(\frac{a}{a^2+b^2}\right) - \left(\frac{b}{a^2+b^2}\right)i \in \mathbb{C} \end{aligned}$$

$\mathbb{C}$ form a field $\rightarrow$ can add, multiply, and divide (anything but 0)

Theorem. $\mathbb{C}^* = \mathbb{C} - \{0\}$

a) $(\mathbb{C}^*, \cdot)$ is an abelian group

leave details to notes

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

is a subgroup of $(\mathbb{C}^*, \cdot)$ and is the unit circle

Pf. To check S^1 is a subgroup
 of $a, b \in S^1$ then $ab^{-1} \in S^1$

Know $|a| = |b| = 1$ WTS. $|ab^{-1}| = 1$

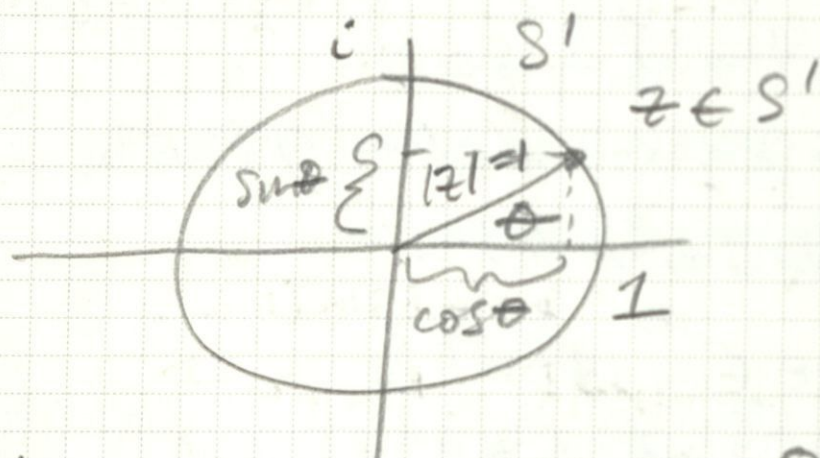
$$|ab^{-1}| = \left| \frac{a}{b} \right| = \frac{|a|}{|b|} = \frac{1}{1} = 1$$

note this would not have been true
 if the radius of the circle was 2

Theorem Every finite subgroup of
 $(\mathbb{C}^*, \cdot)$ is cyclic

§ 2 of today, Euler's Formula and
 de Moivre's theorem

Suppose $z \in S^1 \subset \mathbb{C}^*$



Then $z = \cos \theta + i \sin \theta$ $\theta \in [0, 2\pi)$

Theorem, Euler

$$e^{ix} = \cos x + i \sin x$$

$$\text{Pf. } e^x = 1 + x + \frac{x^2}{2!} + \frac{x^3}{3!} + \frac{x^4}{4!} + \dots$$

$$\cos x = 1 - \frac{x^2}{2!} + \frac{x^4}{4!} - \frac{x^6}{6!} \dots$$

note

$$\cos^{(k)}(x) : @ 0$$

$$\begin{pmatrix} \cos x & 1 \\ -\sin x & 0 \\ -\cos x & -1 \\ \sin x & 0 \\ \cos x & 1 \end{pmatrix}$$

$$\sin^{(k)}(x) : @ 0$$

$$\begin{pmatrix} \sin x & 0 \\ \cos x & 1 \\ -\sin x & 0 \\ -\cos x & -1 \\ \sin x & 0 \end{pmatrix}$$

$$\sin x = \frac{x}{1!} - \frac{x^3}{3!} + \frac{x^5}{5!} \dots$$

check

$$e^{ix} = 1 + (ix) + \frac{(ix)^2}{2!} + \frac{(ix)^3}{3!} + \frac{(ix)^4}{4!} + \dots$$

$$= \left[1 - \frac{x^2}{2!} + \frac{x^4}{4!} - \frac{x^6}{6!} \dots \right] + i \left[x - \frac{x^3}{3!} + \frac{x^5}{5!} \dots \right]$$

Theorem de Moivre

$$(e^{ix})^n = e^{inx}$$

$$(\cos x + i \sin x)^n = \cos(nx) + i \sin(nx)$$

More Generally. $z = re^{i\theta} = |z| \cdot e^{i\theta}$

$$\text{so } z^n = |z|^n e^{in\theta}$$

note. $\cos(3x) + i \sin(3x) = (\cos x + i \sin x)^3$

$$= \cos^3 x + 3i \cos^2 x \sin x - 3 \cos x \sin^2 x - i \sin^3 x$$

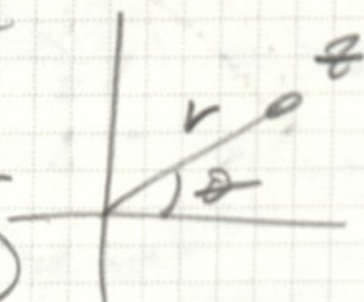
$$\text{so } \cos(3x) = \cos^3 x - 3 \cos x \sin^2 x$$

Last Time. $z = re^{i\theta} \in \mathbb{C}$

$$|z| = r$$

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

(using Taylor Series)



de Moivre. $(\cos\theta + i\sin\theta)^n$

$$= (e^{i\theta})^n = e^{in\theta} = \cos(n\theta) + i\sin(n\theta)$$

Def. $\mu_n = \{z \in \mathbb{C} \mid z^n = 1\}$ $n \geq 1$

$$\mu_1 = \{1\} \quad z^1 = 1$$

$$\mu_2 = \{-1, 1\} \quad z^2 = 1$$

$$\mu_3 = \{1, \omega, \omega^2\} \quad z^3 = 1$$

$$\mu_4 = \{1, i, -1, -i\} \quad z^4 = 1$$

$$(z^2)^2 = 1$$

$$z^2 = 1 \text{ or } z^2 = -1$$

$$* \quad z^3 - 1 = 0 \Rightarrow (z-1)(z^2 + z + 1) = 0$$

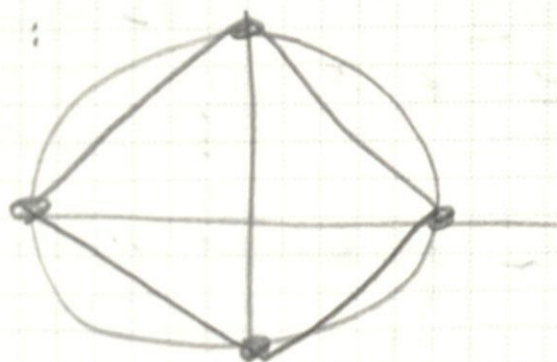
$$\Rightarrow z = 1, \frac{-1 \pm \sqrt{-3}}{2}$$

$$\text{so } \mu_3 = \left\{1, \frac{-1 \pm i\sqrt{3}}{2}\right\}$$

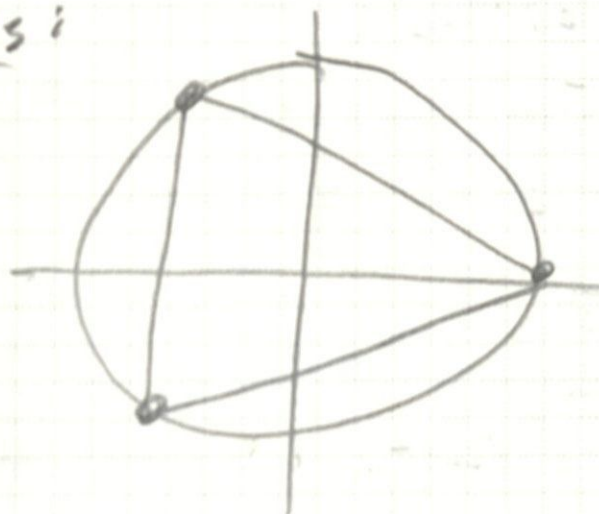
Theorem (a) μ_n is a subgroup of $(\mathbb{C}^+, \cdot)$

- cyclic of order n
- elements form vertices of a regular n -gon ($n \geq 3$)

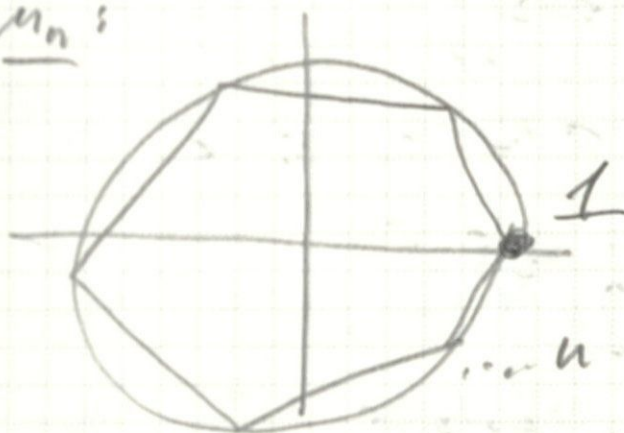
μ_4 :



μ_3 :



μ_n :



(b) These are the only finite subgroups of $\mathbb{C}^\times$

Pf. $a, b \in \mu_n$ check $ab^{-1} \in \mu_n$

$$a^n = 1 \quad b^n = 1 \quad \text{WTS } (ab^{-1})^n = a^n b^{-n} = 1/1 = 1$$

only works since $\mathbb{C}^\times$ is abelian!

Let's solve $z^n = 1$:

$$\Rightarrow |z^n| = 1 \Rightarrow |z|^n = 1$$

$\underbrace{\quad}_{\in (0, \infty)}$

$$\text{so } |z| = \sqrt[n]{1} = 1$$

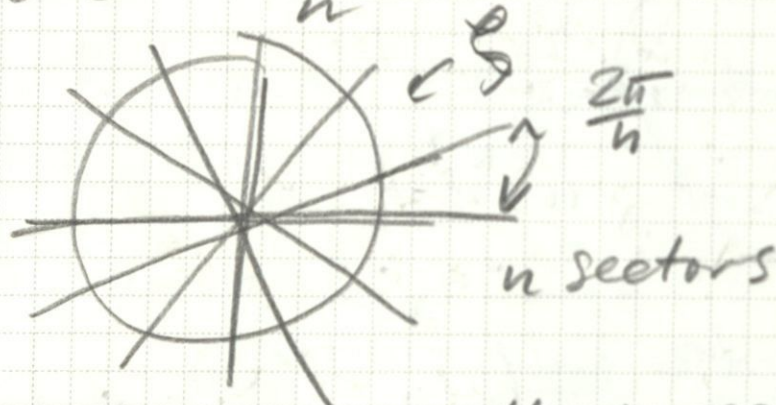
$$\Rightarrow \mu_n \subset S^1$$

so $z = e^{i\theta}$ is solving $z^n = 1$

$$\Rightarrow e^{in\theta} = 1 = \cos(n\theta) + i \sin(n\theta) = 1$$

$$\Rightarrow \begin{cases} \cos(n\theta) = 1 \\ \sin(n\theta) = 0 \end{cases} \Leftrightarrow \begin{cases} n\theta = 2\pi k \end{cases}$$

$$\text{so } \theta = \frac{2\pi k}{n} \text{ where } k \in \frac{2\pi}{n} \mathbb{Z}$$



$\Rightarrow \mu_n$ has exactly n points
vertices of a regular n -gon

Conclusion: $\mu_n = \{e^{i\theta} / \theta \in \frac{2\pi}{n}\mathbb{Z}\}$
 $= \{1, e^{\frac{2\pi i}{n}}, e^{\frac{2\pi \cdot 2i}{n}}, \dots, e^{\frac{2\pi \cdot (n-1)i}{n}}\}$

elements of μ_n are called the n^{th} roots of unity

note: $(e^{\frac{2\pi ki}{n}})^n = e^{2\pi i k} = 1$ identity

$$e^{2\pi i k} = \cos(2\pi k) + i \sin(2\pi k) \\ = 1 + i \cdot 0 = 1$$

To show μ_n is cyclic, find A generator:

$\zeta = e^{\frac{2\pi i}{n}} = \cos(\frac{2\pi}{n}) + i \sin(\frac{2\pi}{n})$
 (zeta)

$$\zeta^k = (e^{\frac{2\pi i}{n}})^k = e^{\frac{2\pi i k}{n}}$$

$$\text{so } \mu_n = \{1, \zeta, \zeta^2, \dots, \zeta^{n-1}\}$$

$$\zeta^n = 1$$

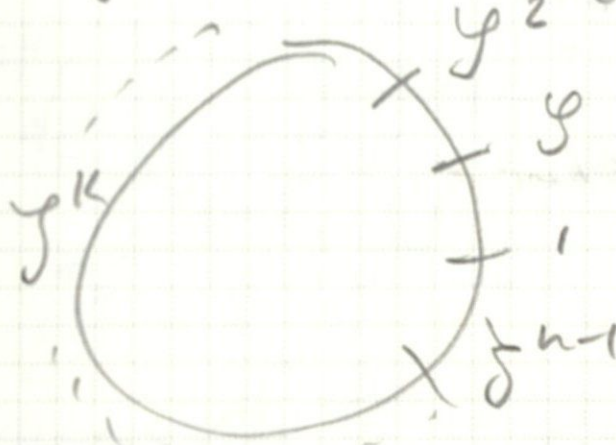
$$\text{ord}(\zeta) = n$$

$$\zeta^k \neq 1 \text{ if}$$

$$1 \leq k \leq n-1$$

$$\mu_n = \langle \zeta \rangle$$

cyclic.



