1/1

MATH 561 H1 (561/562) Fall 2011
Abstract Algebra I
MM 117, MW 3:35-4:50

Drew Armstrong
armstrong@math.miami.edu

Look at syllabus

What is this course about?
What is "algebra"?

prehistory ⟶ 1830 ⟶ today

MTH 461
- solving polynomial equations

MTH 561/562
- study of abstract structures

eg group
ring
field
vector space
module
algebra
category
⋮

SYMMETRY

NOT a prerequisite

Notes still on my webpage

(1) Algebra before ~1830
(a sketch of MTH 461)

Goal: Solve 1 polynomial equation in 1 unknown

eg $ax^2 + bx + c = 0$.

$$\Rightarrow x = \frac{-b \pm \sqrt{b^2 - 4ac}}{2a}$$

Quadratic Formula. (prehistory)

eg. the equation $x^3 + px + q = 0$ has at least one solution given by

$$x = \sqrt[3]{-\frac{q}{2} + \sqrt{\frac{q^2}{4} + \frac{p^3}{27}}} + \sqrt[3]{-\frac{q}{2} - \sqrt{\frac{q^2}{4} + \frac{p^3}{27}}}$$

"Cardano's formula" (1545).

Cubic & Quartic polynomials
- completely solved
- Italy, 1500's
- led to discovery/invention of complex numbers.

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

($\mathbb{R}$: real numbers.)

Q: Is there ($\exists$?) a formula to solve the quintic

$$ax^5 + bx^4 + cx^3 + dx^2 + ex + f = 0.$$

A: Theorem (Abel, 1824)

There is no ($\nexists$) formula for x in terms of

$\underbrace{a, b, c, d, e, f}$
coefficients

and algebraic operations $+, -, \times, \div, \sqrt[n]{}$.

However, some quintics can be "solved"

eg $x^5 - 5x^3 + 4x = 0$

has complete solution

$$x \in \{-2, -1, 0, 1, 2\}.$$

Because

$$x^5 - 5x^3 + 4x = (x+2)(x+1)x(x-1)(x-2) \quad ///$$

Q: Which (quintic) polynomials can be "solved"?

A: (Galois, 1830)

Given polynomial $f(x)$, let G be the "group" of symmetries of the roots of $f(x)$.

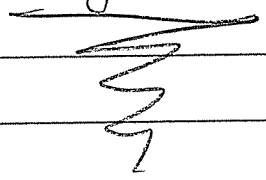
Then

$f(x)$ is "solvable" $\Leftrightarrow$ G is a "solvable group"

TECHNICAL TERMS

Idea: Everything we want to know about $f(x)$ is encoded by its "group" of symmetries.

Paradigm Shift



(2) Algebra after ~1830

Idea: Study collections of symmetries and their structure.

What structure?

Example: Let D = regular dodecahedron

Def: a "symmetry" of $D \subseteq \mathbb{R}^3$ is a distance-preserving map $f: \mathbb{R}^3 \to \mathbb{R}^3$ that sends D to itself.

eg: let f = rotation by $2\pi/3$ around line through two opposite vertices.

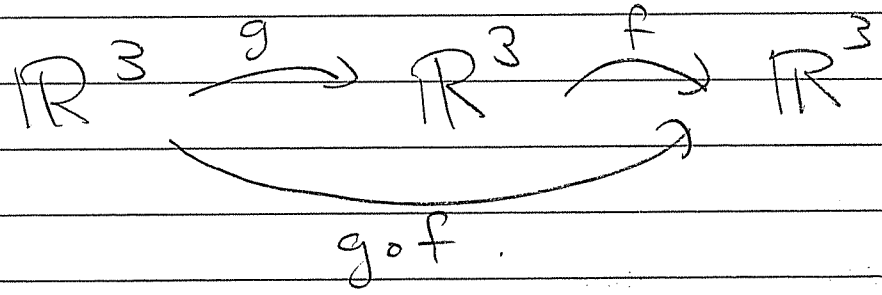
Let G = the set of symmetries of D

Note: If $f, g \in G$ then

$f \circ g \in G$

functional composition.

"do g then do f".



We say G is closed under composition.
The pair $(G, \circ)$ is called a group.

This group has a special name

$G = A_5$.

