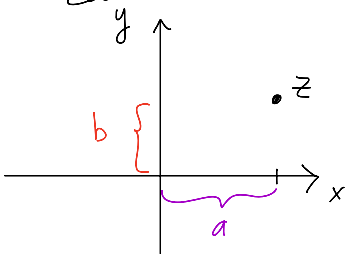
Document last updated: Fri, Oct 11 2024

Abstract Algebra Notes Week 6 Wed, Oct 9 2024

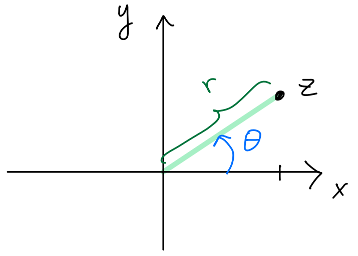
Group of complex numbers (Sec 4.2)

$\mathbb{C} = \{\text{complex numbers}\} = \{\underset{\text{real part}}{a} + \underset{\text{imaginary part}}{bi} : a, b \in \mathbb{R}\}$ where $i^2 = -1$

Cartesian/rectangular coordinates



polar coordinates



$$z = a + bi = r(\cos\theta + i\sin\theta) = re^{i\theta}$$

$$r = |z| = \sqrt{a^2+b^2},$$

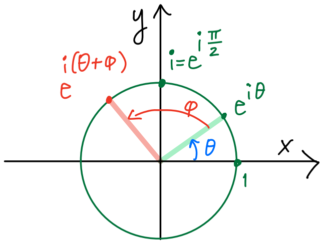
called absolute value or modulus or magnitude of z

$$a = r\cos\theta$$
$$b = r\sin\theta$$

Thm ① $e^{i\theta}e^{i\varphi} = e^{i(\theta+\varphi)}$

② If $z = re^{i\theta}$ then $z^n = r^n e^{in\theta}$

③ $(Ae^{i\theta})(Be^{i\varphi}) = ABe^{i(\theta+\varphi)}$



Def $\mathbb{C}^* \overset{\text{def}}{=} \mathbb{C}\setminus\{0\}$ is a group w/ multiplication as group operation.

Identity: 1

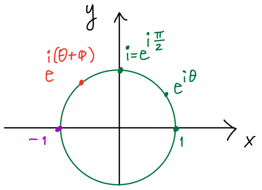
The inverse of $z = a+bi = Re^{i\theta}$ is $z^{-1} = \frac{a-bi}{a^2+b^2} = \frac{1}{R}e^{-i\theta}$

Some subgroups of $\mathbb{C}^*$:

① $\mathbb{R}^* = \mathbb{R} \setminus \{0\}$

② $\mathbb{Q}^* = \mathbb{Q} \setminus \{0\}$

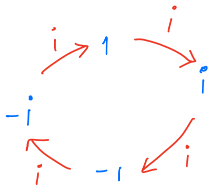
③ The circle group $\mathbb{T} \overset{\text{def}}{=} \{z \in \mathbb{C} : |z| = 1\}$

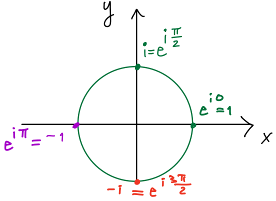


$\mathbb{T}$ contains $1, -1, i, -i, \frac{\sqrt{3}}{2} + \frac{1}{2}i = \cos(\frac{\pi}{6}) + i\sin(\frac{\pi}{6}) = e^{i\frac{\pi}{6}}$

All of these subgroups above have infinite order

④ The subset $H = \{1, -1, i, -i\}$ of the circle group is a subgroup. It's a cyclic group generated by i or $-i$.





Note that each elt of H satisfies the equation $z^4 = 1$

Def/Thm If $n \geq 2$, the <u>n-th roots of unity</u> are the complex numbers satisfying the equation $z^n = 1$.

$$\{n\text{-th roots of unity}\} = \{e^{i\frac{2\pi k}{n}} : k = 0, 1, 2, \dots, n-1\}$$

The n-th roots of unity form a cyclic group of $\mathbb{T}$ of order n. A generator for this group is called a <u>primitive n-th root of unity</u>.

Ex: $\{5\text{th roots of unity}\} = \{1, e^{i\frac{2\pi}{5}}, e^{i\frac{4\pi}{5}}, e^{i\frac{6\pi}{5}}, e^{i\frac{8\pi}{5}}\}$

All 5-th roots of unity (except 1) is primitive.