(b) These are the only finite subgroups of $\mathbb{Q}^+$

Suppose G is a subgroup of $\mathbb{Q}^+$ of order n . G is abelian

From worksheet.

if G = abelian of order n

then $a^n = 1 \quad \forall a \in G$

$$\text{Pf. } G = \{x_1, \dots, x_n\} \quad \# \\ = \{ax_1, \dots, ax_n\} \quad \#$$

$$\prod_{i=1}^n x_i = \prod_{i=1}^n ax_i = a^n \prod_{i=1}^n x_i \\ 1 = a^n$$

$$\text{eg. } U_5 = \{1, 2, 3, 4\} \\ a = 2 \quad \{2 \cdot 1, 2 \cdot 2, 2 \cdot 3, 2 \cdot 4\} \\ = \{2, 4, 1, 3\}$$

* this works for any finite group

AND this works since G is abelian

$$\prod a x_i = a x_1 \odot x_2 \odot \dots \odot x_n = a^n \prod x_i$$

$$\text{So } \forall a \in G, a^n = 1$$

$$G \subset \mu_n \\ \text{order } n \quad \text{order } n$$

$$\text{So } G = \mu_n$$

Let's look at $\mu_n = \langle \zeta \rangle$
What other generators are there?

Suppose $\zeta^k \in \mu_n = \langle \zeta \rangle$

when is $\mu_n = \langle \zeta^k \rangle$?

$$\text{ord}(\zeta^k) = \text{ord}(\langle \zeta^k \rangle) \\ = \text{ord}(\mu_n) = n$$

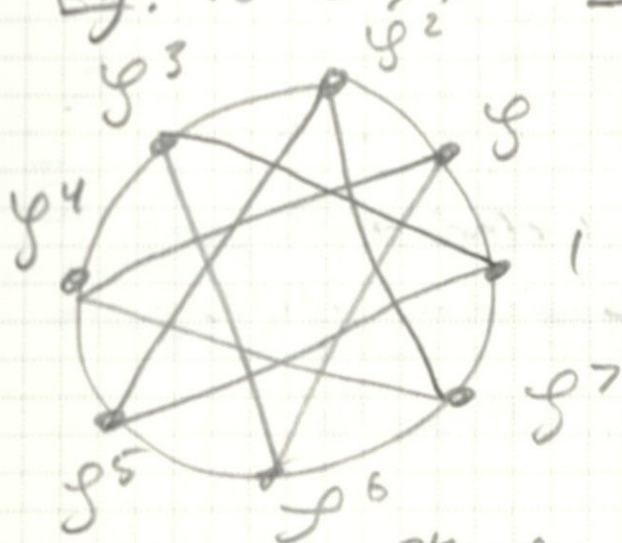
so ζ^k generator $\iff \text{ord}(\zeta^k) = n$
we know $\text{ord}(\zeta) = n$

$$\text{ord}(\zeta^k) = \frac{n}{(k, n)} = n$$

$$\iff (k, n) = 1 \iff k \in U_n$$

Conclusion There are exactly
 $\phi(n)$ generators of μ_n

Eg. $n=8$, $k=3$ generates



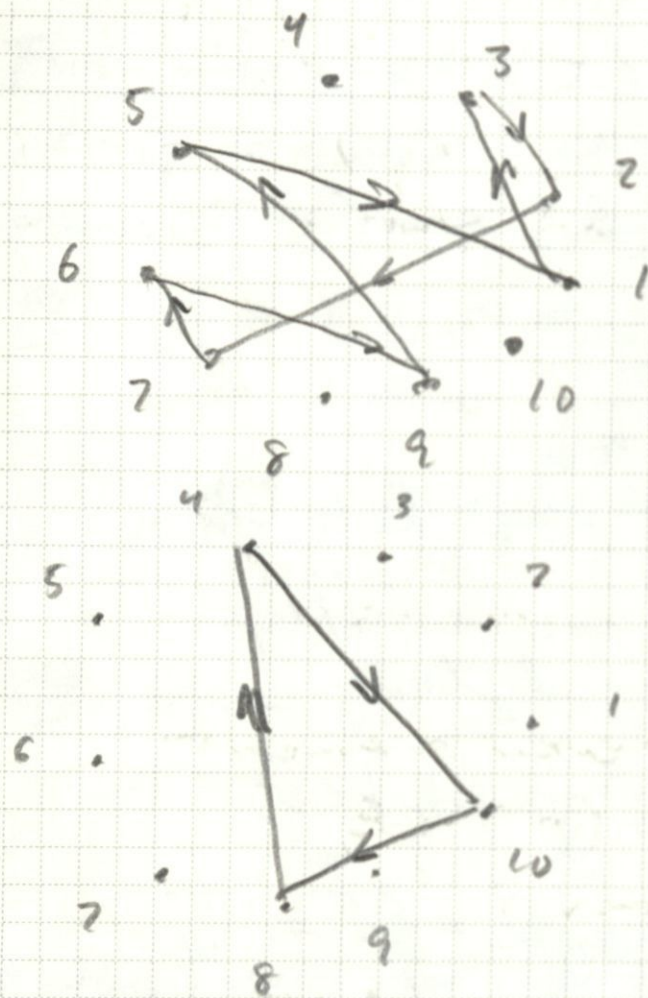
$$\text{angle} = \frac{2\pi}{8} = \frac{\pi}{4}$$

Generators ζ^k of μ_n $(k, n) = 1$
are called primitive n th roots of unity

Back to S_n

Graphical way to represent $\sigma \in S_n$

$$\sigma = \begin{pmatrix} 1 & 2 & 3 & 4 & 5 & 6 & 7 & 8 & 9 & 10 \\ 3 & 7 & 2 & 10 & 1 & 9 & 6 & 4 & 5 & 8 \end{pmatrix}$$



note. how these are all closed loops
these are called permutation cycles

we can decompose all σ into
such cycles

Lecture Notes:

3.19.25

Symmetric groups, cycles, and parity:

We saw a graphical representation of permutation by drawing the elements $1, 2, \dots, n$ as vertices of a regular n -gon, and putting arrows from i to $\sigma(i)$

Def. A k -cycle $(i_1, i_2, \dots, i_k)$ is a permutation in S_n such that:

$$\sigma(i_1) = i_2$$

$$\sigma(i_2) = i_3$$

$$\vdots$$
$$\sigma(i_{k-1}) = i_k$$

$$\sigma(i_k) = i_1$$

$$\sigma(j) = j \quad \forall j \neq i_1, \dots, i_k$$

Ex. A 1-cycle fixes every element

$$(1) = (2) = \dots = (n) = e$$

is identity permutation

Ex. A 2-cycle (i, j) is a transposition, interchanging i and j but leaving everything else in fact

Prop. if $\sigma = (i_1, \dots, i_k)$ and $\tau = (j_1, \dots, j_l)$ are disjoint, i.e. $\{i_1, \dots, i_k\}$ and $\{j_1, \dots, j_l\}$ are disjoint sets, then:

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

Which also means $(\sigma\tau)^n = \sigma^n\tau^n$

Proof. Check that $\sigma\tau(x) = \tau\sigma(x)$ for all x .

if $x = i_u$, then $\sigma\tau(x) = \tau\sigma(x) = i_{u+1}$

if $x = j_v$, then $\sigma\tau(x) = \tau\sigma(x) = j_{v+1}$

finally, if x is not i_u or j_v , then

$$\sigma\tau(x) = \tau\sigma(x) = x$$

Remark. This commutativity is no longer true if the cycles are NOT disjoint

Ex. $(1, 2)(1, 2) = e$

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

$$(1, 2)(2, 3)(3, 4) = (1, 2, 3, 4)$$

$$(i_1, i_2)(i_2, i_3) \dots (i_{k-1}, i_k)$$

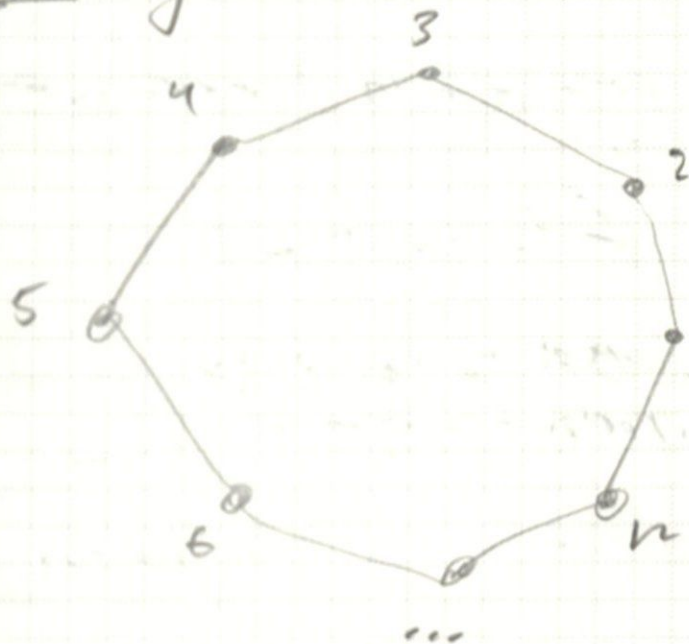
$$= (i_1, i_2, \dots, i_k)$$

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

Send x to $f(x)$

Theorem. Every $\sigma \in S_n$ can be represented as a product of disjoint cycles

Proof. geometric. take a regular n -gon



Corollary. Every $\sigma \in S_n$ is a product of not necessarily disjoint transpositions

Proof. σ is a product of cycles, and each cycle is a product of transpositions, as shown above

Theorem. A permutation $\sigma \in S_n$ can be written as a product of transpositions in many ways, but if

$$\sigma = t_1 t_2 \dots t_k = t_1' t_2' \dots t_l',$$

are two different products of transpositions, then $k \equiv l \pmod{2}$

Pf. see thm 5.15 in textbook

Def. σ is even/odd if it is a product of an even/odd number of transpositions

Lecture Notes.

3.21.25

Def. The sign of a permutation is

$\epsilon(\sigma) = 1$ if σ is even and $\epsilon(\sigma) = -1$ if σ is odd

The function $\epsilon: S_n \rightarrow \{-1, 1\}$ is the sign function

Ex. $\epsilon((a, b)) = -1$

$$\epsilon((a, b)(c, d)) = 1$$

$$\epsilon((a, b, c)) = \epsilon((a, b)(b, c)) = 1$$

$$\epsilon((i_1, i_2, \dots, i_k)) =$$

$$\epsilon((i_1, i_2) \dots (i_{k-1}, i_k)) = (-1)^{k-1}$$

Def. Let $A_n = \{\sigma \in S_n \mid \varepsilon(\sigma) = 1\}$ be the set of all even permutations. It is a very special subgroup of S_n , but need group homomorphisms to discuss further

Cosets and Lagrange:

We have encountered cosets before:

$$\int 2x dx = x^2 + C$$

$$\int \frac{1}{x} dx = \ln x + C$$

$$\begin{aligned}\int (2x + \frac{1}{x}) dx &= \int 2x dx + \int \frac{1}{x} dx \\ &= (x^2 + C) + (\ln x + C) \\ &= x^2 + \ln x + C\end{aligned}$$

Similarly,

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

$$\overline{1} = \{\dots, -n+1, 1, n+1, \dots\} = 1+n\mathbb{Z}$$

$$\overline{k} = k+n\mathbb{Z}$$

$$\begin{aligned}\overline{a} + \overline{b} &= (a+n\mathbb{Z}) + (b+n\mathbb{Z}) \\ &= (a+b) + n\mathbb{Z} \\ &= \overline{a+b}\end{aligned}$$

both $x^2 + C$ and $k+n\mathbb{Z}$ are cosets!

Def. Suppose G is a group and H is a subgroup. A left coset of H is a set of the form

$$Hg = \{ hg \mid h \in H \} \text{ for some } g \in G$$

Similarly, a right coset is of the form

$$gH = \{ gh \mid h \in H \} \text{ for some } g \in G$$

note. if G is abelian, $gh = hg$ so left and right cosets are the same thing

Moreover. if the group operation is $+$, then cosets are of the form $H + g$

Exs.

1. $G = \mathbb{Z}$, $H = n\mathbb{Z}$, $g = k$, then cosets are of the form $H + g = g + H = k + n\mathbb{Z}$, so the elements of $\mathbb{Z}_n$.

They are all translates of each other

2. $x^2 + C$ are all translates of the parabola up and down

3. $G = \mathbb{R}^2$ and $H = \mathbb{R}N_0$ for some nonzero vector N_0 . Given a vector $V \in G$ we have the coset $H + V$, which is a line passing through V and parallel to N_0 . All the cosets are these parallel lines

4. $G = S_3$, $H = A_3$. In this case we can list all the distinct elements

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

$$H = A_3 = \{1, (1, 2, 3), (1, 3, 2)\}$$

Each element of G gives a coset:

$g \in G$	The left coset of Hg
e	$\{1, (1, 2, 3), (1, 3, 2)\}$
$(1, 2)$	$\{(1, 2), (2, 3), (1, 3)\}$
$(2, 3)$	$\vdots$
$(1, 3)$	$\vdots$
$(1, 2, 3)$	$\{1, (1, 2, 3), (1, 3, 2)\}$
$(1, 3, 2)$	$\vdots$

Observations

1. Cosets have the same size
2. cosets are disjoint
3. Every element of G is in some coset

Cosets. $\int 2x dx = x^2 + C$

coset for constant functions

"class" of functions

G group, H subgroup

A left coset. $Hg = \{hg \mid h \in H\}$

note. this is a set - not a group

Ex. $G = S_3 = \{e, (12), (13), (23), (123), (132)\}$

$H = \{e, (12)\} = \langle (12) \rangle$

g	Hg
e	$\{e, (12)\}$
(12)	$\{(12), e\}$
(23)	$\{(23), (123)\}$
(13)	$\{(13), (132)\}$
(123)	$\{(123), (23)\}$
(132)	$\{(132), (13)\}$

note. $(12)(23) = (123)$

$(12)(13) = (21)(13) = (213) = (132)$

can only cycle them!
not associative!