Fact: $|A_5| = 60$

↑

D has 60 symmetries

... to break the suspense

Definition: (G, f)

A group is a set G together with a binary operation

$f: G \times G \to G$

[$G \times G := \{(g,h) : g, h \in G\}$ ordered pairs from G]

satisfying 3 AXIOMS:

(G1) $\forall\, a, b, c \in G$ we have

$$f(f(a,b), c) = f(a, f(b,c))$$

"f is ASSOCIATIVE"

(G2) $\exists$ special element $e \in G$ such that

$$\forall\, g \in G,\ f(e, g) = g.$$

"e is called the IDENTITY ELEMENT".

(G3) $\forall\, g \in G\ \exists\, h \in G$ such that

$$f(g, h) = e.$$

"h is the INVERSE of g". ///

What!?

Office Hours
3:30 – 5:00 PM Tues & Thurs

Exams
Wed Sep 28
Mon Oct 31
Wed Nov 30

HW 1 – ?

Review:

Definition: A group is a set G together with a binary operation $G \times G \to G$, $(a,b) \mapsto ab$ (juxtaposition)

satisfying:

Assoc. (G1) $\forall a,b,c \in G,\ (ab)c = a(bc)$.

Ident. (G2) $\exists e \in G,\ \forall a \in G\ \ ae = ea = a$.

Inverse. (G3) $\forall a \in G\ \exists a^{-1} \in G,\ aa^{-1} = a^{-1}a = e$. ///

Loose ends...
What does "=" mean?

Def: Let S be a set. An equivalence relation is a subset $R \subseteq S \times S$

(for $x, y \in S$ we say $x \sim y \iff (x,y) \in R$)

satisfying

Trans (ER1) $x \sim y$ AND $y \sim z \Rightarrow x \sim z$

Symm. (ER2) $x \sim y \Rightarrow y \sim x$

Reflexive (ER3) $x \sim x \quad \forall x \in S$ ///

So ... a group is a triple $(G, =, (a,b) \mapsto ab)$ satisfying ER1, ER2, ER3, G1, G2, G3.

Prop: Given $a \in G$, its inverse is unique.

Proof: Suppose $\exists\, b, c \in G$, $ab = ba = e$ & $ac = ca = e$.

Then

$$b = be = b(ac) = (ba)c = ec = c$$

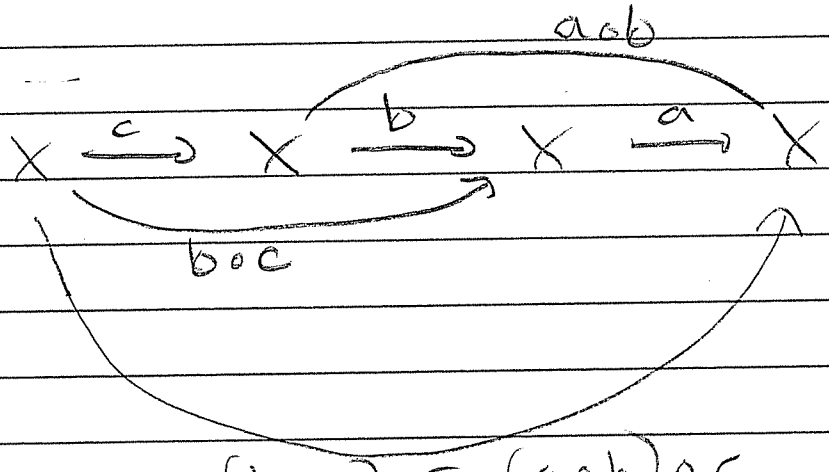
Cor: We can call it "the" inverse of a and give it a name "a^{-1}".

Think $ab = a+b$ $\quad (a+b)+c = a+(b+c)$

$= a \times b$ $\quad (a \times b) \times c = a \times (b \times c)$

$= a \circ b$ $\quad (a \circ b) \circ c = a \circ (b \circ c)$

Let $a, b, c : X \to X$ be functions



Automatic!

$a \circ (b \circ c) = (a \circ b) \circ c$

Think $a + 0 = 0 + a = a$

$a \times 1 = 1 \times a = a$

$a \circ id = id \circ a = a$

$a + (-a) = (-a) + a = 0$

$a \times (1/a) = (1/a) \times a = 1$

$a \circ a^{-1} = a^{-1} \circ a = id.$

↖ inverse function

Examples.

Consider $\mathbb{Z} \subseteq \mathbb{Q} \subseteq \mathbb{R} \subseteq \mathbb{C}$.

