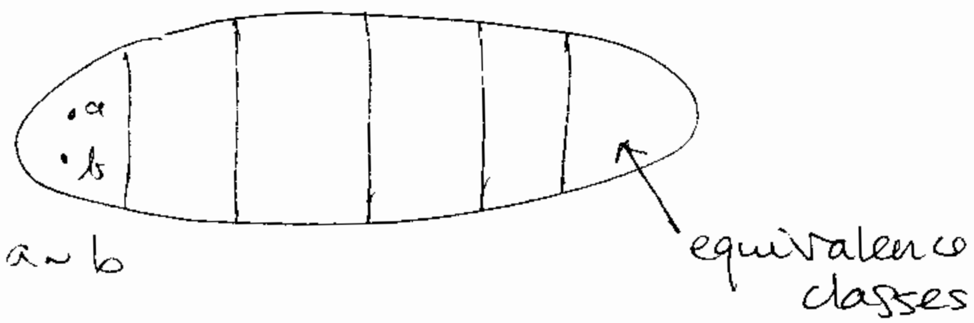
LECTURE 5

Sept. 24/2003

§ Equivalence relation on a set S

= partition into disjoint subsets



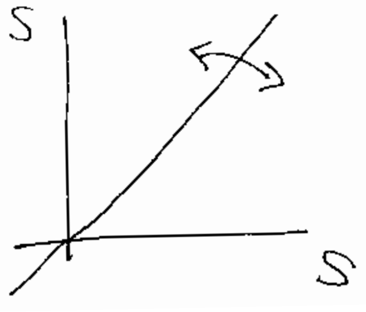
$a \sim b$

Defining properties:

- $a \sim a$
- $a \sim b \Rightarrow b \sim a$
- $a \sim b$ & $b \sim c \Rightarrow a \sim c$

Can also understand as subset of $S \times S$:

$$\{(a,b) : a \sim b\}$$

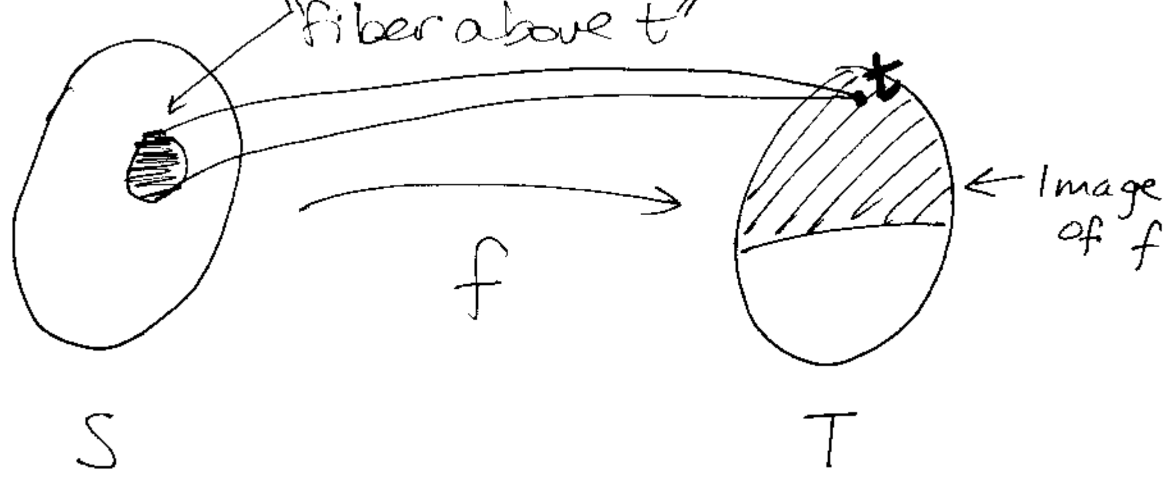


$$\begin{cases} S \longrightarrow \overline{S} = \{\text{equivalence classes in } S\} \\ a \longmapsto \overline{a} = \text{the equivalence class containing } a \end{cases}$$

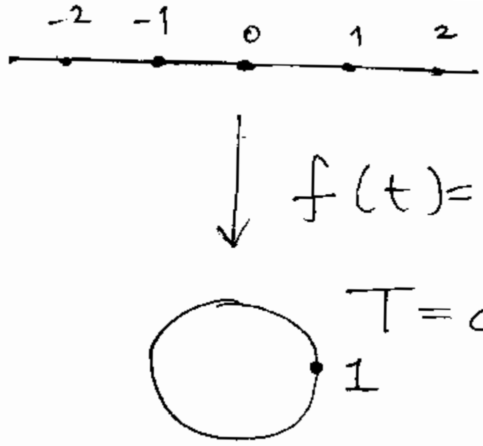
this is a surjective map of sets.