Theorem. H subgroup of G , $g_1, g_2 \in G$

Either. $Hg_1 = Hg_2 \Leftrightarrow g_2 g_1^{-1} \in H$

OR $Hg_1 \cap Hg_2 = \emptyset \Leftrightarrow g_2 g_1^{-1} \notin H$

Eg. from last page

$$g_1 = (23), g_2 = (123)$$

$$g_2 g_1^{-1} = (123)(23)^{-1} = (123)(23) \\ = (12)(3) = (12) \in H$$

$$\text{so } H(23) = H(123)$$

$$\text{Eg. } g_1 = (23), g_2 = (13)$$

$$g_2 g_1^{-1} = (13)(23)^{-1} = (13)(23) \\ = (132) \notin H$$

$$H(23) \cap H(13) = \emptyset$$

Remark. For right cosets gH

$$g_1 H = g_2 H \Leftrightarrow g_1^{-1} g_2 \in H$$

$$g_1 H \cap g_2 H = \emptyset \Leftrightarrow g_1^{-1} g_2 \notin H$$

Proof. When is $Hg_1 \cap Hg_2 \neq \emptyset$?

there is an element $\underline{h_1 \cdot g_1}$ of Hg_1 , equal to an element $\underline{h_2 \cdot g_2}$ of Hg_2

$$\text{since } Hg_1 = \{hg_1 \mid h \in H\}$$

$$Hg_2 = \{hg_2 \mid h \in H\}$$

So $h_1 g_1 = h_2 g_2$ must be true

put h 's on the left and g 's on the right

$$h_1 g_1 g_1^{-1} = h_2 g_2 g_1^{-1}$$

$$h_2^{-1} h_1 = g_2 g_1^{-1} \in H$$

$$\text{because } h_1, h_2 \in H \Rightarrow h_2^{-1} \cdot h_1 \in H$$

note. for right cosets solve

$$g_1 h_1 = g_2 h_2$$

only works since H is a subgroup

so if $g_2 g_1^{-1} \notin H$ then $Hg_1 \cap Hg_2 = \emptyset$

What if $g_2 g_1^{-1} \in H \Rightarrow g_2 g_1^{-1} = h_0 \in H$

$$g_2 = h_0 g_1 \quad \Downarrow$$

$$Hg_2 = \{h g_2 \mid h \in H\}$$

$$= \{h h_0 g_1 \mid h \in H\}$$

$$= \{h g_1 \mid h \in H\} = Hg_1$$

since $h g_1 = \underbrace{h h_0^{-1} \cdot h_0}_{\in H} \cdot g_1$

Theorem. Suppose H, G are finite groups where $H \leq G$

(1) $|Hg| = |H|$

(2) $G = \text{disjoint union of cosets}$
 $= Hg_1 \cup Hg_2 \cup \dots \cup Hg_k$

note. $\cup = \text{union}$

$\sqcup = \text{disjoint union}$

(3) $k = [G : H] = \frac{|G|}{|H|}$
index of H in G

set of all cosets

Lagrange's. $|H| \mid |G|$

$\nearrow$

notation. $G/H = \{Hg_1, Hg_2, \dots, Hg_n\}$

$H = \{h_1, \dots, h_m\}$ size m

$Hg = \{h_1 \cdot g, \dots, h_m \cdot g\}$ size m

$g \in Hg$ since $e \in H$ so $e \cdot g \in Hg$

$G = \text{union of } Hg$
 $= \text{disjoint union}$

$$|G| = \sum |Hg_i| = \sum |H| = k|H|$$

Corollary. G any finite group of order n

(1) if $a \in G$ then $a^n = e$

(2) if $n = \text{prime}$ then G is cyclic

Pf. $\langle a \rangle \subset G$

Lagrange $|\langle a \rangle| \mid |G| = n$

$$\text{ord}(a) \mid n \Rightarrow a^n = e$$

if n is prime $\text{ord}(a) \mid n$

$$\Rightarrow \text{ord}(a) = n \quad (a \neq e)$$

$$\text{so } G = \langle a \rangle$$

Reminder. gH = left coset Hg = right cosetequal on disjoint $G = \sqcup$ left cosets $G = \sqcup$ right cosetsif G is finite: $|H| \mid |G|$ and $[G:H] = \frac{|G|}{|H|} = \#$ of distinct cosetsApplication. if $|G| = p$ a prime $\neq$
then G is cyclicEg. $G = S_3$, $|G| = 3! = 6$ What are the subgroups of G ? $H \subset G$ subgroup: $|H| \mid 6$ so $|H| \in \{1, 2, 3, 6\}$

$ H $	H
1	$\{e\}$
2	cyclic $\langle g \rangle$ $\text{ord}(g) = 2$
3	cyclic $\langle g \rangle$ $\text{ord}(g) = 3$
6	S_3

 $G = \{e, (12), (13), (23), (123), (132)\}$ * 2: $\langle (12) \rangle, \langle (13) \rangle, \langle (23) \rangle$ ** 3: $\langle (123) \rangle, \langle (132) \rangle$

all possible options

Remark. if $K \subset H \subset G$ subgroups

$$[G:K] = [G:H] \cdot [H:K]$$

$$\frac{|G|}{|K|} = \frac{|G|}{|H|} \cdot \frac{|H|}{|K|}$$

eg. $G = D_4 = \{e, r, r^2, r^3, s, rs, r^2s, r^3s\}$

$$H = \{e, r, r^2, r^3\} \supset K = \{e, r^2\}$$

$$[G:H] = 2 \quad \exists 2 \text{ left } H\text{-cosets in } G$$

$$[H:K] = 2 \quad \exists 2 \text{ left } K\text{-cosets in } H$$

$$[G:K] = 4 \quad \exists 4 \text{ left } K\text{-cosets in } G$$

G/H = collection of all left cosets

$$\# = [G:H]$$

Homomorphisms & Isomorphisms:

how to compare groups

Good, $(\mathbb{R}^+, \cdot) \subset (\mathbb{C}^+, \cdot)$

Bad, $(\mathbb{R}^+, \cdot) \subset (\mathbb{R}, +)$
incompatible

Def. Suppose H and G are groups

A homomorphism (hom) is a function
 $f: G \rightarrow H$ st $f(x \cdot y) = f(x) \cdot f(y)$
for all $x, y \in G$ in G in H

Examples.

(1) $f: G \rightarrow G$ $f = \text{id}$ f is a hom.

(2) if $H \subset G$ subgroup

$f: H \rightarrow G$ $f(x) = x$ (inclusion map)

then f is a hom.

$$f(x \cdot y) = f(x) \cdot f(y)$$

$$\underset{H}{x} \cdot \underset{H}{y} = \underset{G}{x} \cdot \underset{G}{y} \text{ by def of subgroup}$$

$$(3) f: \mathbb{R}^+ \rightarrow \mathbb{R}^+ \quad f(x) = x^2$$

$$(x \cdot y)^2 = x^2 \cdot y^2 \text{ is a group hom } \checkmark$$

$$(4) f: (\mathbb{R}^+, \cdot) \rightarrow (\mathbb{R}, +) \quad f(x) = x$$

is Not a hom.

$$f(x \cdot y) \stackrel{G}{=} f(x) \stackrel{+}{+} f(y)$$

$$xy \neq x + y \text{ not true } \forall x, y$$

$$(5) |x|: (\mathbb{R}, +) \rightarrow (\mathbb{R}, +) \text{ is not a group hom}$$

$$|x + y| \neq |x| + |y| \text{ for all } x, y$$

$$(6) f: (\mathbb{R}, +) \rightarrow (\mathbb{R}^+, \cdot)$$

$$f(x) = e^x \text{ is a hom}$$

$$f(x + y) \stackrel{G}{=} f(x) \stackrel{+}{+} f(y)$$

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

$$e^{x+y} = e^x e^y \text{ yes } \checkmark$$

$$(7) f: GL_n(\mathbb{R}) \rightarrow (\mathbb{R}^+, \cdot)$$

$$f(x) = \det x \text{ is a hom}$$

$$\det(xy) = \det(x) \det(y)$$

Composing Groups:

Hom $f: G \rightarrow H$ st $f(xy) = f(x) \cdot f(y)$
 $\quad \quad \quad G \quad \quad \quad H$

Ex: $f: (\mathbb{R}, +) \rightarrow (GL_2(\mathbb{R}), \cdot)$

$$f(x) = \begin{pmatrix} 1 & x \\ 0 & 1 \end{pmatrix}$$

matrix multiplication

WTS $f(x+y) = f(x) \cdot f(y)$

$$\begin{pmatrix} 1 & x+y \\ 0 & 1 \end{pmatrix} = \begin{pmatrix} 1 & x \\ 0 & 1 \end{pmatrix} \begin{pmatrix} 1 & y \\ 0 & 1 \end{pmatrix}$$

* on the midterm!

Ex. $\forall G, H$ groups there is a hom $G \rightarrow H$

$$f: G \rightarrow H \text{ st } f(xy) = f(x)f(y)$$

the map $f(x) = e_H \quad \forall x \in G$ since
 $e_H = e_H \cdot e_H$ ✓ trivial hom

Prop. For any hom $f: G \rightarrow H$

$$f(e_G) = e_H$$

$$\text{Pf: } e_G = e_G \cdot e_G$$

$$f(e_G) = f(e_G \cdot e_G) = f(e_G) \cdot f(e_G)$$

$$\text{so } f(e_G) = e_H$$

$$u \in H$$

$$\begin{aligned} u &= u \cdot u \\ uu^{-1} &= uuu^{-1} \\ e_H &= u \end{aligned}$$

Prop. Suppose $f: G \rightarrow H$ is a hom
If f is bijective then $f^{-1}: H \rightarrow G$
is also a hom

In this case say f is an isomorphism

$$\mathbb{Z} = \{ \dots, 0, 1, 2, 3, \dots \} \xrightarrow{f} \{ \dots, -1, 1, 1, 1, \dots \}$$

f is an isomorphism

$G \cong H$ G is isomorphic to H

Pf. WTS $f^{-1}(x \cdot y) = f^{-1}(x) \cdot f^{-1}(y)$
 $f^{-1}: H \rightarrow G$

Because f is injective, to verify

$$A = B \iff f(A) = f(B)$$

$$\text{WTS } f(f^{-1}(x \cdot y)) = f(f^{-1}(x) \cdot f^{-1}(y))$$

$$\implies xy = f(f^{-1}(x)) \cdot f(f^{-1}(y))$$

$$\implies xy = xy \quad \text{since } f \text{ is a hom}$$

Elaborate Ex: Chinese Remainder Theorem

Setup. Suppose G, H two groups

Def. Product group

$$G \times H = \{ (g, h) \mid g \in G, h \in H \}$$

$$(g, h) \bullet (g', h') = (gg', hh') \in G \times H$$

Prop. $G \times H$ is also a group

Pf. unit (e_G, e_H)

$$(g, h)^{-1} = (g^{-1}, h^{-1})$$

Ex. $\mathbb{R}^2 = \mathbb{R} \times \mathbb{R}$ gives vectors

Remark. $(x, y) \mapsto (x, 0)$

projection is a linear map of rank 1
rank = dimension of the image

Ex. G, H are 2 groups

$$f: G \times H \rightarrow G \text{ st } f(g, h) = g$$

projection

this is a group hom. It is surjective
but not injective (unless $H = \{e_H\}$)

Pf. Check $f(xy) = f(x)f(y)$

$$f((g, h)(g', h')) = f((g, h))f((g', h'))$$

$$f(gg', hh') = gg' = g \cdot g'$$

Theorem (CRT). $G = \mathbb{Z}_m, H = \mathbb{Z}_n$
st $(m, n) = 1$

$$\text{Then } \mathbb{Z}_m \times \mathbb{Z}_n \cong \mathbb{Z}_{m \cdot n}$$

Ex. $\mathbb{Z}_2 \times \mathbb{Z}_3 \cong \mathbb{Z}_6$

But $\mathbb{Z}_2 \times \mathbb{Z}_2 \not\cong \mathbb{Z}_4$

Lecture Notes:

3.31.25

$f: G \rightarrow H$ homs & isoms $G \cong H$ or $G \simeq H$
means $\exists$ some isom $G \cong H$
 $G \times H$ is a group

Theorem. if $(m, n) = 1$ then $\mathbb{Z}_m \times \mathbb{Z}_n \cong \mathbb{Z}_{mn}$

Pf. To show $G \cong H$ we must produce
 $f: G \rightarrow H$ which is an isom

Def. $f: \mathbb{Z}_{mn} \rightarrow \mathbb{Z}_m \times \mathbb{Z}_n$

$$f(x \bmod mn) = (x \bmod m, x \bmod n)$$

$$\mathbb{Z}_6 \rightarrow \mathbb{Z}_2 \times \mathbb{Z}_3 = \{0, 1\} \times \{0, 1, 2\}$$

$$0 \quad (0, 0)$$

$$1 \quad (1, 1)$$

$$2 \quad (0, 2)$$

$$3 \quad (1, 0)$$

$$4 \quad (0, 1)$$

$$5 \quad (1, 2)$$

every possible
pair ✓

Why does this make sense?