$(\mathbb{Z}, +)$
$(\mathbb{Q}, +)$
$(\mathbb{R}, +)$
$(\mathbb{C}, +)$
} are (additive) groups

$(\mathbb{Q}^\times, \times)$
$(\mathbb{R}^\times, \times)$
$(\mathbb{C}^\times, \times)$
} are (multiplicative) groups

Def: $\mathbb{R}^\times = \mathbb{R} - \{0\}$

$(\mathbb{Z}^\times, \times)$ is <u>not</u> a group. (Why?)

because $2 \in \mathbb{Z}^\times$ has no inverse.

$\exists\, x \in \mathbb{Z}^\times$ s.t. $2x = 1$.

"$\frac{1}{2}$" $\notin \mathbb{Z}$.

we <u>cannot</u> divide.

$(\mathbb{R}, \times)$ is not a group. (Why?)

Suppose $\exists\, \alpha \in \mathbb{R}$, $\alpha 0 = 0\alpha = 1$
$(\alpha = 0^{-1})$

Then for any $a, b \in \mathbb{R}$ we have

$$0a = 0 = 0b.$$
$$\alpha(0a) = \alpha(0b)$$
$$(\alpha 0)a = (\alpha 0)b$$
$$1a = 1b$$
$$a = b$$

Contradiction. ☹

"Can't Divide by zero"

Prop (Cancellation)

Given group G let $a, b, c \in G$.
Then $ab = ac \Rightarrow b = c$.

Proof: $ab = ac$
$$a^{-1}(ab) = a^{-1}(ac)$$
$$(a^{-1}a)b = (a^{-1}a)c$$
$$1b = 1c$$
$$b = c.$$

O.H. 3:30 – 5:00 PM Tues & Thurs

Exams Wed Sep 28
Mon Oct 31
Wed Nov 30

HW 1 due **Mon Sep 12**.

A group is a set with a binary operation that is
- Closed — G
- Associative — A
- Identity — I
- Inverse. — N

Theorem: We don't need to write brackets.

eg. $(ab)c = a(bc)$
So just say "abc".

$((ab)c)d$ "Associahedron"

$(a(bc))d$ $(ab)(cd)$

$a((bc)d) = a(b(cd))$

So just say "abcd".

To be precise . . .

Prop 1.4 in the book.

Given $a_1, a_2, \ldots, a_n \in G$

$\exists!$ way to define the product

(call it $[a_1 a_2 \cdots a_n] \in G$) such that

i) $[a] = a \quad \forall\, a \in G$

ii) $[ab] = ab \quad \forall\, a, b \in G$

iii) $[a_1 a_2 \cdots a_n] = [a_1 \cdots a_i][a_{i+1} \cdots a_n] \quad \forall\, 1 < i < n.$

Proof by induction on n.

True for $n = 3$ because

$[abc] = a(bc) = (ab)c$.

Suppose $[a_1 \cdots a_r]$ exists and is unique for $r \leq n-1$.

We then define

$$[a_1 a_2 \cdots a_n] := [a_1 \cdots a_{n-1}][a_n]$$

Does it satisfy (iii)?

If $i = n-1$, YES by definition.

So let $1 < i < n-1$. Then

$$\begin{aligned}
[a_1 a_2 \cdots a_n] &= [a_1 \cdots a_{n-1}][a_n] && \text{definition} \\
&= \left([a_1 \cdots a_i][a_{i+1} \cdots a_{n-1}]\right)[a_n] && \text{by induction} \\
&= [a_1 \cdots a_i]\left([a_{i+1} \cdots a_{n-1}][a_n]\right) && G1 \\
&= [a_1 \cdots a_i][a_{i+1} \cdots a_n] && \text{by induction.}
\end{aligned}$$

... So just say "$[a_1 a_2 \cdots a_n] = a_1 a_2 \cdots a_n$" and never use brackets again (unless we need them).

Recall:
If $ab = ba \ \forall a, b \in G$, we say G is abelian.

eg $\mathbb{Z}, \mathbb{Q}, \mathbb{R}, \mathbb{C}, +$.
$\mathbb{Q}^\times, \mathbb{R}^\times, \mathbb{C}^\times, \times$

are all abelian.

Q: Is there a natural, non-abelian group?
A:
Yes. Matrix Groups.

Let $M_n(\mathbb{R}) = \{ n \times n \text{ matrices with elements in } \mathbb{R} \}$

Remark: $M_n(\mathbb{R})$ is a ring (T.O.U.) with componentwise addition $+$ and a matrix product $\times$ defined as follows.