Ex: i and $-i$ are primitive 4 th roots of unity.

Homomorphisms & isomorphisms (Ch 9 and 11)

Def Let $f : A \to B$ be a function.

$\ast$ The *image* of f, denoted $\operatorname{Im} f$ or $f(A)$ is the subset $\{f(a) : a \in A\}$ of B

$\ast$ Let $C \subset B$.

— The *preimage* of C under f, denoted $f^{-1}(C)$ is the subset $\{a \in A : f(a) \in C\}$ of A.

— When C is a singleton set $C = \{b\}$, the preimage $f^{-1}(\{b\}) = \{a \in A : f(a) = b\}$ is called the *fiber* of b under f.

Def Let $(G, \ast)$ and $(H, \square)$ be groups.

A (group) *homomorphism* is a function

$\overset{\text{phi}}{\varphi} : \overset{\text{domain}}{G} \longrightarrow \overset{\text{codomain}}{H}$ such that

$$\varphi(g_1 \underset{\substack{|\\ \text{operation}\\ \text{in } G}}{\ast} g_2) = \varphi(g_1) \underset{\substack{|\\ \text{operation}\\ \text{in } H}}{\square} \varphi(g_2) \quad \text{for all } g_1, g_2 \in G.$$

$\ast$ If the homomorphism is also a bijection, then φ is called an *isomorphism* and we write $G \cong H$ and say *G is isomorphic to H*.

$\ast$ An isomorphism from G to itself is called an *automorphism* of G.

$\ast$ The *kernel of φ* is $\varphi^{-1}(\{e_H\}) = \{g \in G : \varphi(g) = e_H\}$

- Notation : $\operatorname{Ker} \varphi$

Ex $\varphi : \mathbb{Z} \longrightarrow D_4$ defined by

$$k \longmapsto R^k \quad \text{where } R \text{ is a rotation by } \frac{2\pi}{4} \text{ in } D_4$$

is a homomorphism which is not injective and not surjective.

Proof

* φ is a homomorphism: For all $k, l \in \mathbb{Z}$, we have

$$\varphi(k+l) = R^{k+l} = R^k R^l = \varphi(k)\varphi(l).$$

* It's not injective, e.g. $\varphi(2) = R^2 = R^4 R^2 = R^6 = \varphi(6)$ but $2 \neq 6$ in $\mathbb{Z}$.

* It's also not surjective: $\varphi(\mathbb{Z})$ doesn't contain any reflection. □

Note

$\ker \varphi = 4\mathbb{Z} = \{\dots, -4, 0, 4, 8, \dots\}$

$\operatorname{Im} \varphi = \{\text{Rotations by } 0, \frac{\pi}{2}, \pi, \frac{3\pi}{2}\}$

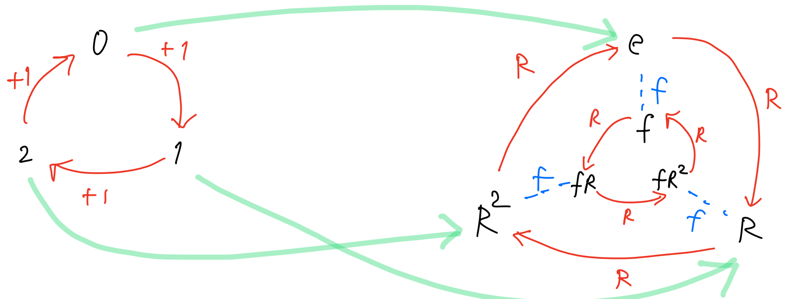
Ex $\varphi : \mathbb{Z}_3 \longrightarrow D_3$ defined by

$k \longmapsto R^k$ where R is a rotation by $\frac{2\pi}{3}$ in D_3

is an injective homomorphism which is not surjective.

Visualization

$\mathbb{Z}_3 = \langle 1 \rangle$ $D_3 = \langle R, f \rangle$ one of the flips



$0 \longmapsto e$

$1 \longmapsto R$

$2 \longmapsto R^2$

Remark D_3 contains a subgroup $\langle R \rangle = \{e, R, R^2\}$ which is "identical in structure" to $\mathbb{Z}_3$.

We say "the structure of $\mathbb{Z}_3$ shows up in D_3".

We say "$\mathbb{Z}_3$ embeds into D_3 as a subgroup".

Def An injective homomorphism is also called an embedding

(A surjective homomorphism also has a special visual and name, but we need more background before we're ready to discuss it)

Thm 1 Suppose $G = \langle a \rangle$ is a cyclic group.