Here is a function that does not make sense:

$$h: \mathbb{Z}_5 \rightarrow \{-1, 1\} \quad h(x) = (-1)^x$$

$$\text{in } \mathbb{Z}_5, 0 \equiv 5 \quad h(0) = (-1)^0 = 1 \quad +$$

$$h(-1) \equiv -1$$

For our function, change by mn but
 $mn \equiv 0 \pmod{m}$
 $\equiv 0 \pmod{n}$

f is a hom. $f(x+y) = f(x) + f(y)$

$$f(x+y \bmod mn) = (x+y \bmod m, x+y \bmod n)$$

$$f(x) + f(y) = (\underbrace{x \bmod m}, \underbrace{x \bmod n}) + (\underbrace{y \bmod m}, \underbrace{y \bmod n})$$

pairwise addition $\nearrow$

To check f is bijective, need $(m, n) = 1$

f inj. Suppose $f(x) = f(y)$

$$(\underbrace{x \bmod m}, \underbrace{x \bmod n}) = (\underbrace{y \bmod m}, \underbrace{y \bmod n})$$

$$x \equiv y \pmod{m} \Rightarrow m \mid x - y$$

$$x \equiv y \pmod{n} \Rightarrow n \mid x - y$$

so $mn \mid x - y$ because $[m, n] = m \cdot n$

$$\text{as } (m, n) = 1 \quad ([m, n] = \frac{mn}{(m, n)})$$

$$\text{so } x \equiv y \pmod{mn}$$

$$\text{so } x = y \text{ in } \mathbb{Z}_{mn}$$

f surj. $\forall (a, b) \in \mathbb{Z}_m \times \mathbb{Z}_n$

seek $x \in \mathbb{Z}_{mn}$ st $f(x) = (a, b)$

$$\text{ie. } \begin{cases} x \equiv a \pmod{m} \\ x \equiv b \pmod{n} \end{cases}$$

$$\text{eg. } \mathbb{Z}_{15} \rightarrow \mathbb{Z}_3 \times \mathbb{Z}_5$$

$$f(x) = (2, 1)$$

$$2 \bmod 3 : 2, 5, 8, \textcircled{11}, 14$$

$$1 \bmod 5 : 1, 6, \textcircled{11}$$

$$f(11) = (2, 1)$$

$$\begin{cases} x \equiv a \pmod{m} \\ x \equiv b \pmod{n} \end{cases}$$

$$(m, n) = 1$$

$$\text{Bezout: } m\mathbb{Z} + n\mathbb{Z} = \mathbb{Z}$$

$$mu + nv = 1 \text{ for some } u, v$$

$$a \neq b$$

$$\text{Claim: } f(mu + nv) = (a, b)$$

$$\text{Check: } \underbrace{mu + nv}_{\equiv 0} \equiv a \pmod{m}$$

$$\equiv nva \pmod{m}$$

$$mu + nv = 1 \text{ so } nv \equiv 1 \pmod{m}$$

$$\equiv 1 \cdot a \pmod{m}$$

We don't want to keep doing all this.

$$\text{Lin Alg: } T: V \rightarrow W$$

$$T \text{ is injective} \iff \ker T = 0$$

$$T \text{ is surjective} \iff \text{Im } T = W$$

vector space

$$f: G \rightarrow H \text{ hom}$$

$$\ker f = \{ x \in G \text{ st } f(x) = e_H \} \text{ subgroup of } G$$

normal

$$\text{Im } f \text{ subgroup of } H$$

Lecture Notes

4.2.25

$f: G \rightarrow H$ group hom

Def. $\ker f = \{x \in G \mid f(x) = e_H\}$

eg. $T: V \rightarrow W$

$$\ker T = \text{Null } T = \{v \text{ st } T(v) = 0\}$$

Theorems

- (1) $\ker f$ subgroup of G
- (2) $\text{Im } f$ subgroup of H
- (3) f is injective $\Leftrightarrow \ker f = \{e_G\}$

Ex.

(1) $f: \mathbb{C}^\times \rightarrow \mathbb{C}^\times$ $f(x) = x^n$ hom

$$\ker f = \{x \mid x^n = 1\} = \mu_n$$

(n^{th} roots of unity)

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

$$\ker \det = \{X \in GL_n(\mathbb{R}) \mid \det X = 1\}$$

$\cong SL_n(\mathbb{R})$ subgroup of $GL_n(\mathbb{R})$

(3) $\varepsilon: S_n \rightarrow \{1, -1\}$

claim. ε is a group hom

$$\varepsilon(\sigma\tau) = \varepsilon(\sigma)\varepsilon(\tau) \quad \forall \sigma, \tau \in S_n$$

$$\sigma = t_1 \dots t_k \quad t_i \text{ transposition}$$

$$\tau = s_1 \dots s_\ell \quad s_i \text{ transposition}$$

$$\epsilon(\sigma) = (-1)^k, \epsilon(\tau) = (-1)^\ell \Rightarrow \epsilon(\sigma\tau) = \epsilon(\sigma)\epsilon(\tau)$$

$$\sigma\tau = t_1 \dots t_k s_1 \dots s_\ell = (-1)^{k+\ell}$$

$$\ker \epsilon = \{ \sigma \in S_n \mid \epsilon(\sigma) = 1 \} = A_n$$

subgroup of S_n

Pf.

(1) $x, y \in \ker f$ then $xy^{-1} \in \ker f$
 $f(x) = f(y) = e_H$

Aside. $f(g^{-1}) = f(g)^{-1}$
 $f(g \cdot g^{-1}) = f(e) = e$
 $f(g)f(g^{-1}) = e$
 $f(g^{-1}) = f(g)^{-1}$

$$f(xy^{-1}) = f(x)f(y^{-1}) = ee^{-1} = e$$

(2) $x, y \in \text{Im } f$ $xy^{-1} \in \text{Im } f$
 $x = f(a) \quad xy^{-1} = f(a)f(b)^{-1}$
 $y = f(b) \quad = f(a \cdot b^{-1}) \in \text{Im } f$

since G group $a, b \in G$
 $\Rightarrow ab^{-1} \in G$

Eg. G abelian. $f: G \rightarrow G$

$f(x) = x^k$ group hom

$\text{Im } f = \{x^k \mid x \in G\}$ subgroup

(3) if $\ker f \ni a \neq e$ $f(a) = f(e) = e$
not injective

if $\ker f = \{e\}$ show f is injective

$f(a) = f(b)$ wts $a = b$

$$f(a)f(b)^{-1} = e$$

$$f(ab^{-1}) = e$$

$$\text{so } ab^{-1} \in \ker f = \{e\}$$

$$ab^{-1} = e \Rightarrow a = b$$

eg. CRT. $f(x) = (x \bmod m, x \bmod n)$

$$\ker f = \{x \bmod mn \mid \begin{matrix} x \equiv 0 \pmod{m} \\ x \equiv 0 \pmod{n} \end{matrix} \}$$

$$= \{x \mid x \equiv 0 \pmod{[m, n]}\}$$

if $(m, n) = 1$, $\ker f = \{0\}$

eg. $f: \mathbb{Z}_{24} \rightarrow \mathbb{Z}_4 \times \mathbb{Z}_6$

$$f(x) = (x \bmod 4, x \bmod 6)$$

$$\ker f = \{x \bmod 24 \mid x \equiv 0 \bmod 12\}$$

$$= \{0, 12\}$$

not injective

Def. A subgroup N of G is normal if
 (a) every left coset of N is also
 a right coset

$\iff$

$$(b) gN = Ng \quad \forall g \in G \iff gNg^{-1} = N$$

(eg) $\{e, s\}$ is not normal in D_4

but $\{e, r, r^2, r^3\}$ is normal in D_4

$$N = \{e, r, r^2, r^3\} \text{ in } G = D_4$$

$$[G : N] = \frac{8}{4} = 2 \quad 2 \text{ cosets}$$

$$N, sN \quad \text{where } sN = Ns$$

$$sN = \{s, sr, sr^2, sr^3\}$$

$$Ns = \{s, rs, r^2s, r^3s\}$$

$$sr = r^3s$$

$$N = rN = r^2N = r^3N$$

$$sr^3 = rs$$

$$sN = rsN = r^2sN = r^3sN$$

$$sr^2 = r^2s$$

$$s = s$$

Check. $gNg^{-1} = N \quad \forall g \in N$

same set

$$g = r^i \quad r^i N r^{-i} = \{r^i x r^{-i} \mid x \in N\} \\ = \{r^i r^j r^{-i}\} = \{r^j\}$$

$$g = r^i s \quad r^i s N (r^i s)^{-1} = r^i s N s r^{-i} \\ = \{r^i s r^j s r^{-i}\} = \{r^i r^j r^{-i}\} = \{r^j\}$$

Theorem. $\ker f$ is always a normal subgroup of G

Pf. $g \ker f g^{-1} = \ker f$

$g x g^{-1}$ where $x \in \ker f$

know $f(x) = e$ want $f(g x g^{-1}) = e$

$\underbrace{f(g)}_e f(x) \underbrace{f(g^{-1})}_e = e$ yes

Lecture Notes

4.7.24

Recall. $H \subset G$ is a normal subgroup

if (a) every left coset is a right coset

$$gH = Hg$$

(b) $gHg^{-1} = H \quad \forall g \in G$

Lemma. if $gHg^{-1} \subset H \quad \forall g \in G$

$$\Leftrightarrow ghg^{-1} \in H \quad \forall h \in H \quad g \in G$$

then H is normal in G

Pf. Apply A to g & g^{-1}

for g : $gHg^{-1} \subset H \subset gHg^{-1}$

for g^{-1} : $g^{-1}Hg \subset H$

$Hg \subset gH$

$H \subset gHg^{-1}$

Exam 2 Review:

4.3.25

Def. $S_n = \{ \text{all permutations} \}$

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

$(S_n, \text{composition of functions}) = \text{group of order } n!$

note. $\sigma \circ \tau = \sigma \circ \tau = \sigma(\tau(i)) \forall i$

$$\sigma = (\sigma(1) \sigma(2) \dots \sigma(n))$$

note. f is bijective $\iff f^{-1}$ exists

Def. $\langle \sigma \rangle = \{ e, \sigma, \sigma^2, \dots, \sigma^{N-1} \}$ where $\sigma^N = e$

Def. $\langle g \rangle = \{ g^x \mid x \in \mathbb{Z} \} \subset G$

Def. G is a group. $g \in G$

$$H_g = \{ n \mid g^n = e \} = N\mathbb{Z} \subset \mathbb{Z}$$

$$\textcircled{1} \quad \{ 0 \} \text{ i.e. } g^0 = e \text{ \& no other } g^n = e$$

$$\textcircled{2} \quad N\mathbb{Z} \text{ i.e. } N > 0 \text{ and smallest possible entry in } H_g$$

Corollary. if case $\textcircled{2}$:

$$g^m = e \iff N \mid m$$

$$g^x = g^y \iff x \equiv y \pmod{N}$$

Def. if case $\textcircled{1}$ $\text{ord}(g) = \infty$
if case $\textcircled{2}$ $\text{ord}(g) = N$

Theorem. if $g \in G$ then $\langle g \rangle$ has order $\text{ord}(g)$

Theorem. Every subgroup of a cyclic group is cyclic, and we can relate their orders

Observation. $\langle g \rangle \leq G$ if $(g, |G|) = 1$

note. $\phi(n) = |\mathcal{U}_n|$

Prop. G group w/ $g \in G$

if $\text{ord}(g) = \infty$ then $\text{ord}(g^m) = \infty$ if $m \neq 0$

if $\text{ord}(g) = N$ then $\text{ord}(g^m) = \frac{N}{(m, N)}$

Corollary. Suppose $\text{ord}(g) = N$, $G = \langle g \rangle$
every element of G has order $|N|$
and if $n | N$ there are $\phi(n)$ elements
of order n

Consequence. if G = abelian group of
order N , then $a^N = e \quad \forall a \in G$ and
 $\text{ord}(a) | N$

Euler's Theorem. $\forall a \in \mathcal{U}_n, a^{\phi(n)} \equiv 1 \pmod{n}$

Fermat's Little Theorem.

if $a \not\equiv 0 \pmod{p}$ then $a^{p-1} \equiv 1 \pmod{p}$

Def. $\mathbb{C} = \{z = a + bi \mid a, b \in \mathbb{R}\}$

$|z|$ = dist to origin = $\sqrt{a^2 + b^2}$

$\text{Re } z = a$ real part

$\text{Im } z = b$ imaginary part

$\arg z = \theta$

$\bar{z} = a - bi$

note. complex numbers are both numbers
and vectors

Theorem. $(\mathbb{C}^*, \cdot)$ is an abelian group

$S^1 = \{z \in \mathbb{C}^* \mid |z| = 1\}$ is a subgroup
of $(\mathbb{C}^*, \cdot)$ and is the unit circle

Theorem. Every finite subgroup of $(\mathbb{C}^*, \cdot)$ is cyclic

Euler's Theorem: $e^{ix} = \cos x + i \sin x$

de Moivre's Theorem: $(e^{ix})^n = e^{inx}$

Def. $\mu_n = \{z \in \mathbb{C} \mid z^n = 1\}$ $n \geq 1$

Theorem. μ_n is a subgroup of $(\mathbb{C}^*, \cdot)$
cyclic of order n
elements form vertices of a regular n -gon
($n \geq 3$)

Theorem. These are the only finite
subgroups of $(\mathbb{C}^*, \cdot)$

Def. $\mu_n = \{e^{i\theta} \mid \theta \in \frac{2\pi}{n}\mathbb{Z}\}$ and
are called the n^{th} roots of unity

$\mu_n = \langle \zeta \rangle$ where $\zeta = e^{\frac{2\pi i}{n}}$

Remark. There are $\phi(n)$ generators of μ_n

Def. generators ζ^k of μ_n ($k, n = 1$)
are called primitive n^{th} roots of unity

Def. A k -cycle is a permutation in S_n st:

$$\sigma(i_1) = i_2$$

$$\sigma(i_2) = i_3$$

$\vdots$

$$\sigma(i_{k-1}) = i_k$$

$$\sigma(i_k) = i_1$$

$$\sigma(j) = j \quad \forall j \neq i_1, \dots, i_k$$

note.

