Lecture 5

Last time: classified cyclic subgroups.

The main proposition from last time:

Prop. G a group, $x \in G \rightsquigarrow \langle x \rangle_G = \{x^k \mid k \in \mathbb{Z}\}$

Then:

Case 1 $\langle x \rangle_G = \{1, x, \dots, x^{n-1}\}$

all distinct

multiplication as in $\mathbb{Z}/n\mathbb{Z}$ (identify $x^k \leftrightarrow k$)

We define $\operatorname{ord}(x) := \#\langle x \rangle_G = n$

Case 2 $\langle x \rangle_G = \{\dots x^{-1}, 1, x, x^2, \dots\}$

all distinct

multiplication as in $\mathbb{Z}$ (identify $x^k \leftrightarrow k$)

$\operatorname{ord}(x) := \infty$

Examples:

(1) S_3 $\quad x = (123)$, $\langle x \rangle = \{1, (123), (132)\}$
$\qquad\qquad\qquad\qquad\qquad\qquad\qquad\quad = \{1, x, x^2\}$

order of x is $\underline{3}$

$y = (12)$, $\quad \langle y \rangle = \{1, (12)\}$
$\qquad\qquad\qquad\qquad\quad = \{1, y\}$

order of y is $\underline{2}$

(2) $(\mathbb{Z}/6\mathbb{Z}, +)$

$\underline{1} \rightsquigarrow \langle 1 \rangle = \mathbb{Z}/6\mathbb{Z}$

order of 1 is $\underline{6}$

$2 \rightsquigarrow \langle 2 \rangle = \{2, 4, 0\}$, $\quad ord(2) = \underline{3}$

$3 \rightsquigarrow \langle 3 \rangle = \{3, 0\} \Rightarrow ord(3) = \underline{2}$

$4 \rightsquigarrow \langle 4 \rangle = \{4, 2, 0\} \Rightarrow ord(4) = \underline{3}$

$5 \rightsquigarrow \langle 5 \rangle = \{5, 4, 3, 2, 1, 0\} \Rightarrow ord(5) = \underline{6}$

Question: take $m \in \mathbb{Z}/n\mathbb{Z}$, $\operatorname{ord}(m) = ???$

③ $(\mathbb{Q}, +)$, $\frac{2}{3} \in \mathbb{Q}$, $\operatorname{ord}\left(\frac{2}{3}\right) = \infty$

④ $(\mathbb{Z}/12\mathbb{Z})^\times \leftarrow \{1, 5, 7, 11\}$

every element (not equal to 1) has order = 2

·	1	5	7	11
1	1	5	7	11
5	5	1	11	7
7	7	11	1	5
11	11	7	5	1

Exercise: if S a group that contains ≤ 3 elements then S a cyclic (generated by one element)

Exercise $(\mathbb{Z}/12\mathbb{Z})^\times = \langle a, b \rangle / a^2 = b^2 = (ab)^2 = 1$

Question: in what sense are two cyclic groups of order n **the same**?

How to formalize this?

Answer: they are **isomorphic**

Homomorphisms

G, G' — two groups

A **homomorphism** $\varphi: G \to G'$ is a map such that:

$$\varphi(ab) = \varphi(a)\,\varphi(b)$$

(φ of multiplication in G = φ of a, φ of b, multiplication in G')

isomorphism — **bijective** homomorphism

Examples

"trivial homomorphism"

$G \to G', \quad g \mapsto e_{G'}$ ← not an iso (in general)

"identity"

$G \xrightarrow{id} G, \quad g \mapsto g$ ← iso

$\mathbb{Z} \to \mathbb{Z}, \quad m \mapsto 2m$ ← not an iso

not an iso

$\mathbb{Z} \to \mathbb{Z}/n\mathbb{Z}, \quad m \mapsto m \bmod n$

$(\mathbb{R}, +) \to (\mathbb{R}^{\times}, \cdot), \quad t \xmapsto{\varphi} e^t$ ← iso!

$\varphi(t_1+t_2) = e^{t_1+t_2} = e^{t_1} \cdot e^{t_2} = \varphi(t_1)\varphi(t_2)$

$S_3 \hookrightarrow S_4; \quad \sigma \mapsto \begin{bmatrix} 1 & 2 & 3 & 4 \\ \sigma(1) & \sigma(2) & \sigma(3) & 4 \end{bmatrix}$

$= \begin{bmatrix} 1 & 2 & 3 \\ \sigma(1) & \sigma(2) & \sigma(3) \end{bmatrix}$

not an iso

Basic properties of homomorphisms

Proposition Let $\varphi: G \to G'$ ← homomorphism

(a) If $a_1, \dots, a_k \in G$ then $\varphi(a_1 \dots a_k) = \varphi(a_1) \dots \varphi(a_k)$

(b) $\varphi(e_G) = e_{G'}$

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

Proof (a) ← exercise (use induction!)