(Thm 9.7 & 9.8) Then either a has infinite or finite order n.

If $|a| = \infty$ then $\varphi: \mathbb{Z} \to G$, $k \mapsto a^k$

is an isomorphism.

Proof $$\varphi(k+l) = a^{k+l} \overset{\text{exponent laws}}{\overset{?}{=}} a^k a^l = \varphi(k)\varphi(l)$$

so φ is a homomorphism.

To show φ is injective: Let $\varphi(k) = \varphi(l)$

$$\text{Then } a^k = a^l$$

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

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

Since a is of infinite order, $k-l$ must be 0, so $k=l$. □

To show φ is surjective: Every elt of G is of the form a^k for some $k \in \mathbb{Z}$, so $\varphi(k) = a^k$.

Similarly, if $|a| = n$ then $\varphi: \mathbb{Z}_n \to G$, $k \mapsto a^k$

is an isomorphism. □

Ex $U(9) = \{1, 2, 4, 5, 7, 8\} = \langle 2 \rangle$

Since the order of 2 in $U(9)$ is 6,

$U(9) \cong \mathbb{Z}_6$.

Prop Let G, H, K be groups.

① $\mathrm{id}_G : G \longrightarrow G$ is an isomorphism
$x \longmapsto x$

[Pf: id_G a homomorphism: $\mathrm{id}_G(ab) = ab = \mathrm{id}_G(a)\, \mathrm{id}_G(b)$. ✓
id_G a bijection. ✓]

② If $\varphi : G \to H$ is an isomorphism, then the inverse bijection φ^{-1} is also an isomorphism.

[Pf The inverse bijection φ^{-1} is a bijection. ✓

Given $c, d \in H$, $c = \varphi(a)$ and $d = \varphi(b)$ for some $a, b \in G$ since φ is a bijection.

Then $\varphi(ab) = \varphi(a)\ \varphi(b)$ since φ is a homomorphism
$= c \quad d$

So $\varphi^{-1}(cd) = ab = \varphi^{-1}(c)\, \varphi^{-1}(d)$, and thus φ^{-1} is a homomorphism. ✓ □]

③ (The composition of two isomorphisms is also an isomorphism)

If $\overset{\text{phi}}{\varphi} : G \to H$ and $\overset{\text{psi}}{\psi} : H \longrightarrow K$ are isomorphisms, then $\psi \circ \varphi : G \longrightarrow K$ is an isomorphism.

[Proof Composition of bijections is a bijection. ✓

For $a, b \in G$, $\psi(\varphi(ab)) = \psi(\varphi(a)\varphi(b))$ since φ is a homomorphism
$= \psi(\varphi(a))\, \psi(\varphi(b))$ since ψ is a homomorphism. ✓]

Remark The set $\mathrm{Aut}(G) \overset{\text{def}}{=} \{\text{automorphisms of } G\}$ forms a group under composition. It's called the automorphism group of G.

Prop $\cong$ is an equivalence relation on the set of all groups.

Proof ① (reflexivity) $G \cong G$ since id_G is an isomorphism

② (symmetry) If $G \cong H$ then $H \cong G$

since if $\varphi: G \to H$ is an isomorphism
then $\varphi^{-1}: H \to G$ is an isomorphism

③ (transitivity) If $G \cong H$ and $H \cong K$ then $G \cong K$

since if $\overset{\text{phi}}{\varphi}: G \to H$ and $\overset{\text{psi}}{\psi}: H \to K$ are isomorphisms,
then $\psi \circ \varphi: G \to K$ is an isomorphism. □

The equivalence classes of $\cong$ are called isomorphism classes.

Goal: Classify all groups up to isomorphism,
i.e. describe all isomorphism classes.

Thm 2
Up to isomorphism, there is only one cyclic group of infinite order
and only one cyclic group of order n

Pf $\boxed{\text{Thm 1}}$ tells us that all cyclic groups of infinite order are isomorphic to $\mathbb{Z}$, and all cyclic groups of order n are isomorphic to $\mathbb{Z}_n$. □

Thm 3 Up to isomorphism, there is only one group of prime order,
the isomorphism class containing $\mathbb{Z}_p$.

Def $V_4 = \{e, a, b, c\}$ is the group w/
multiplication (Cayley) table

	e	a	b	c
e	e	a	b	c
a	a	e	c	b
b	b	c	e	a
c	c	b	a	e

Thm 4 Up to isomorphism, there are two groups of order 4, $\mathbb{Z}_4$ and V_4.