A 1-cycle fixes every element

$$(1) = (2) = \dots = (n) = e$$

A 2-cycle (i, j) is a transposition, interchanging i and j but leaving everything else intact

Prop. if $\sigma = (i_1, \dots, i_k)$ and $\tau = (j_1, \dots, j_l)$ are disjoint:

$$\sigma\tau = \tau\sigma \iff (\sigma\tau)^n = \sigma^n\tau^n$$

Corollary Every $\sigma \in S_n$ is a product of transpositions. $\forall \alpha \in \sigma$,

$$(a_1 a_2 \dots a_k) = (a_1 a_k)(a_1 a_{k-1}) \dots (a_1 a_2)$$

Def. σ is even/odd if it is a product of even/odd number of transpositions

$$\epsilon: S_n \rightarrow \{-1, 1\}$$

$$\text{Def. } A_n = \{ \sigma \in S_n \mid \epsilon(\sigma) = 1 \}$$

Def. G group H subgroup

left coset: $Hg = \{hg \mid h \in H\}$ for some $g \in G$

right coset: $gH = \{gh \mid h \in H\}$ for some $g \in G$

note. if G abelian, $gh = hg$ so cosets the same

Theorem H subgroup of G , $g_1, g_2 \in G$

$$\textcircled{1} Hg_1 = Hg_2 \iff g_2 g_1^{-1} \in H$$

$$\textcircled{2} Hg_1 \cap Hg_2 = \emptyset \iff g_2 g_1^{-1} \notin H$$

note. for right cosets opposite is true

Theorem. H, G finite groups $H \subset G$

$$1) |Hg| = |H|$$

$$2) G = Hg_1 \cup Hg_2 \cup \dots \cup Hg_k$$

$$3) k = [G:H] = \frac{|G|}{|H|}$$

Lagrange's Theorem. $|H| \mid |G|$

Notation: $G/H = \{Hg_1, Hg_2, \dots, Hg_n\}$
set of all cosets

Application. if $|G| = p$ then G is cyclic

Def. A homomorphism is a function
 $f: G \rightarrow H$ st $f(x \cdot y) = f(x) \cdot f(y)$
 $\forall x, y \in G$ $\in G$ $\in H$

Prop. For any hom $f: G \rightarrow H$
 $f(e_G) = e_H$

note. $\forall G, H$ groups $\exists$ hom f
 $f(x) = e_H \quad \forall x \in G$

Def Suppose $f: G \rightarrow H$ is a hom
if f is bijective then $f^{-1}: H \rightarrow G$
is also a hom and f is an isomorphism
 $G \cong H$

Recall. f inj: $f(a) = f(b) \Rightarrow a = b$
 f surj: $\forall x \in G \exists f(x) \in H$

Theorem. Chinese Remainder Theorem

$G = \mathbb{Z}_m, H = \mathbb{Z}_n$ st $(m, n) = 1$

then $\mathbb{Z}_m \times \mathbb{Z}_n \cong \mathbb{Z}_{m \cdot n}$

$$\text{Ex. } G = S_4, H = \{e, (12)(34), (13)(24), (14)(23)\}$$

Claim. H is normal in G

How? $\forall \sigma \in S_4 \quad \forall h \in H, \sigma h \sigma^{-1} \in H$

$$\text{eg } \sigma = (231)$$

$$h = e, \sigma h \sigma^{-1} = \sigma e \sigma^{-1} = e$$

$$h = (12)(34): (231)(12)(34)(132) \\ = (14)(23) \in H$$

$$h = (13)(24): (231)(13)(24)(132) \\ = (12)(34) \in H$$

and so on ... 96 computations ...
 $|S_4| = |H|$

Better way. use lemma:

$$\sigma(i_1, \dots, i_k) \sigma^{-1} = (\sigma(i_1), \sigma(i_2), \dots, \sigma(i_k))$$

Remark. $\sigma c_1 \cdot c_2 \cdot \dots \cdot c_r \sigma^{-1}$ (c = cycle)

$$= \sigma c_1 \sigma^{-1} \sigma c_2 \sigma^{-1} \sigma c_3 \sigma^{-1} \dots \sigma c_r \sigma^{-1}$$

$$\sigma = (231):$$

$$\sigma(12)(34) \sigma^{-1} = \sigma(12) \sigma^{-1} \sigma(34) \sigma^{-1} \\ = (23)(14)$$

$$\sigma = (1324) : \sigma(12)(34)\sigma^{-1} = (34)(21)$$

still 96 computations but much quicker

We proved. if $G \rightarrow H$ is a group hom

$\ker f$ normal in G

$\text{Im } f$ subgroup in H

eg.

$$(1) \text{SL}_n(\mathbb{R}) = \ker \det$$

normal in $\text{GL}_n(\mathbb{R})$

$$(2) A_n = \ker \varepsilon : S_n \rightarrow \{\pm 1\}$$

A_n is normal in S_n

$$(3) n\mathbb{Z} \text{ is normal in } \mathbb{Z}$$

note. normal means $gHg^{-1} = H$

automatic if G is abelian

$$\text{prove (3): } g + n\mathbb{Z} - g = n\mathbb{Z}$$

Claim. If N is normal in G then

G/N " G mod N " = collection
of all left cosets of N in G

becomes a group

$$G, N \rightsquigarrow G/N \text{ a new group}$$

ex. $G = \mathbb{Z}$, $N = n\mathbb{Z}$

$$G/N = \mathbb{Z}/n\mathbb{Z} = \text{the set of cosets}$$

a coset is of the form " gN "

$$\text{is } g + n\mathbb{Z} = \bar{g}$$

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

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

G/N tries to emulate $\mathbb{Z}_n$ for general groups

Def. $G/N = \{ \text{all cosets } gN \} \Rightarrow eN$

$$gN \cdot hN = ghN$$

operations

unit $\uparrow$

note. $\bar{2}$ in $\mathbb{Z}_n$

$$2 \text{ or } 2+n \text{ or } 2+2n \text{ or } \dots$$

$$2 + n\mathbb{Z}$$

note $\bar{a} + \bar{b} = \overline{a+b}$

$$(a+n\mathbb{Z}) + (b+n\mathbb{Z}) = a+b+n\mathbb{Z}$$

Prop. (1) this is well defined

$$(2) (gN)^{-1} = g^{-1}N$$

(3) this produces a group on G/N

Pf. (1) $gN \cdot hN = g \underbrace{h(h^{-1}Nh)}_e N$
 $= gh \cdot N \cdot N = ghN$

$$(2) gNg^{-1}N = gg^{-1}N = eN$$

Lecture Notes.

4.9.25

$N \trianglelefteq G$ normal subgroup ($N \trianglelefteq G$)

$N = \ker f$ always normal where
 $f: G \rightarrow H$ is a group hom

$G/N = \{ \text{set of cosets of } N \text{ in } G \}$
this is a group where $gN \cdot hN = ghN$

Ex. $n\mathbb{Z} \subset \mathbb{Z}, \mathbb{Z}/n\mathbb{Z} = \mathbb{Z}_n$

Ex $N = A_3, G = S_3$
 $= \ker \varepsilon: S_3 \rightarrow \{ -1, 1 \}$

$$G/N = S_3/A_3 = \{ eA_3, (12)A_3 \}$$

$$|G/N| = [G:N] = \frac{|G|}{|N|} = \frac{6}{3} = 2$$

note. $(12)A_3 = (13)A_3 = (23)A_3$

group $(12)A_3 \cdot (12)A_3 = eA_3$

Ex. $G = A_4$

$$N = \{e, (12)(34), (13)(24), (14)(23)\}$$

$$|G/N| = [G:N] = \frac{|G|}{|N|} = \frac{12}{4} = 3$$

$$G/N = \{eN, (123)N, (132)N\}$$
$$= \{eN, (123)N, ((123)N)^2\}$$

all groups with a prime # of elements are cyclic!

Proposition - $|G/N| < |G|$
simpler

Observation -

↳ In G/N every $n \in N$ becomes the identity

Recall. in $\mathbb{Z}_n$ we have $n \equiv 0 \pmod{n}$
remainder of 7^{100} when divide by 9
 $7^2 = 49 \equiv 4 \pmod{9}$

Prop. The map $\pi: G \rightarrow G/N$
where $\pi(g) = gN$

a) this is a group hom

b) $\ker \pi = N$

Pf.

group hom? $\pi(gh) = \pi(g)\pi(h) \forall g, h \in G$
 $ghN = gN \cdot hN$ true by def

$\ker \pi = N$?

$$\ker \pi = \{g \in G \mid \pi(g) = eN\}$$
$$gN = eN$$

recall. $g_1H = g_2H$

$$\Leftrightarrow g_1^{-1}g_2 \in H \Leftrightarrow g_2^{-1}g_1 \in H$$

$$\ker \pi = \{g \in G \mid e^{-1} \cdot g \in N\} = N$$
$$= \{g \in G \mid g \in N\} = N$$

Observation 2.

$$\pi: G \rightarrow G/N, \ker \pi = N, \operatorname{Im} \pi = G/N$$

Remark. $\operatorname{Im} \pi = G/\ker \pi$

This is the only thing that can happen

This is called the 1st Isomorphism Theorem

If $f: G \rightarrow H$ is a group hom

$$\operatorname{Im} f \cong G/\ker f$$

Ex. $T: V \rightarrow W$ lin map of VS

$$\operatorname{Im} T = V/\ker T$$

$$\dim \operatorname{Im} T = \dim V - \dim \ker T$$

Eg. $G = H = (\infty \text{ differentiable functions } / +)$
 $= C^\infty(\mathbb{R})$

$$D: C^\infty(\mathbb{R}) \rightarrow C^\infty(\mathbb{R})$$

$D(f) = f'$ is a group hom

$$(f+g)' = f' + g'$$

$$\text{Im } D = C^\infty(\mathbb{R})$$

since every $h = \frac{d}{dx} \left(\int_0^x h(t) dt \right)$

$$\text{Ker } D = \text{constant}$$

1st Isom Thm.

$$C^\infty(\mathbb{R}) / \text{const} \cong C^\infty(\mathbb{R})$$

$$\text{solving } D(f) = e^x$$

$$f = e^x + C \leftarrow$$

coset for constant
functions

$$f \in C^\infty(\mathbb{R}) / \text{constants}$$

1st Isom Thm.

$$f: G \rightarrow H \text{ st. } f(xy) = f(x)f(y) \quad \forall x, y$$

$$\text{then } G/\ker f \simeq \text{Im } f$$

quotient of G subgroup of H

$$\text{eg. } \pi: G \times H \rightarrow G \text{ st. } \pi(g, h) = g$$

$$\ker \pi = \{(e, h) \mid h \in H\} = \{e\} \times H \simeq H$$

$$G \times H / \{e\} \times H \simeq G \quad \text{1st isom}$$

$$\text{so } G \times H / H \simeq G \quad \leftarrow \text{generalizes this}$$

$$\text{note. } \simeq = \cong$$

Recall. in G/N everything in N becomes e
 $G \times H / H$ everything in H becomes e " $\{g, e\}$ "

$$\text{eg. } \det: GL_n(\mathbb{R}) \rightarrow \mathbb{R}^*$$

$$\text{st. } \det(xy) = \det(x)\det(y)$$

$$\det \begin{pmatrix} x & & \\ & 1 & \\ & & \ddots \end{pmatrix} = x, \quad \ker \det = SL_n(\mathbb{R})$$

$$\text{so } GL_n(\mathbb{R}) / SL_n(\mathbb{R}) \simeq \mathbb{R}^*$$

eg. $\varphi: S_n \rightarrow \{-1, 1\}$

$\ker \varphi = A_n \trianglelefteq S_n$

$S_n / A_n \cong \{-1, 1\}$

$S_n = A_n \cup (12)A_n$

$S_n / A_n = \{A_n, (12)A_n\}$
 $\cong \{1, -1\}$

note. if $[G:H]=2$,

$G = H \cup aH$ where $a \notin H$

eg $f: \left\{ \begin{pmatrix} x & y \\ 0 & 1 \end{pmatrix} \right\} \rightarrow \left\{ \begin{pmatrix} x & 0 \\ 0 & 1 \end{pmatrix} \right\}$

$f(gh) = f(g)f(h)$ group hom

st. $f\left(\begin{pmatrix} x & y \\ 0 & 1 \end{pmatrix}\right) = \begin{pmatrix} x & 0 \\ 0 & 1 \end{pmatrix}$

$\ker f = \left\{ \begin{pmatrix} 1 & y \\ 0 & 1 \end{pmatrix} \right\} \trianglelefteq \left\{ \begin{pmatrix} x & y \\ 0 & 1 \end{pmatrix} \right\}$

$\text{Im } f = \left\{ \begin{pmatrix} x & 0 \\ 0 & 1 \end{pmatrix} \right\} < \left\{ \begin{pmatrix} x & 0 \\ 0 & 1 \end{pmatrix} \right\}$

$\left\{ \begin{pmatrix} x & y \\ 0 & 1 \end{pmatrix} \right\} / \left\{ \begin{pmatrix} 1 & y \\ 0 & 1 \end{pmatrix} \right\} \cong \left\{ \begin{pmatrix} x & 0 \\ 0 & 1 \end{pmatrix} \right\}$

for contrast, $\left\{ \begin{pmatrix} x & y \\ 0 & z \end{pmatrix} \right\} \subset GL_2(\mathbb{R})$
not normal

$$\begin{pmatrix} 1 & 0 \\ 0 & 1 \end{pmatrix} \begin{pmatrix} x & y \\ 0 & z \end{pmatrix} \begin{pmatrix} 1 & 0 \\ 0 & 1 \end{pmatrix} = \begin{pmatrix} z & 0 \\ y & x \end{pmatrix} \notin \left\{ \begin{pmatrix} x & y \\ 0 & z \end{pmatrix} \right\}$$