Dot/Inner Product:

For column vectors $\vec{u} = \begin{pmatrix} u_1 \\ \vdots \\ u_n \end{pmatrix}, \vec{v} = \begin{pmatrix} v_1 \\ \vdots \\ v_n \end{pmatrix} \in \mathbb{R}^n$

let $\vec{u} \cdot \vec{v} = (\vec{u}, \vec{v}) = \vec{u}^T \vec{v}$

$$= (u_1 u_2 \cdots u_n) \begin{pmatrix} v_1 \\ v_2 \\ \vdots \\ v_n \end{pmatrix} = u_1 v_1 + u_2 v_2 + \cdots + u_n v_n$$

$$= \sum_i u_i v_i$$

Define length/norm $\|\vec{u}\|$ by $\|\vec{u}\|^2 = (\vec{u}, \vec{u})$

$$\|\vec{u}\| = \sqrt{u_1^2 + u_2^2 + \cdots + u_n^2}$$

Pythagoras

Matrix Product: Given $A, B \in M_n(\mathbb{R})$

define $AB \in M_n(\mathbb{R})$ by

$$(AB)_{i,j} := \sum_k (A)_{i,k} (B)_{k,j}$$

i,j-entry

$$AB = \begin{pmatrix} — \vec{a}_1^T — \\ — \vec{a}_2^T — \\ \vdots \\ — \vec{a}_n^T — \end{pmatrix} \begin{pmatrix} | & | & & | \\ \vec{b}_1 & \vec{b}_2 & \cdots & \vec{b}_n \\ | & | & & | \end{pmatrix} := \begin{pmatrix} (\vec{a}_1, \vec{b}_1) & (\vec{a}_1, \vec{b}_2) & \\ (\vec{a}_2, \vec{b}_1) & \ddots & \\ & & (\vec{a}_n, \vec{b}_n) \end{pmatrix}$$

Why this? ☹

dot products.

☆ GOOD REASON ☆

Think of $A \in M_n(\mathbb{R})$ as a (linear) function $A: \mathbb{R}^n \to \mathbb{R}^n$ defined by

$$\vec{x} \longmapsto A\vec{x}$$

col. vector col. vector

Then (theorem) we have

$$(A \circ B)\vec{x} \overset{\text{DEF}}{=} A(B\vec{x}) \overset{\text{THM}}{=} (AB)\vec{x}$$

Big idea

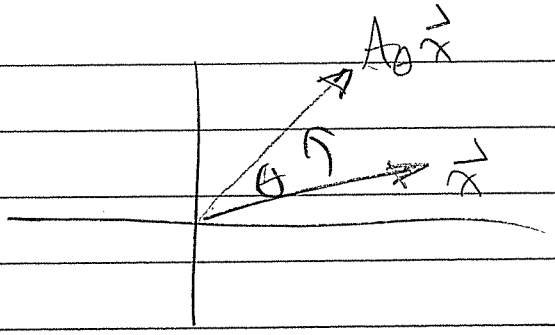
$$\left[\begin{array}{l} M_n(\mathbb{R}) \text{ with} \\ \text{matrix product} \end{array}\right] \hookrightarrow \left[\begin{array}{c} \text{linear functions} \\ \mathbb{R}^n \to \mathbb{R}^n \\ \text{with composition} \end{array}\right]$$

eg. Let $A_\theta = \begin{pmatrix} \cos\theta & -\sin\theta \\ \sin\theta & \cos\theta \end{pmatrix}$

So $A_\theta \vec{x} = \begin{pmatrix} \cos\theta & -\sin\theta \\ \sin\theta & \cos\theta \end{pmatrix} \begin{pmatrix} x \\ y \end{pmatrix}$

$$= \begin{pmatrix} x\cos\theta - \sin\theta \cdot \\ x\sin\theta + y\cos\theta \end{pmatrix}$$

Picture:



Then

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

theorem.

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

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

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

eg let $A, B \in M_3(\mathbb{R})$ be

A = rotate 90° in x,y-plane

B = rotate 90° in y,z-plane.

$$A = \begin{pmatrix} & -1 & \\ 1 & & \\ & & 1 \end{pmatrix} \quad \& \quad B = \begin{pmatrix} 1 & & \\ & & -1 \\ & 1 & \end{pmatrix}$$

blanks are zeroes.

