Math 122 19 September 2003

§ The story so far

1) Groups are everywhere.
   Examples – $GL_n(\mathbb{R})$; S_n; $(\mathbb{Z}, +)$ (from previous lectures)
   – all are types of structure-preserving bijections
2) Making new groups – ~~subgroups~~ (similar to vector subspaces)
   Ex: $\mathrm{Hom}(\mathbb{R}^n, \mathbb{R}^n)$ is a vector space; and $\mathrm{Aut}(G)$ is a group
   (the automorphisms of a group G)
3) Subgroups of $\mathbb{Z}$ – all have form $b\mathbb{Z}$, $b \in \mathbb{Z}_{\geq 0}$. (use Euclidean algorithm)
4) Cyclic subgroup – powers of one element

   Ex: $\left\langle \begin{pmatrix} 1 & 1 \\ 0 & 1 \end{pmatrix} \right\rangle = \left\{ \begin{pmatrix} 1 & 1 \\ 0 & 1 \end{pmatrix}^n \middle| n \in \mathbb{Z} \right\} = \begin{pmatrix} 1 & n \\ 0 & 1 \end{pmatrix}$, $n \in \mathbb{Z}$
   $\cap$
   $GL_2(\mathbb{R})$ – has infinite order $\left(\begin{pmatrix} 1 & 1 \\ 0 & 1 \end{pmatrix}^n \neq I \text{ for any } n > 0 \right)$

   $\left| \left\langle \begin{pmatrix} -1 & 0 \\ 0 & -1 \end{pmatrix} \right\rangle \right| = 2$, (order 2) since $\begin{pmatrix} -1 & 0 \\ 0 & -1 \end{pmatrix}^2 = I$

§ Isomorphisms

Consider
1) $G_1 = \{\pm 1, \pm i\} \subset \mathbb{C}^\times$
2) Consider subgroup $\langle \rho \rangle \subset S_4$, where ρ is:  (~~cycles elem~~

   note $\rho^2 \neq e, \rho$, and $\rho^3 \neq e, \rho, \rho^2$.
   However $\rho^4 = e$. So the mult. table for $\langle \rho \rangle$ is:

	e	ρ	ρ^2	ρ^3
e	e	ρ	ρ^2	ρ^3
ρ	ρ	ρ^2	ρ^3	e
ρ^2	ρ^2	ρ^3	e	ρ
ρ^3	ρ^3	e	ρ	ρ^2

– so G_1 and $\langle \rho \rangle$ are in fact "the same" group, b/c if we relabel i as ρ, we have the mult. table at right
i.e., $i^4 = 1$ $(= e)$, but $i^3 \neq e, i, i^2$ + $i^2 \neq e, i$.

<u>Def:</u> an <u>Isomorphism</u> $f: G_1 \to G_2$ is a bijection s.t.

$$f(x \cdot y) = f(x) \cdot f(y)$$

(multiplication in G_1 ↑, ↑ multiplication in G_2)

In the example prev., $i^k \longmapsto \rho^k$; i.e., $f(i^k) = \rho^k$

<u>Fact:</u> any two cyclic groups of order n are isomorphic.

<u>Def:</u> a <u>cyclic group</u> is a Group G s.t. $G = \langle g \rangle$ for some $g \in G$

<u>Def:</u> two groups G_1, G_2 are <u>isomorphic</u> if $\exists$ an isomorphism $f: G_1 \to G_2$

<u>Pf of fact:</u> let $G_1 = \langle x_1 \rangle$, $G_2 = \langle x_2 \rangle$ and then

$f: G_1 \to G_2 \mid f(x_1^k) = x_2^k$ is a well-defined bijection,

which clearly preserves multiplication.

<u>Note:</u> There is a cyclic group of order n $\forall n$, given by the span of the cycle $\sigma_n = \begin{pmatrix} 1 & 2 & 3 & \cdots & n \\ 2 & 3 & 4 & \cdots & 1 \end{pmatrix}$ in S_n. i.e. $C_n = \langle \sigma_n \rangle \subset S_n$

<u>Example:</u> $(\underset{G_1}{\mathbb{R}}, +)$ and $(\underset{G_2}{\mathbb{R}_{>0}}, \cdot) \leftarrow$ (strictly >0 real #s under multiplication)

Are these isomorphic? <u>YES</u>

$f: G_1 \to G_2$ $f(x) = e^x$ is an isomorphism, since $\log x$ is an inverse and $e^{(x+y)} = e^x \cdot e^x$.