$GL_2(\mathbb{R}) / \left\{ \begin{pmatrix} x & y \\ 0 & z \end{pmatrix} \right\}$ not a group
 $\hookrightarrow \mathbb{R} \cup \{\infty\}$

note, will have to check normality of groups

ex. $a=6, b=30, a|b$.

$$f: \mathbb{Z} \rightarrow a\mathbb{Z}/b\mathbb{Z} = 6\mathbb{Z}/30\mathbb{Z}$$

note, both $a\mathbb{Z}$ and $b\mathbb{Z}$ are groups and
 $a\mathbb{Z} \supset b\mathbb{Z}$ also true

$$f(x) = ax + b\mathbb{Z} = \underbrace{6x + 30\mathbb{Z}}_{\substack{\text{coset} \\ \in 6\mathbb{Z}}}$$

$$\text{recall: } G/H = \{gH\}$$

$$\begin{aligned} \text{Im } f &= 6\mathbb{Z}/30\mathbb{Z} = \{g + 30\mathbb{Z} \mid g \in 6\mathbb{Z}\} \\ &= \{6x + 30\mathbb{Z} \mid x \in \mathbb{Z}\} \end{aligned}$$

group hom. $f(x+y) = f(x) + f(y)$

$$6(x+y) + 30\mathbb{Z} = (6x + 30\mathbb{Z}) + (6y + 30\mathbb{Z})$$

$$\begin{aligned} \ker f &= \{x \in \mathbb{Z} \mid 6x + 30\mathbb{Z} = 0 + 30\mathbb{Z}\} \\ &= \left(\frac{b}{a}\right) \cdot \mathbb{Z} \iff 6x \in 30\mathbb{Z} \\ &\quad x \in 5\mathbb{Z} \end{aligned}$$

1st Iso.

$$\mathbb{Z}/5\mathbb{Z} \cong 6\mathbb{Z}/30\mathbb{Z}$$

more generally,

$$\mathbb{Z}/(\frac{b}{a})\mathbb{Z} \cong a\mathbb{Z}/b\mathbb{Z}$$

Remark. $\mathbb{Z}, \mathbb{Z}_n, \mathbb{R}, \mathbb{Q}, \mathbb{C}$ you
can $+$ & $\cdot$

Def. A ring is a collection

$$(R, +, \cdot, 0, 1)$$

R : set

$+$: addition on R , id unit 0

$\cdot$: multiplication on R id unit 1

In particular, used:

• distributive

• associative

Ex. $\mathbb{Z}, \mathbb{Z}_n, \mathbb{R}, \mathbb{Q}, \mathbb{C}$ are rings

$\mathbb{R}[x]$ = polynomials in x is a ring

$M_{n \times n}(\mathbb{R})$ is a ring $+, \cdot, 0_n, I_n$

Non Ex. V = vector space not a ring

$(1, 1) \cdot (1, 2)$ not a vector

in $\mathbb{R}^3$ $v_1 \cdot v_2$ $\checkmark$ ~~$\mathbb{R}^3$~~ still not a ring

A ring is a set $(R, +, -, 0, 1)$ which satisfies $(R, +, 0)$, abelian group note. 1 unit for $\cdot$, which is associative

$$x(y+z) = xy + xz$$

$$(x+y)z = xz + yz$$

Ex. $\mathbb{Z}, \mathbb{Q}, \mathbb{R}, \mathbb{C}, \mathbb{Z}[x],$

$\mathbb{C}[x, y, z],$

$$R(x) = \left\{ \frac{P(x)}{Q(x)} \mid P, Q \text{ polynomials in } \mathbb{R}[x] \right. \\ \left. (\text{rational function}) \right\}$$

$M_n(\mathbb{R})$ ring but not commutative

Def. A subring S of a ring R is a subset $S \subset R$ with $0, 1 \in S$ and $a+b, a \cdot b \in S \forall a, b \in S$

Eg. $\mathbb{Z} \subset \mathbb{Q} \subset \mathbb{R} \subset \mathbb{C}$ subring

$$\mathbb{Z}[x] \subset \mathbb{Q}[x] \subset \mathbb{R}[x] \subset \mathbb{C}[x]$$

Ex. $S = \left\{ \begin{pmatrix} a & b \\ -b & a \end{pmatrix} \in M_{2 \times 2}(\mathbb{R}) \right\}$

S is a subring of $M_{2 \times 2}(\mathbb{R})$.

Pf. $1 \in S$?

$R = M_{2 \times 2}(\mathbb{R}) \quad 1 = \begin{pmatrix} 1 & 0 \\ 0 & 1 \end{pmatrix} \in S?$

$$\begin{pmatrix} a & b \\ -b & a \end{pmatrix} - \begin{pmatrix} a' & b' \\ -b' & a' \end{pmatrix} = \begin{pmatrix} a-a' & b-b' \\ -(b-b') & a-a' \end{pmatrix} \in S$$

$$\begin{pmatrix} a & b \\ -b & a \end{pmatrix} \begin{pmatrix} c & d \\ -d & c \end{pmatrix} = \begin{pmatrix} ac-bd & ad+bc \\ -bc-ad & -bd+ac \end{pmatrix} \in S$$

Ex. $R = M_{2 \times 2}(\mathbb{C})$

$S = \left\{ \begin{pmatrix} a & b \\ -\bar{b} & \bar{a} \end{pmatrix} \right\}$ subring.

Remark. Rings capture number theory, algebraic geometry, analysis, etc

Ex. $\mathbb{Z}[\sqrt{3}] = \{m+n\sqrt{3} \mid m, n \in \mathbb{Z}\}$
subring of $\mathbb{R}$.

$1 \in S \quad 1 = 1 + 0 \cdot \sqrt{3} \quad \checkmark$

$a+b\sqrt{3} + c+d\sqrt{3} = (a+c) + (b+d)\sqrt{3} \quad \checkmark$

$(a+b\sqrt{3})(c+d\sqrt{3}) = (ac+3bd) + (ad+bc)\sqrt{3}$
subring

eg. $\mathbb{Z}[i]$ subring of $\mathbb{C}$
called Gaussian integers

Def of Subring. $S \subset R$ is a subring if

- $1 \in S$
- $(S, +)$ is a subgroup of R
- $a \cdot b \in S$ if $a, b \in S$

careful,

$$\mathbb{N} \subset \mathbb{Z}, 1 \in \mathbb{N}$$

$$a, b \in \mathbb{N} \Rightarrow a+b, a \cdot b \in \mathbb{N}$$

but $\mathbb{N}$ is not a subgroup of $\mathbb{Z}$

Non Ex. $R = \mathbb{R}$

$$S = \{ m + n\sqrt[3]{2} \mid m, n \in \mathbb{Z} \}$$

is this a subring of $\mathbb{R}$?

$$a) 1 = 1 + 0 \cdot \sqrt[3]{2} \in S$$

$$b) a + b\sqrt[3]{2} - (c + d\sqrt[3]{2})$$

$$= a - c + (b - d)\sqrt[3]{2} \in S$$

$$c) \sqrt[3]{2} \cdot \sqrt[3]{2} = \sqrt[3]{4} \neq m + n\sqrt[3]{2} \\ \notin S$$

not a subring!

Remark. Use of algebra/rings is NT

Def. α algebraic = root of some polynomial in $\mathbb{Z}[x]$

transcendental = not algebraic

eg. π, e, e^π are transcendental

α algebraic integer = root of some monic poly in $\mathbb{Z}[x]$

$\sqrt[3]{2}$ root of $x^3 - 2$ ✓

$\frac{1}{7}$ root of $7x - 1$ ✗

Lecture Notes.

4.16.25

Rings & Subrings:

Special Rings - integral domains, fields $\rightarrow$

Def. Suppose R is a ring. A divisor of 0 is an element $a \in R$ $a \neq 0$ st $a \cdot b = 0$ for some $b \neq 0$

Eg. $\mathbb{Z}$ no divisors of 0

Eg. $\mathbb{Z}_6$ $2 \neq 0 \pmod{6}$

$3 \neq 0 \pmod{6}$

but $2 \cdot 3 \equiv 0 \pmod{6}$

2 & 3 are divisors of 0

Ex. $R = M_{2 \times 2}(\mathbb{R})$, $a = \begin{pmatrix} 0 & 1 \\ 0 & 0 \end{pmatrix} \neq 0$
but $a^2 = 0$ so a is a divisor of 0

Groups. $ax = ay$
 $\Rightarrow x = y$
true because a^{-1} exists

Lemma. Cancellation

Suppose $ax = ay$ in some ring and
 a is NOT a zero divisor. $a \neq 0$
then $x = y$

Ex. in $\mathbb{Z}$ $5x = 5y$ w/o dividing
 $\Rightarrow x = y$ by 5!

Pf. $ax = ay$
 $\Rightarrow a(x - y) = 0$ and $a \neq 0$
 $\Rightarrow x - y = 0$ or else
 a would be a zero divisor

Def. A commutative ring R is an
integral domain if it has no
zero divisors

$$\text{i.e. } x \cdot y = 0 \Leftrightarrow x = 0 \text{ or } y = 0$$

Ex. $\mathbb{Z} \checkmark$ $\mathbb{R} \checkmark$ $\mathbb{Z}_3 \checkmark$ $\mathbb{Z}_{15} \times$
 $\mathbb{Q} \checkmark$ $\mathbb{C} \checkmark$ $\mathbb{Z}_8 \times$ $\mathbb{Z}_{29} \checkmark$

Lemma. $\mathbb{Z}_n$ ($n \geq 2$) is an integral domain $\iff n$ is prime

Pf. if $n = a \cdot b$ $a, b \neq 1$, n

$$a, b \not\equiv 0 \pmod{n}$$

$$a \cdot b \equiv 0 \pmod{n}$$

$$\text{if } n = p \quad a \cdot b \equiv 0 \pmod{p}$$

$\Rightarrow p \mid ab$ since p prime

$p \mid a$ or b by Bézout

* Bézout will appear on final!

Def. A field is a ring F which

a) $[+]$ is commutative

b) Every $x \neq 0$ has $x^{-1} \in F$

Ex. $\mathbb{Q}, \mathbb{R}, \mathbb{C}, \mathbb{Z}_2, \mathbb{R}(x)$

NOT $\mathbb{Z}, \mathbb{R}[x]$

Remarks.

(1) A field is an integral domain

(2) if $R \subset F$ then R is also an integral domain

$\Rightarrow \mathbb{Z}$ is an integral domain $\mathbb{Z} \subset \mathbb{R}$

$\Rightarrow \mathbb{R}[x]$ is domain $\mathbb{R}[x] \subset \mathbb{R}(x)$

Theorem. If p prime $\mathbb{Z}_p$ is a field

Pf. $\mathbb{Z}_p = \{0, \underbrace{1, \dots, p-1}_{\text{coprime to } p}\}$

$$U_p = \{1, 2, \dots, p-1\} = \mathbb{Z}_p - \{0\}$$

Remark. If F is a field

$$(F, +) = \text{group}$$

$$(F^\times, \cdot) = F - \{0\} = \text{group}$$

Def. A ring hom/isom $f: R \rightarrow S$

$$f(x+y) = f(x) + f(y) \quad (\Rightarrow f(0) = 0)$$

$$f(x \cdot y) = f(x) \cdot f(y)$$

$$f(1) = 1 \quad (\text{needs to be hardcoded in})$$

Remark. if $f: (R, +, \cdot) \rightarrow (S, +, \cdot)$

is a ring hom then

$f: (R, +) \rightarrow (S, +)$ is a

commutative group hom

Fields. $\mathbb{Z}_n = \text{integral domain}$
 $\iff n = p \text{ prime}$

in this case $\mathbb{Z}_p = \text{field}$

Notation. When we use $\mathbb{Z}_p$ as a field
we denote it as $\mathbb{F}_p = \mathbb{Z}_p$

Ex. $\mathbb{Z}$ is an integral domain that is
not a field

Theorem - $\mathbb{F}_{p^n}$

a) if F is a finite field

then $|F| = p^n$ for some prime $p, n \geq 1$

b) If $p = \text{prime}$ & $n \geq 1$

there is a field F st $|F| = p^n$

c) There is only 1 such field

Eg. when $n=1$ $F = \mathbb{F}_p = \mathbb{Z}_p$

Today. Suppose F is a field $|F| < \infty$

Initial Challenge. find p

Lemma. There exists a smallest positive
integer n st $n \cdot 1 = 0$ in F and
 $n = p$ is a prime

Eg. p in $\mathbb{F}_p$, $p \equiv 0 \pmod{p}$ in $\mathbb{Z}_p$

Pf.