Then $A \circ B = AB = \begin{pmatrix} 1 & & \\ & 1 & \\ & & 1 \end{pmatrix}$

$B \circ A = BA = \begin{pmatrix} -1 & & \\ & -1 & \\ & & 1 \end{pmatrix}$

$AB \neq BA$.

Matrices don't (generally) commute !!

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

$(M_n(\mathbb{R}), \times)$ is NOT.

some matrices/linear funcs. are not invertible. eg. $\begin{pmatrix} 0 & 0 \\ 0 & 0 \end{pmatrix}$, $\begin{pmatrix} 1 & 0 \\ 0 & 0 \end{pmatrix}$

Define:

$$GL_n(\mathbb{R}) = \{ A \in M_n(\mathbb{R}) : A^{-1} \text{ exists} \}$$
$$= \{ A \in M_n(\mathbb{R}) : \det(A) \neq 0 \}.$$

"the general linear group".

Note. $GL_n(\mathbb{R}) = M_n(\mathbb{R})^\times$

$= $ invertible elements of $M_n(\mathbb{R})$

a NATURAL, NON-ABELIAN group.

Other important groups

$$SL_n(\mathbb{R}) = \{A \in M_n(\mathbb{R}) : \det(A) = 1\}$$
$$O_n(\mathbb{R}) = \{A \in M_n(\mathbb{R}) : AA^T = I\}$$
$$SO_n(\mathbb{R}) = \{A \in M_n(\mathbb{R}) : AA^T = I, \det A = 1\}$$

What does $AA^T = I$ mean?

Let $A^T = \begin{pmatrix} | & | & & | \\ \vec{a}_1 & \vec{a}_2 & \cdots & \vec{a}_n \\ | & | & & | \end{pmatrix}$

column vectors.

Then

$$AA^T = \begin{pmatrix} - \vec{a}_1^T - \\ - \vec{a}_2^T - \\ \vdots \\ - \vec{a}_n^T - \end{pmatrix} \begin{pmatrix} | & | & & | \\ \vec{a}_1 & \vec{a}_2 & \cdots & \vec{a}_n \\ | & | & & | \end{pmatrix} \qquad I.$$

$$= \begin{pmatrix} (\vec{a}_1, \vec{a}_1) & (\vec{a}_1, \vec{a}_2) & & \\ (\vec{a}_2, \vec{a}_1) & \ddots & & \\ & & & (\vec{a}_n, \vec{a}_n) \end{pmatrix} = \begin{pmatrix} 1 & & 0 \\ & 1 & \\ & & \ddots \\ 0 & & & 1 \end{pmatrix}$$

identity matrix.

So $(AA^T)_{i,j} = (\vec{a}_i, \vec{a}_j) = \begin{cases} 1 & i = j \\ 0 & \text{else} \end{cases}$

$i \neq j \implies (\vec{a}_i, \vec{a}_j) = 0$ orthogonal

$i = j \implies (\vec{a}_i, \vec{a}_i) = 1 \implies \|\vec{a}_i\| = 1$.

unit vector.

HW 1 due Monday
- beginning of class

Food for Thought:

(1) Given $A, B \in M_n(\mathbb{R})$ we have

$$AB = I \implies BA = I$$

Why?

(2) In a ANY (non abelian) group G, we can replace axiom

(Inv) $\forall a \in G \; \exists b \in G$ s.t. $ab = ba = e$

with

(Inv') $\forall a \in G \; \exists b \in G$ s.t. $ab = e$

i.e. (Inv) $\iff$ (Inv')

why?

Today: Subgroups

Def: Let $(G, (a,b) \mapsto ab)$ be a group and let $H \subseteq G$ be a subset of elements. We say H is a subgroup of G (and write $H < G$) if

- $\forall a, b \in H$, $ab \in H$. (H is "closed")
- $e \in H$.
- $\forall a \in H$, $a^{-1} \in H$.

i.e. H is itself a group with the same operation, identity, and inverses.

eg. The set

$$H = \left\{ \begin{pmatrix} 1 & a \\ 0 & 1 \end{pmatrix} : a \in \mathbb{R} \right\} \subseteq GL_2(\mathbb{R})$$

is a subgroup of $GL_2(\mathbb{R})$.