Ex Other groups isomorphic to $\mathbb{Z}_4$:

- $\{ Id, R, R^2, R^3 \} \leq D_4$

  Rot(90°)

- $\{ Id, (1263), (16)(23), (3621) \} = \langle (1263) \rangle = \langle (3621) \rangle$ from Quiz 03
- $U(5) = \{1, 2, 3, 4\} = \langle 2 \rangle = \langle 3 \rangle$ from Quiz 02

Other groups isomorphic to V_4:

- the 2-light switch group from Day 1
- $\mathbb{Z}_2 \times \mathbb{Z}_2 = \{ (00), (10), (01), (11) \}$
- $U(8)$
- $U(12)$
- $\{ Id, R, f, fR^2 \} \leq D_4$

  Rot(90°) any flip

- $\{ Id, (12)(34), (13)(24), (14)(23) \} \leq S_4$

Proof of Thm 4 Suppose G is a group of order 4.

Case 1: G contains an elt g of order 4.

Then $\langle g \rangle$ is a subgroup of order 4, so $\langle g \rangle = G$.

Every cyclic group of order 4 is isomorphic to $\mathbb{Z}_4$ by $\boxed{\text{Thm 2}}$. □

Case 2: G contains no elt of order 4.

By Lagrange's Thm, $|g| = 2$ for all non-identity $g \in G$.

So $g^{-1} = g$ for all $g \in G$.

Claim: If $x, y \in G$ are distinct non-identity elts,
then xy is the third non-identity elt.

Proof of claim: Suppose x, y are distinct non-identity elts in G.

If $xy = e$ then $y = x^{-1} = x$, giving a contradiction.

If $xy = x$ then $y = e$, giving a contradiction.

If $xy = y$ then $x = e$, giving a contradiction.

So xy must be the third non-identity elt.

So this group has the same multiplication table as V_4.
Thus $G \cong V_4$.

Claim: $\mathbb{Z}_4$ is not isomorphic to V_4

Pf Suppose $\mathbb{Z}_4 \longrightarrow V_4$ is an isomorphism.

Case $\varphi(1) = e$: Then $\varphi(2) = \varphi(1+1) = \varphi(1)\varphi(1) = ee = e = \varphi(1)$.

Having $\varphi(2) = \varphi(1)$ means φ is not injective.

So $\varphi(1) \neq e$.

Case $\varphi(1) \neq e$: Then $\varphi(1) = x$ where $x = a, b,$ or c.

$$\begin{aligned}
\text{Then } \varphi(3) &= \varphi(1+1+1) \\
&= \varphi(1)\varphi(1)\varphi(1) \\
&= x^3 = x^2 x \\
&= x \quad \text{since } |x| = 2 \\
&= \varphi(1)
\end{aligned}$$

Having $\varphi(3) = \varphi(1)$ means φ is not injective.

In both cases, φ is not a bijection.

So there is no isomorphism from $\mathbb{Z}_4$ to V_4 $\boxed{\text{claim}}$

— end of Proof of Thm 4 —

(Extra notes)

Prop Let $\varphi : G \to H$ be a homomorphism of groups.

(Prop 11.4 & Thm 11.5)

① φ sends e_G to e_H

② For each $x \in G$, $\varphi(x^{-1}) = [\varphi(x)]^{-1}$

③ If K is a subgroup of G then the image $\varphi(K)$ is a subgroup of H.

④ If J is a subgroup of H then the preimage $\varphi^{-1}(J)$ is a subgroup of G.

⑤ $\operatorname{Ker} \varphi$ is a subgroup of G

Proof ① to ④: (Prop 11.4)

Proof of ⑤: * The identity $e_G \in \ker \varphi$ since $\varphi(e_G) = e_H$ by ①

* (Closure) Suppose $x, y \in \ker \varphi$. Then $\varphi(xy) = \varphi(x)\varphi(y) = e_H e_H = e_H$, so $xy \in \ker \varphi$.

* (Inverses) Given $x \in \ker \varphi$, we need to show that $x^{-1} \in \ker \varphi$:

$$\varphi(x^{-1}) = [\varphi(x)]^{-1} \quad \text{by ②}$$
$$= (e_H)^{-1} \quad \text{since } x \in \ker \varphi$$
$$= e_H.$$

Cor If $\varphi : G \to H$ is an injective group homomorphism then $G \cong \varphi(G)$.