Define. $f: (\mathbb{Z}, +) \rightarrow (F, +)$

$$f(n) = n = \underbrace{(1_F + \dots + 1_F)}_{n \text{ times}}$$

f is NOT injective

$$|\mathbb{Z}| = \aleph_0 \quad |F| < \infty$$

f is a group homomorphism

$$f(m+n) = f(m) + f(n)$$

so $\ker f \neq \{0\}$ so $\ker f \trianglelefteq \mathbb{Z}$

$$\ker f = n\mathbb{Z} \quad n \in \{1, 2, 3, \dots\} \quad \text{normal subgroup}$$

$n \geq 2$ $\nexists \text{ } 1 \neq 0$

1st Isom. Theorem.

$$\mathbb{Z}/\ker f = \mathbb{Z}/n\mathbb{Z} \simeq \text{Im } f \text{ subring of } F$$

$$\mathbb{Z}_n = \mathbb{Z}/n\mathbb{Z} \simeq \text{Im } f \subset F$$

$$\begin{array}{ccccc} \text{prime} & \Leftarrow & \text{integral domain} & \Leftarrow & \text{integral subring field} \\ & & & & \Leftarrow \end{array}$$

NT.

n is the smallest positive integer $n \neq 0$ in F

if $n \neq \text{prime} \Rightarrow n = a \cdot b < n, b < n$

$a, b \neq 0$ in $F \Rightarrow a = 0$ or $b = 0$
contradiction

Back to Thm a

$F = \text{field}$, $p = 0 \text{ in } F$, p prime

$$\text{Im } f \cong \mathbb{Z} / \ker f = \mathbb{Z}_p = \mathbb{F}_p$$

Conclusions. $\mathbb{F}_p \subset F$

Setup. $(F, +, \cdot)$ is a field. $\mathbb{F}_p \subset F$,
 $|F| < \infty$

Suppose $N_1, N_2 \in F \Rightarrow N_1 + N_2 \in F$

$$\alpha \in \mathbb{F}_p \subset F \Rightarrow \alpha \cdot N_1 \in F$$

Implies F is a vector space over $\mathbb{F}_p$

so $\dim_{\mathbb{F}_p} F = n < \infty$

$$F \leftrightarrow \{ (x_1, x_2, \dots, x_n) \mid x_1, x_2, \dots, x_n \in \mathbb{F}_p \}$$

$$|F| = \underbrace{p \cdot p \cdot \dots \cdot p}_{n \text{ times}} = p^n$$

(p choices for each x_i in tuple)

all you need to be a VS is to be able to add and multiply by scalars

all VS has a dim

note, comparing 2 cosets will be on final!

Recall.

$$|F| < \infty$$

$$F \supset \mathbb{F}_p = \mathbb{Z}/p$$

 $F = \mathbb{F}_p$ - vector space

$$F \cong \mathbb{F}_p^n$$

$$|F| = p^n$$

Def. A ring hom is $f: R \rightarrow S$ s.t.

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

$$f(xy) = f(x)f(y)$$

$$f(1) = 1$$

Note. $(R, +)$ is an abelian group by def
so $f: (R, +) \rightarrow (S, +)$ is a
group hom $\Rightarrow f(0) = 0$

this is why you need to check $f(1) = 1$
but not $f(0) = 0$

Ex. (1) $f: \mathbb{Z} \rightarrow \mathbb{Z}$ the only ring
hom is $f(x) = x$

Pf. $f(1) = 1$ by def

$$f(2) = f(1+1) = f(1) + f(1) = 1+1 = 2$$

by ind $f(n) = n \quad \forall n \geq 0$ integer

$(\mathbb{Z}, +) \rightarrow (\mathbb{Z}, +)$ where $g(x) = 2x$
is a group hom

$$f(x) + f(-x) = f(x-x) = f(0) = 0$$

$$f(-x) = -f(x)$$

$$2(x+y) = 2x+2y$$

$$2 \cdot 1 \neq 1$$

$$2xy \neq 2x2y$$

Ex 2. If $f: \mathbb{R} \rightarrow \mathbb{R}$ is a ring hom
then $f(x) = x$

Pf. $f(1) = 1 \Rightarrow f(n) = n \quad \forall n \in \mathbb{Z}$

$$f\left(\frac{m}{n}\right) f(n) = f\left(\frac{m}{n} \cdot n\right) = f(m) = m \quad \forall m, n \in \mathbb{Q}$$

$$f\left(\frac{m}{n}\right) = \frac{m}{n}$$

if $x \geq 0$

$$f(x) = f(\sqrt{x} \cdot \sqrt{x})$$

$$= f(\sqrt{x})^2 \geq 0$$

$$x \geq y \Rightarrow f(x) - f(y)$$

$$= f(x-y) \geq 0$$

f is increasing $\Rightarrow f(x) - f(y) \geq 0$

$$q_n < x < q'_n \quad \lim q_n = \lim q'_n = x$$

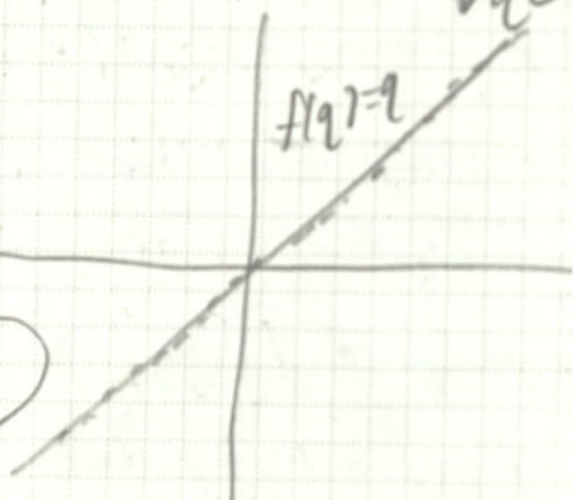
$$f(q_n) < f(x) < f(q'_n) \quad \text{Take limit}$$

$$q_n$$

$$q'_n$$

$$x \leq f(x) \leq x$$

$$f(x) = x$$



BUT $f(z) = \bar{z}$ is a ring hom
for $f: \mathbb{C} \rightarrow \mathbb{C}$

$$(3) f: \mathbb{C} \rightarrow \mathbb{C} \quad f(z) = \bar{z}$$

$$\overline{x+y} = \bar{x} + \bar{y} \quad \checkmark$$

$$\overline{xy} = \bar{x} \cdot \bar{y} \quad \checkmark$$

$$\overline{1} = 1 \quad \checkmark$$

Group homs

$$f: G \rightarrow H$$

$$f(e) = e$$

$$f(xy) = f(x)f(y)$$

Thm.

$$\ker f = \{x \mid f(x) = e\}$$

normal subgroup of G

$\text{Im } f = \text{subgroup of } H$

Ring homs

$$f: R \rightarrow S$$

$$f(0) = 0, \quad f(1) = 1$$

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

$$f(xy) = f(x)f(y)$$

Thm.

$$\ker f = \{x \in R \mid f(x) = 0\}$$

is an IDEAL of R

$\text{Im } f$ subring of S

Ex (4). $f: \mathbb{C} \rightarrow M_{2 \times 2}(\mathbb{R})$

$$f(a+bi) = \begin{pmatrix} a & b \\ -b & a \end{pmatrix} \text{ is a ring hom}$$

check. $f(x+y) = f(x) + f(y)$

$$f(xy) = f(x)f(y)$$

$$f(1) = \begin{pmatrix} 1 & 0 \\ 0 & 1 \end{pmatrix}$$

Def. An ideal $I \subset R$ is a subset

- (1) $(I, +)$ is a subgroup of $(R, +)$
- (2) $\forall r \in R \forall x \in I \Rightarrow r \cdot x \in I$

Ex (1) $R = \mathbb{Z}$ $I = n\mathbb{Z}$

- (1) $(n\mathbb{Z}, +)$ subgroup $(\mathbb{Z}, +)$ ✓
- (2) $\forall r \in \mathbb{Z}, x \in n\mathbb{Z}, x = ny \forall y \in \mathbb{Z}$
 $r \cdot x = rny \in n\mathbb{Z}$ multiple of n ✓

Remark. These are all the ideals of $\mathbb{Z}$

Ex (2) $R = \mathbb{R}[x, y]$

$I = \{P \in R \mid P(0,0) = 0\}$
is an ideal

(1) $(I, +)$ subgroup $(R, +)$

$P, Q \in I$ check $P - Q \in I$
no constant term!

(2) $P(0,0)$ means no constant term

$$P(x, y) = \sum_{a+b \geq 1} c x^a y^b$$

$$= x A(x, y) + y B(x, y)$$

removing all terms with
terms with only x or y

$$\langle x, y \rangle = \{x A(x, y) + y B(x, y)\}$$

$$I = \langle x, y \rangle$$

Ex 3. $R = \mathbb{Z}[x]$

$$I = \{P \in \mathbb{Z}[x] \mid P(0) \text{ is even}\}$$

(1) $P, Q \in I \Rightarrow P - Q \in I$

(2) $P \in I, T(x) \in \mathbb{Z}[x]$

$$P \cdot T \in I$$

$$PT(0) = \underbrace{P(0)}_{\text{even}} \cdot \underbrace{T(0)}_{\text{integer}} = \text{even}$$

$$P(x) = \underbrace{c_0}_{\text{even}} + c_1 x + \dots + c_d x^d$$

$$= 2 \cdot \left(\frac{c_0}{2}\right) + x(c_1 + c_2 x + \dots + c_d x^{d-1})$$

$$\in \langle 2, x \rangle$$

$$I = \langle 2, x \rangle$$

Def. Ideal (rewritten)

$(I, +)$ subgroup $(R, +)$

$$I \cdot R = I$$

Ring homs & ideals. $f: R \rightarrow S$

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

$$f(xy) = f(x)f(y)$$

$$f(1) = 1$$

$\Rightarrow f: (R, +) \rightarrow (S, +)$ is an abelian group hom

$$\Rightarrow f(0) = 0$$

note. $(R, \cdot)$ NOT a group

Eg. $f: \mathbb{Z} \rightarrow \mathbb{Z}$

group homs: $f(x) = ax$, $a = f(1)$

ring homs: $f(x) = x$

Ideals. $I \subset R$ st. $(I, +)$ subgroup

$$I \cdot R \subset I$$

eg. $I = n\mathbb{Z} \subset \mathbb{Z}$ only ideal

$\forall R$, fix $a_1, \dots, a_n \in R$

$$\langle a_1, a_2, \dots, a_n \rangle = \{ a_1 x_1 + a_2 x_2 + \dots + a_n x_n \mid x_i \in R \}$$

no constant $\langle x, y \rangle \subset R[x, y]$

even constant $\langle 2, x \rangle \subset \mathbb{Z}[x]$

Theorem. If $f: R \rightarrow S$ is a ring hom then

$$a) \ker f = \{x \in R \mid f(x) = 0\} \subset R$$

is an ideal

b) $\text{Im} f \subset S$ is a subring

Pf. $(\text{Im} f, +, \cdot, 0, 1)$ is a ring

$$0 = f(0)$$

$$1 = f(1)$$

$\forall x, y \in \text{Im} f, +, \cdot ?$

a) $f: G \rightarrow H$ group hom

$$\ker f = \{g \mid f(g) = e\} \triangleleft G$$

subgroup. $f(g) = e, f(h) = e$

$$f(gh^{-1}) = f(g)f(h)^{-1} = ee^{-1} = e$$

normal. $\forall x \in \ker f, \forall g \in G,$

$$g x g^{-1} \in \ker f$$

$$f(g x g^{-1}) = f(g) \underbrace{f(x)}_e f(g)^{-1} = f(g) f(g)^{-1} = e$$

b) $f: R \rightarrow S$ ring hom

$$\ker f = \{x \mid f(x) = 0\} \text{ ideal of } R$$

subgroup. $f(x) = 0, f(y) = 0$

$$f(x-y) = f(x) - f(y) = 0 - 0 = 0$$

$$\Rightarrow x-y \in \ker f$$

ideal. $\forall i \in \ker f, \forall x \in R$, check $ix \in \ker f$

$$f(i) = 0, f(ix) = f(i)f(x) = 0 \in \ker f$$

Ex. $R = \mathbb{R}[x]$, $S = \mathbb{R}$

$f: \mathbb{R}[x] \rightarrow \mathbb{R}$ st $f(P(x)) = P(\pi)$

Claim. f is a ring hom

Check. $f(P(x) + Q(x)) = f(P(x)) + f(Q(x))$

$f(P(x)Q(x)) = f(P(x))f(Q(x))$

$f(1) = 1$

true of all functions

$\ker f = \{P(x) \in \mathbb{R}[x] \mid f(P(x)) = 0\}$
 $P(\pi) = 0$

$= \{P \text{ st } x - \pi \mid P\}$

$= \langle \underbrace{x - \pi}_{a_1} \rangle = \{(x - \pi) \cdot Q(x) \mid Q(x) \in \mathbb{R}[x]\}$

But. $R = \mathbb{R}[x]$, $S = \mathbb{C}$

$f: \mathbb{R}[x] \rightarrow \mathbb{C}$ st $f(P(x)) = P(i)$

$f(x^3 + 2) = i^3 + 2 = 2 - i$

$\ker f = \{P \in \mathbb{R}[x] \mid P(i) = 0\}$

$= \{P \text{ st } x - i \mid P(x)\}$

$P(x) = a_0 + a_1x + \dots + a_dx^d$ $a_i \in \mathbb{R}$

need $P(i) = a_0 + a_1i + a_2i^2 + \dots + a_di^d = 0$

$\overline{P(i)} = \overline{a_0} + \overline{a_1}i + \overline{a_2}i^2 + \dots + \overline{a_d}i^d = 0$

$= P(\bar{i}) = P(-i) = 0$

$$P(i) = 0 = P(-i)$$

$$(x-i)(x-(-i)) \mid P(x)$$

$$x^2+1 \mid P(x)$$

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

Remark. $f: R \rightarrow S$ ring hom

then $f: R^\times \rightarrow S^\times$ is a group hom
 $\forall$ all x st $x^{-1} \in R$

if $f: R \rightarrow S$ a ring isom

$\Rightarrow f: R^\times \rightarrow S^\times$ is a group isom

Applications. CRT if $(m, n) = 1$

$\mathbb{Z}_{mn} \cong \mathbb{Z}_m \times \mathbb{Z}_n$ as abelian groups
 also as rings!

$$\Rightarrow \underbrace{\mathbb{Z}_{mn}^\times}_{U_{mn}} \cong \underbrace{\mathbb{Z}_m^\times}_{U_m} \times \underbrace{\mathbb{Z}_n^\times}_{U_n}$$