Check:

$$\begin{pmatrix} 1 & a \\ 0 & 1 \end{pmatrix} \begin{pmatrix} 1 & b \\ 0 & 1 \end{pmatrix} = \begin{pmatrix} (1\ a)\binom{1}{0} & (1\ a)\binom{b}{1} \\ (0\ 1)\binom{1}{0} & (0\ 1)\binom{b}{1} \end{pmatrix}$$

$$= \begin{pmatrix} 1 & a+b \\ 0 & 1 \end{pmatrix} \in H$$

closed ✓.

$\begin{pmatrix} 1 & 0 \\ 0 & 1 \end{pmatrix} \in H$ ✓ identity

$\begin{pmatrix} 1 & a \\ 0 & 1 \end{pmatrix}^{-1} = \begin{pmatrix} 1 & -a \\ 0 & 1 \end{pmatrix} \in H$ ✓ inverse.

eg Cyclic Subgroups

Let G = finite group, $g \in G$.

$\exists!$ way to bracket $\underbrace{ggg\cdots g}_{n \text{ times}}$.

Call it g^n.

Define $g^0 = e$. Define $g^{-n} := (g^{-1})^n$.

The list

$$e, g, g^2, g^3, \ldots\ldots$$

cannot be infinite since $|G| < \infty$.

Hence $\exists\, k < l$ such that

$$g^k = g^l.$$

Multiply (left or right) by g^{-k}

$$g^k = g^l$$
$$g^{k} g^{-k} = g^{l} g^{-k}$$
$$e = g^{l-k}$$

Conclusion: $\exists$ integer $n > 0$ s.t. $g^n = e$.
The smallest such is called the "order" of $g \in G$.

Say $g \in G$ has order r. The powers of g repeat.

$$e, g, g^2, \cdots, g^{r-1}, e, g, g^2, \cdots, g^{r-1}, \text{etc.}$$

Let $\langle g \rangle := \{ e, g, g^2, \cdots, g^{r-1} \} \subseteq G$.

Claim: $\langle g \rangle$ is a subgroup called the cyclic subgroup generated by g.

$|\langle g \rangle| = r$, the "order" of g.

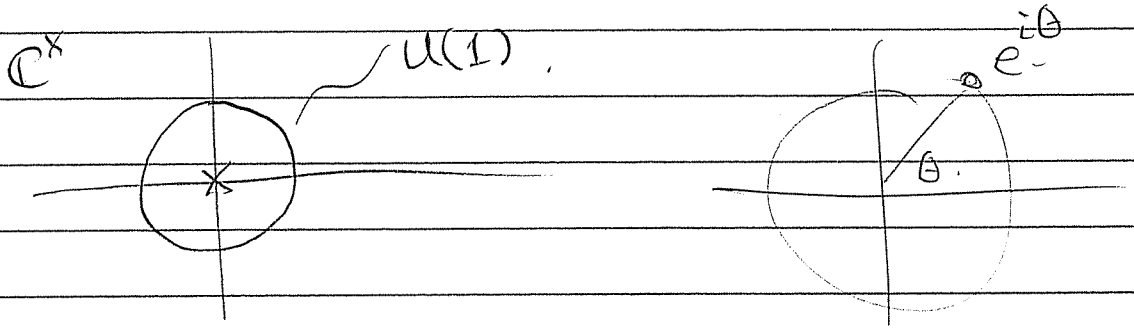
HW 1.3.
For $a, b \in G$ show that

$$|\langle ab \rangle| = |\langle ba \rangle|.$$

eg $U(1) := \{ z \in \mathbb{C} : |z| = 1 \}$

is a subgroup of

$\mathbb{C}^\times := \{ z \in \mathbb{C} : |z| \neq 0 \} = GL_1(\mathbb{C})$



Note $U(1) = \{ e^{i\theta} : \theta \in \mathbb{R} \}$

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

$e^{i\alpha} e^{i\beta} = e^{i(\alpha+\beta)}$.

Q: Is $U(1) < GL_1(\mathbb{C}) = \mathbb{C}^\times$ a cyclic subgroup? NO.