+

$a_1 \dots a_n = (a_1 \dots a_{n-1}) \cdot (a_n)$

Sketch: $\varphi(a_1 \dots a_n) = \varphi((a_1 \dots a_{n-1}) \cdot (a_n)) = \varphi(a_1 \dots a_{n-1}) \cdot \varphi(a_n) =$

$\overset{\text{induction}}{=\!=} (\varphi(a_1) \dots \varphi(a_n)) \cdot (\varphi(a_n)) = \varphi(a_1) \dots \varphi(a_n)$

(b) Want to check that $\varphi(e_G) = e_{G'}$

Know: $e_G \cdot e_G = e_G$

$\Downarrow$

$\varphi(e_G \cdot e_G) = \varphi(e_G)$

$\varphi(e_G) \cdot \varphi(e_G) = \varphi(e_G)$ (cancellation law)

$\Downarrow$

$\varphi(e_G) = e_{G'}$ ✓

(c) Want: $\varphi(a^{-1}) = \varphi(a)^{-1}$?

Need to check:

$$\underbrace{\varphi(a^{-1}) \cdot \varphi(a)}_{\varphi(a^{-1} \cdot a) = \varphi(e_G) = e_{G'}} = e_{G'} = \underbrace{\varphi(a) \cdot \varphi(a^{-1})}_{\varphi(a \cdot a^{-1}) = \varphi(e_G) = e_{G'}}$$

✓ ✓

Isomorphisms

Recall: $\varphi: G \to G'$ is an isomorphism if

- φ is homomorphism
- φ is bijective

Lemma if $\varphi: G \to G'$ is isomorphism, then $\varphi^{-1}: G' \to G$ is an isomorphism

proof Need to check that:

$$\varphi^{-1}(xy) = \varphi^{-1}(x)\varphi^{-1}(y) \quad \forall x, y \in G'$$

(xy: mult. in G'; $\varphi^{-1}(x)\varphi^{-1}(y)$: mult. in G)

Set $a := \varphi^{-1}(x)$; $b := \varphi^{-1}(y)$; $c := \varphi^{-1}(xy)$

$c = ab$ ← want to check this

φ is bijective, so enough to check:

$$\varphi(c) = \varphi(ab)$$

Indeed: $\varphi(ab) = \varphi(a)\varphi(b) = xy = \varphi(c)$ ✓

Two groups G, G' are <u>isomorphic</u> if $\exists\, \varphi : G \xrightarrow{\sim} G'$. We will write $G \simeq G'$.

↑ <u>isomorphism</u>

Warning: isomorphism is <u>NOT</u> unique in general!

Example: $S_3 \xrightarrow{\sim} S_3$; $x \mapsto (12)\cdot x \cdot (12)$ ← nontrivial identification of S_3 with itself

Examples (of isomorphic and not isomorphic groups)

$(\mathbb{Z}^\times, \cdot) = \{\pm 1\} \simeq \mathbb{Z}/2\mathbb{Z}$

$1 \longmapsto 0$

$-1 \longmapsto 1$

S_3

$\cup$

$\langle (123) \rangle \simeq \mathbb{Z}/3\mathbb{Z}$

$\wr$

$1 \longmapsto 0$

$(123) \longmapsto 1$

$(132) \longmapsto 2$

NOT isomorphic

note that both contain 4 elements

$(\mathbb{Z}/12\mathbb{Z})^\times \not\simeq \mathbb{Z}/4\mathbb{Z}$

↑ every element has order ≤ 2

↑ has element of order 4

More examples

$\{1, x, \dots, x^{n-1}\}$

$x \in G$, $\operatorname{ord}(x) = n \Rightarrow \langle x \rangle_G \simeq \mathbb{Z}/n\mathbb{Z}$

$x^k \longmapsto k$

$x \in G$, $\operatorname{ord}(x) = \infty \Rightarrow \langle x \rangle_G \simeq \mathbb{Z}$

We see that two isomorphic groups are "the same" and we do not want to distinguish them.

- The groups isomorphic to a given group G from what is called isomorphism class of G.

Lemma: if $G_1 \simeq G_2$, $G_2 \simeq G_3 \Rightarrow G_1 \simeq G_3$

in other words, any two groups in the isomorphism class are isomorphic

~~Proof~~

Lemma above follows from the following general claim.

Claim if $\varphi: G \to H$; $\Psi: H \to S$ homomorphisms of groups

then $\Psi \circ \varphi$ is a homomorphism

Proof $(\Psi \circ \varphi)(ab) = \Psi(\varphi(ab)) =$

$= \Psi(\varphi(a)\varphi(b)) = \Psi(\varphi(a))\Psi(\varphi(b)) =$

$= (\Psi \circ \varphi)(a) \cdot (\Psi \circ \varphi)(b)$ ✓

Very big problem: classify all groups

too hard! i.e., describe their isomorphism classes

Will see: every group of order p is $\simeq \mathbb{Z}/p\mathbb{Z}$

Question: can you describe groups of order 4?