Consequence. $\varphi(mn) = \varphi(m)\varphi(n)$
 if $(m, n) = 1$

$$\Rightarrow \varphi(p_1^{k_1} p_2^{k_2} \dots p_r^{k_r})$$

$$= \varphi(p_1^{k_1}) \varphi(p_2^{k_2}) \dots \varphi(p_r^{k_r})$$

$$\Rightarrow \varphi(\prod p_i^{k_i}) = \prod p_i^{k_i-1} (p_i - 1)$$

Lecture Notes

4.30.25

I ideals in R

- $(I, +)$ subgroup of $(R, +)$
- $I \cdot R = I$

typical ex.

$$I = (a_1, a_2, \dots, a_n)$$

$$= \{a_1 x_1 + a_2 x_2 + \dots + a_n x_n \mid x_1, \dots, x_n \in R\}$$

We saw a while back

$R/I = \{r+I \mid r \in R\}$ is an abelian group

Remark: $(a+I) \cdot (b+I)$

$$= "ab + aI + bI + I^2"$$

$$= ab + I \quad \text{this turns } R/I \text{ into a ring}$$

Recall how cosets work

$$a+I = b+I$$

$$\Leftrightarrow a-b \in I$$

$$g_1 + I = g_2 + I$$

$$\Leftrightarrow g_1^{-1} g_2 \in I$$

R/I is a construction meant to vanish I

$$R = \mathbb{Z}, I = n\mathbb{Z}$$

$$\mathbb{Z}/n\mathbb{Z} = \mathbb{Z}_n \leftarrow \text{sets } n \equiv 0$$

Note -

$$(R/I, +, \cdot, \bar{0}, \bar{1})$$

$$(R/I, +, \bar{0}) \text{ group}$$

$$(a+I) \cdot (1+I) = a \cdot 1 + I$$

$$(a+I)[(x+I) + (y+I)]$$

$$= (a+I)(x+I) + (a+I)(y+I)$$

$$\text{eg. } R = \mathbb{Z}[i]$$

$$I = (2+i) = \{(2+i)x \mid x \in \mathbb{Z}[i]\}$$

$$R/I = \mathbb{Z}[i]/(2+i) \quad \begin{array}{l} \leftarrow \text{variables} \\ (2+i) \end{array}$$

$$2+i \equiv 0 \text{ in } R/I$$

$$i \equiv -2 \text{ in } R/I$$

$$a+ib \equiv a + (-2)b \equiv a - 2b \text{ in } R/I$$

$$a+ib+I = a-2b+I$$

$$\text{Ex. } R = \mathbb{Z}[\sqrt{7}] = \{a+b\sqrt{7} \mid a, b \in \mathbb{Z}\}$$

$$I = (1+\sqrt{7}) = \{(1+\sqrt{7})(x+y\sqrt{7}) \mid x, y \in \mathbb{Z}\}$$

$$R/I = \mathbb{Z}[\sqrt{7}]/(1+\sqrt{7}) \quad \begin{array}{l} \text{we are vanishing} \\ 1+\sqrt{7} \end{array}$$

$$\text{so } 1+\sqrt{7} \equiv 0 \text{ in } R/I$$

$$\sqrt{7} \equiv -1$$

$$\text{note, } m+n\sqrt{7} \equiv m-n \text{ in } R/I$$

But. $R = \mathbb{Z}[i]$, $I = (3)$

It's not true that each coset
 $a + bi + I$ can be written in $k + I$
setting $3 \equiv 0$

note, setting $I \equiv 0$ in R/I

(eg. $R = \mathbb{Z}[x]$).

$$I = (3, 2x) = \{ 3 \cdot P(x) + 2x \cdot Q(x) \mid P, Q \in \mathbb{Z}[x] \}$$

What is R/I ? we vanish I

$$3 \equiv 0 \text{ in } R/I$$

$$2x \equiv 0 \text{ in } R/I$$

$$- 3x \equiv 0$$

$$\hline x \equiv 0$$

A typical element in R/I is

$$P(x) + I$$

$$= a_0 + \underbrace{a_1 x}_0 + \underbrace{a_2 x^2}_0 + \dots + \underbrace{a_d x^d}_0 + I$$

$$\equiv a_0 + I \quad \text{takes care of } x \equiv 0$$

$$\equiv \begin{cases} 0 + I \\ 1 + I \\ 2 + I \end{cases} \quad \begin{array}{l} \text{takes care of} \\ 3 \equiv 0 \end{array}$$

$$R/I = \{ \bar{0}, \bar{1}, \bar{2} \}$$

Eg. $R = \mathbb{R}[x, y]$

$$I = (y^2 - x^3) = \{ (y^2 - x^3) \cdot A(x, y) \mid A \in R \}$$

What is R/I ? Vars in I ,

$$y^2 - x^3 \equiv 0$$

$$y^2 \equiv x^3$$

$$\begin{aligned} P(x, y) &= A_0(x) + A_1(x)y + A_2(x)y^2 + \dots + A_d(x)y^d \\ &\equiv A_0(x) + A_1(x)y + A_2(x)x^3 + A_3(x)x^3y \\ &\quad + A_4(x)x^6 + A_5(x)x^6y + \dots \end{aligned}$$

$$\equiv A(x) + B(x)y \quad \text{these are all distinct in } R/I$$

$$\begin{aligned} \mathbb{R}[x, y]/(y^2 - x^3) &= \{ A(x) + y \cdot B(x) \} \\ &= \mathbb{R}[x] + y \cdot \mathbb{R}[x] \end{aligned}$$

Recall. $f: \mathbb{R}[x] \rightarrow \mathbb{C}$ st

$$f(p(x)) = p(i)$$

$$f(a + bx) = a + bi \quad \text{Surj}$$

$$\ker f = (x^2 + 1)$$

Let Isom. $\mathbb{R}[x]/(x^2 + 1) \cong \mathbb{C}$

in $\mathbb{R}[x]/(x^2 + 1)$ Set $x^2 + 1 = 0$

$$= \{ a + b \underbrace{x}_{i} \mid a, b \in \mathbb{R}, x^2 = -1 \}$$

Theorem. If $F = \text{field}$ and
 $P(x) \in F[x]$, can always do
 $F[x]/P(x)$ is a field iff
 $P(x)$ is irreducible

Ex. $F = \mathbb{R}$, $P(x) = x^2 + 1$
 $\mathbb{R}[x]/(x^2 + 1) \simeq \mathbb{C}$. $x^2 + 1$ is irred

Ex. $R = \mathbb{Z}$, $I = n\mathbb{Z}$

$R/I = \mathbb{Z}/n\mathbb{Z}$ is a field $\Leftrightarrow$ n prime

* Bezout will be an final *

Application. $\forall p$ prime $\forall n \geq 1$
there exists $\mathbb{F}_{p^n}$ elements

$$\mathbb{F}_p = \mathbb{Z}_p$$

how to do $\mathbb{F}_{p^n}$?

eg. $p=2$, $n=3$, $P(x) = x^3 + x + 1 \in \mathbb{F}_2[x]$
is irreducible

$$\mathbb{F}_2[x]/(x^3 + x + 1) = \{a_0 + a_1x + a_2x^2\}$$

$$|\mathbb{F}_2[x]/(x^3 + x + 1)| = 8 = 2^3 \uparrow$$

$f: G \rightarrow H$ is a group hom

Def. $\ker f = \{x \in G \mid f(x) = e_H\} \triangleleft G$

$\text{Im } f = \{f(g) \mid g \in G\} \leq H$

note. f inj $\iff \ker f = \{e_H\}$

Aside. $f(g^{-1}) = f(g)^{-1}$

Def. A subgroup N of G is normal if

a) every left coset of N is also a right coset

$\iff$
 b) $gN = Ng \ \forall g \in G \iff gNg^{-1} = N \ \forall g \in G$
 $\iff gng^{-1} \in N \ \forall n \in N \ \forall g \in G$

Def. $G/N = \{\text{all cosets } gN\} \ni eN$
 $\circ$ $gN \cdot hN = ghN$ is a new ^{unit} group
_{operation}
 $\text{and } (gN)^{-1} = g^{-1}N$

note. $|G/N| = [G:N] = \frac{|G|}{|N|}$
 $|G/N| < |G|$

Recall. all groups with a prime # of elements are cyclic

Observe. $\pi: G \rightarrow G/N$ hom st $\pi(g) = gN$
 $\ker \pi = N$

ie. in G/N every $n \in N$ goes to the identity

Observe $\text{Im } \pi = G/N = G/\ker \pi$

1st Isomorphism Theorem.

if $f: G \rightarrow H$ is a group hom

$G/\ker f \cong \text{Im } f$

Def. A ring is a collection $(R, +, \cdot, 0, 1)$ which satisfies $(R, +, 0)$ abelian group

Def. $S \subset R$ is a subring if

1. $1 \in S$

2. $(S, +)$ subgroup of R

3. $a \cdot b \in S \quad \forall a, b \in S$

Def. R is a ring. A zero-divisor is an element $a \in R$ $a \neq 0$ st $a \cdot b = 0 \quad \exists b \neq 0$

Lemma. Cancellation

in groups, $ax = ay \Rightarrow x = y$ since a^{-1} exists $\forall a \in G$

in rings, $ax = ay$ where $a \neq 0 \Rightarrow x = y$ iff a is not a zero divisor

Def. A commutative ring R is an integral domain if it has no zero-divisors

ie. $x \cdot y = 0 \iff x = 0$ or $y = 0 \quad \forall x, y \in R$

Def. A field is a commutative ring F st every $x \neq 0$ has an $x^{-1} \in F$

note 1) A field is an integral domain

2) All subrings of a field are integral domains

Lemma. $\mathbb{Z}_n$ ($n \geq 2$) is an integral domain $\iff n$ is prime

Theorem. $\mathbb{Z}_n$ is a field if n is prime

Remark. if F is a field

1) $(F, +)$ is a group

2) $(F^\times, \cdot)$ is a group

Def. $f: R \rightarrow S$ is a ring hom/isom if:

- 1) $f(x+y) = f(x) + f(y)$ ($\Rightarrow f(0) = 0$)
- 2) $f(x \cdot y) = f(x) \cdot f(y)$
- 3) $f(1) = 1$

Remark. if $f: (R, +, \cdot) \rightarrow (S, +, \cdot)$ is a ring hom.,
 $f: (R, +) \rightarrow (S, +)$ is a commutative group hom.

Notation. $\mathbb{Z}_p \equiv \mathbb{F}_p$ in the context of fields

Theorem. $\mathbb{F}_{p^n}$ is a finite field iff $|\mathbb{F}_{p^n}| = p^n$
for some prime p and $n \geq 1$, and there
is only one such field

note. $f: (\mathbb{Z}, +) \rightarrow (F, +)$ st
 $f(n) = n = \underbrace{(1_F + 1_F + \dots + 1_F)}_{n \text{ times}}$

$\mathbb{Z}_n \cong \mathbb{Z}/n\mathbb{Z} \cong \text{Inf} \subset F$
 $n \text{ prime} \leftarrow \text{integral domain} \leftarrow \text{integral domain} \leftarrow \text{subring} \leftarrow \text{field}$
i.e. $\mathbb{F}_p \subset F$

Ring homs. for $f: R \rightarrow S$

$\ker f = \{x \in R \mid f(x) = 0\}$ is an ideal of R
 $\text{Im} f = \{f(x) \mid x \in R\}$ is a subring of S

Def. An ideal $I \subset R$ is a subset st:

- 1) $(I, +)$ is a subgroup of $(R, +)$
- 2) $\forall x \in I \quad \forall r \in R \quad \forall x \in I$
i.e. $I \cdot R \subseteq I$

Notation. $a_1, a_2, \dots, a_n \in R$

$$\langle a_1, a_2, \dots, a_n \rangle = \{ a_1 x_1 + a_2 x_2 + \dots + a_n x_n \mid x_i \in R \}$$

note $\langle x, y \rangle \subset R[x, y]$

$$\langle z, x \rangle \subset \mathbb{Z}[x]$$

Remark. $f: R \rightarrow S$ ring hom then
 $f: R^x \rightarrow S^x$ is a group hom

Application. if $(m, n) = 1$

$$\mathbb{Z}_m \times \mathbb{Z}_n \cong \mathbb{Z}_{mn} \text{ as abelian groups}$$

$$\mathbb{Z}_m^x \times \mathbb{Z}_n^x \cong \mathbb{Z}_{mn}^x \text{ as rings}$$

i.e. $U_m \times U_n \cong U_{mn}$

Consequence. if $(m, n) = 1$

$$\varphi(mn) = \varphi(m) \varphi(n)$$

$$\Rightarrow \varphi(p_1^{k_1} p_2^{k_2} \dots p_r^{k_r})$$

$$= \varphi(p_1^{k_1}) \varphi(p_2^{k_2}) \dots \varphi(p_r^{k_r})$$

$$\Rightarrow \varphi(\prod p_i^{k_i}) = \prod p_i^{k_i-1} (p_i - 1)$$

Recall. $R/I = \{ r+I \mid r \in R \}$ is an abelian group

note. $(a+I) \cdot (b+I) = ab+I$, which
turns R/I into a ring

Recall. $a + I = b + I \iff a - b \in I$

$$g_1 + I = g_2 + I \iff g_1^{-1} g_2 \in I$$

note. R/I is a construction that "quotients I "

$$I \equiv 0 \text{ in } R/I$$

Theorem. If F is a field and $P(x) \in F[x]$

$F[x]/P(x)$ is a field iff $P(x)$ is
irreducible

Application. $\forall p$ prime $\forall n \geq 1$,

there exists $|\mathbb{F}_{p^n}|$ elements