Conversely: if you have a map $f: S \to T$, this gives an equivalence relation (or partition) on S (with $\overline{S} = \text{Image}(f)$):

$$a \sim b \iff f(a) = f(b) \text{ in } T$$



Ex:



$S = \mathbb{R}$

$f(t) = e^{2\pi i t}$

$T =$ unit circle in $\mathbb{C}$

$f^{-1}(1) = \{\ldots, -2, -1, 0, 1, 2, \ldots\}$

Ex: Suppose $f : G \to G'$ a group homomorphism.

Let $H \lhd G$ be the kernel of f.

We get an equivalence relation on G, where H is one of the equivalence classes.

Why? Because $H = f^{-1}(e')$
$= \{a \in G : f(a) = f(e) = e'\}$

§ Cosets

In the above example:

__Proposition__ The other equivalence classes have the form $aH = \{ah : h \in H\}$ for some $a \in G$

__Proof:__ Say $f(a) = f(b) \in G'$ (i.e. $a \sim b$)

Then $f(a^{-1}b) = e'$ so $a^{-1}b \in H$, i.e. $a^{-1}b = h \in H$ so $b = ah$.

Conversely if $b \in aH$ is equivalent to a since
$$f(b) = f(ah) = f(a)f(h) = f(a)$$
(since $h \in H =$ kernel)

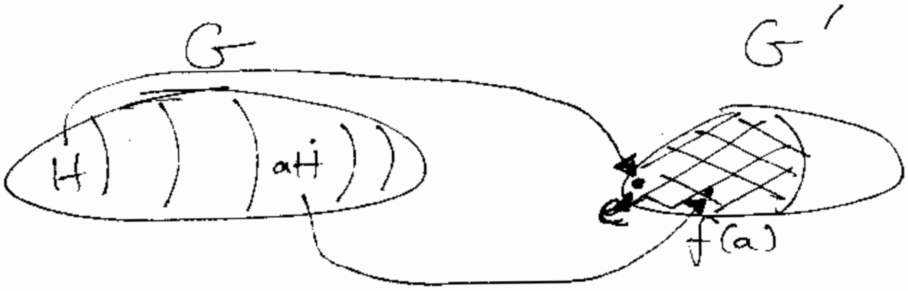
$\boxtimes$

__Terminology__: aH is called a __left coset__ of H in G

<u>Fact</u>: The map $h \mapsto ah$ gives a bijection of sets

$$H \longrightarrow aH$$

In particular,
$$|H| = |aH|$$
so for a <u>group homomorphism</u>, the equiv. classes are of the form aH, $H = \ker f$ and have the <u>same size</u>.



<u>Note</u>: This is not true for a general map of sets

__Corollary__ Assume G is finite, and $f: G \to G'$ is a hom. with kernel H.

Then $|G| = |H| \cdot |\text{Image } f|$

$$H = \ker f$$

This is analagous to result in linear algebra:

If $T: V \to W$ is a linear map, then $\dim V = \dim(\ker T) + \dim(\text{Im } T)$

__Ex__: $|S_n| = n!$

For $n \geq 2$, $|A_n| = \frac{n!}{2}$

__Pf__: $f: S_n \to \{\pm 1\}$ (sign map) is surjective for $n \geq 2$ and kernel is A_n $\boxtimes$.

More generally, let $H \subset G$ be <u>any</u> subgroup — not necessarily normal.

We define the (left) coset of $a \in G$ by $aH = \{ah : h \in H\}$

<u>Prop</u> These subsets are disjoint and partition G. Furthermore, they each are in set-theoretic bijection with H.

Define the index of H, which might be infinite, (denoted $[G:H]$) as the # of distinct left cosets (i.e. equivalence classes)

More general

<u>Corollary</u> $|G| = |H| \cdot [G:H]$

Lagrange's Thm

If $|G|$ is finite, and $g \in G$, then the order of g divides $|G|$.

Ex: You can't have an element of order 3 in a group of order 4.

Pf: Let $H = \langle g \rangle = \{e, g, \ldots, g^{m-1}\}$ (where m = order of g)

Then since $|H| \mid |G|$ by the above corollary, the result follows. $\boxtimes$.

§ Examples

Ex Let G be a finite group, with $|G| = p$. a prime #

Then G is cyclic, generated by any $g \in G$ with $g \neq e$

Furthermore, the only subgroups of G are e and G.

Proof: Let $g \neq e$ in G.
Order of g divides p and is not 1.
Since p is prime, order of $g = p$

$$\underset{\text{order } p}{\langle g \rangle} \subset \underset{\text{order } p}{G}$$

$\therefore$ These are equal.

$\boxtimes$.

Can we show that this is a strong result by exhibiting a non-cyclic group of order p^2?

Yes: Klein 4-group has order 2^2 and is not cyclic.

Similarly: S_3 has order 6, is not abelian (and certainly not cyclic)

But: all groups of order p^2 are abelian!
(Will see this later.)

Defn: A group G is simple if its only normal subgroups H are $\{e\}$ and G.

Ex: Simple groups:

1) Any G of prime order p (these are the only abelian simple groups)

2) Later we'll see: A_n for $n \geq 5$

3) Feit–Thompson theorem: Any finite non-abelian simple group has even order.