<u>Example:</u> Klein 4-group Two ways:

1) $G_1 : \{ e, \tau_1 = \begin{pmatrix} 1 & 2 & 3 & 4 \\ 2 & 1 & 4 & 3 \end{pmatrix}, \tau_2 = \begin{pmatrix} 1 & 2 & 3 & 4 \\ 3 & 4 & 1 & 2 \end{pmatrix}, \tau_3 = \begin{pmatrix} 1 & 2 & 3 & 4 \\ 4 & 3 & 2 & 1 \end{pmatrix} = \tau_2 \tau_1 = \tau_1 \tau_2 \} \subset S_4$

Mult. table:

	e	τ_1	τ_2	$\tau_1\tau_2$
e	e	τ_1	τ_2	$\tau_1\tau_2$
τ_1	τ_1	e	$\tau_1\tau_2$	τ_2
τ_2	τ_2	$\tau_1\tau_2$	e	τ_1
$\tau_1\tau_2$	$\tau_1\tau_2$	τ_2	τ_1	e

N.B. τ_1, τ_2 <u>commute</u>

2) $G_2 = \{ I, \begin{pmatrix} -1 & 0 \\ 0 & 1 \end{pmatrix}, \begin{pmatrix} 1 & 0 \\ 0 & -1 \end{pmatrix}, -I \} \subset GL_2(\mathbb{R})$

Consider $f: G_1 \to G_2$, an isomorphism

$\tau_1 \longmapsto \begin{pmatrix} -1 & \\ & 1 \end{pmatrix}$

$\tau_2 \longmapsto \begin{pmatrix} 1 & \\ & -1 \end{pmatrix}$

$\tau_1 \tau_2 \longmapsto -I$

$e \longmapsto I$

Note: we can talk about V, "the" Klein 4-group

⟶

Non-example: is V isomorphic to C_4?

No. in V, $\nexists$ an element of order 4

Some properties of isomorphic groups:

1) $|G_1| = |G_2|$ (same # of elements)
2) G_1 abelian $\Longleftrightarrow$ G_2 abelian
3) G_1, G_2 have the same # of elts. of every order

Given G, we can construct $\mathrm{Aut}(G)$ - the automorphisms of G, i.e. the isomorphisms from G to itself. also the "symmetries" or "structure-preserving maps" of G

$\mathrm{Aut}(G)$ is a group!

- Certainly composition of isomorphisms is an isomorphism
- identity automorphism is identity map on G
- easy exercise - verify that the inverse of an aut. is an aut.

§ Homomorphisms

Ex: $\det: GL_n(\mathbb{R}) \longrightarrow \mathbb{R}^\times = \{\mathbb{R}\setminus\{0\}, \times\}$

$\det(AB) = \det(A)\cdot\det(B)$

- not 1-1
- $\mathbb{R}^\times$ is abelian but not $GL_n(\mathbb{R})$ $\therefore$ det is not an isomorphism

Def: Homomorphisms are maps $f: G_1 \to G_2$ s.t. $f(x \cdot y) \to f(x)\cdot f(y)$

Ex: any isomorphism

Ex: the trivial hom. $f: G_1 \to G_2 \mid f(x) = e \quad \forall x \in G_1$

Ex: inclusion $S_n \hookrightarrow S_m$, $n < m$

from Wednesday: $f: S_3 \to S_n$ $(n \geq 3)$

$f\begin{pmatrix} 1 & ? & 1 \\ 2 & & 2 \\ 3 & \cdot & 3 \end{pmatrix} \to \begin{pmatrix} 1 & ? & 1 \\ 2 & & 2 \\ 3 & \cdot & 3 \\ 4 & \to & 4 \\ \vdots & \to & \vdots \\ n & \to & n \end{pmatrix}$ etc.

$\longrightarrow$

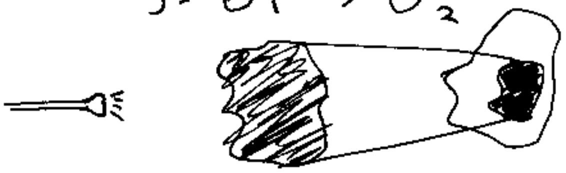
Ex: $f: \mathbb{Z} \to S_2$ clearly a homomorphism

evens $\to e$

odds $\to \tau$

§ Images

$f: G_1 \to G_2$

 $= \{ f(x) \in G_2 \mid x \in G_1 \}$

HW: (from Artin) Read §§ 2.3 + 2.4

Exerc. 2.3.1, 2.3.11, 2.3.12, 2.4.3, 2.4.6, 2.4.11