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

let $\omega = e^{2\pi i/n} = \cos\left(\frac{2\pi}{n}\right) + i\sin\left(\frac{2\pi}{n}\right)$

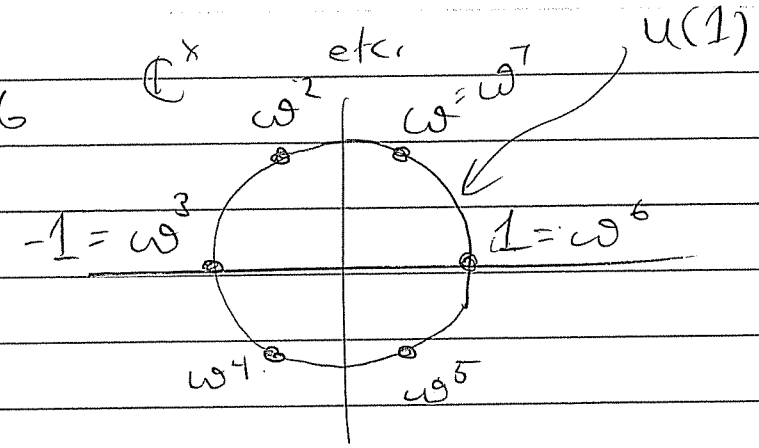
Then $\omega^k = e^{2\pi i k/n} = \cos\left(\frac{2\pi k}{n}\right) + i\sin\left(\frac{2\pi k}{n}\right)$.

de Moivre's Theorem.

and $\langle \omega \rangle = \{ 1, \omega, \omega^2, \cdots, \omega^{n-1} \}$

is a cyclic sbgp. of $U(1)$.

Pic: for $n=6$



Notation:

$\langle \omega \rangle$ = group of nth roots of unity.

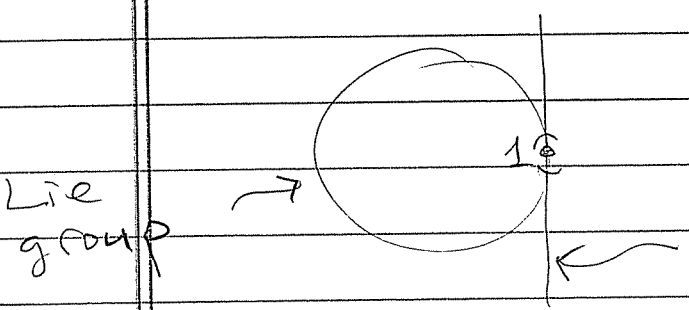
If $|G| = \infty$ we can still define cyclic subgroups.

$$\langle g \rangle := \{\ldots, g^{-2}, g^{-1}, e, g, g^2, \ldots\}$$

↑ the smallest sbgp. of G containing g.

Check: $\langle g \rangle = \bigcap_{\substack{H < G \\ g \in H}} H$

($u(1)$ is still not cyclic.
It's generated by an infinitesimal neighborhood of 1.)



eg Consider $\mathbb{Z}^+ = (\mathbb{Z}, +)$.
Given $a \in \mathbb{Z}^+$ we have

$$\langle a \rangle = \{\ldots, -2a, -a, 0, a, 2a, 3a, \ldots\}$$
$$= a\mathbb{Z}$$

- We say $a\mathbb{Z}$ instead of $\langle a \rangle$.
- In an additive group we say

$$\underbrace{a + a + \cdots + a}_{n \text{ times}} = na$$

NOT a^n.

In fact, $\mathbb{Z}^+$ itself is a cyclic group.

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

Fact: Every subgroup of a cyclic group is cyclic.
Proof: I.O.U.

(Prop 2.4) Special Case: Every subgroup of $\mathbb{Z}^+$ has the form $a\mathbb{Z}$ for some $a \in \mathbb{Z}$.

Proof: Let $H \leq \mathbb{Z}^+$ be a subgroup.
If $H = \{0\}$ then $H = 0\mathbb{Z}$. triv. sbgp.
If $H = \mathbb{Z}$ then $H = 1\mathbb{Z}$. full sb. gp.
In either case, we're done.

So sp. $H \neq 0\mathbb{Z}$ and let a be smallest positive element of H.

Because H is a group we have

$a\mathbb{Z} \subseteq H$.
$(a \in H \Rightarrow ka \in H \ \forall k \in \mathbb{Z})$.

Want to show $H \subseteq a\mathbb{Z}$.
So consider any $n \in H$ and divide by a to get

$$n = qa + r, \quad 0 \leq r < a.$$

Since $n, qa \in H$ we have
$r = n - qa \in H$.

But $r \in H$ and $0 \leq r < a \Rightarrow r = 0$.
(because $a \in H$ is smallest)

Hence $n = qa \in a\mathbb{Z}$.
and we conclude that $H \subseteq a\mathbb{Z}$

∎