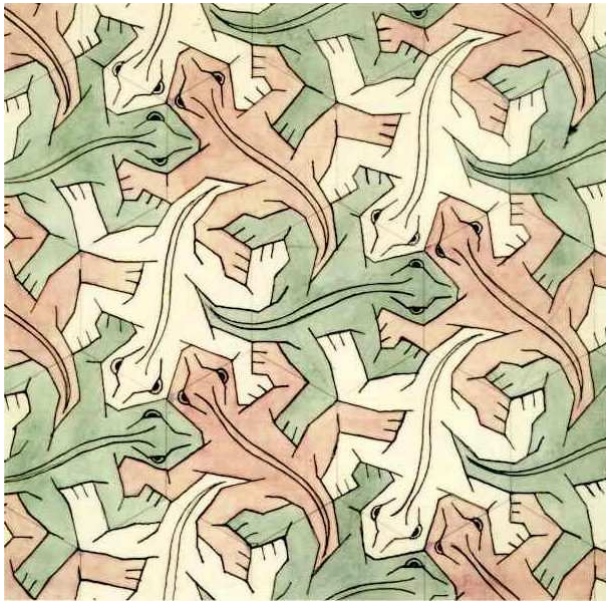
GROUP THEORY



Afra Zomorodian

CS 468 – Lecture 4

2-4-4

M. C. ESCHER

I never got a pass in math. . . . And just imagine–mathematicians now use my prints to illustrate their books.

— M. C. Escher

OVERVIEW

- Why groups?
  - Abstracting core properties
  - Representation
  - Classification
- What to take home: factor groups

ABSTRACTION

1. $5 + x = 2 \implies \mathbb{Z}-$
2. $2x = 3 \implies \mathbb{Q}$
3. $x^2 = -1 \implies \mathbb{C}$

$$
\begin{aligned}
5 + x &= 2 && \text{Given} \\
-5 + (5 + x) &= -5 + 2 && \text{Addition property of equality} \\
(-5 + 5) + x &= -5 + 2 && \text{Associative property of addition} \\
0 + x &= -5 + 2 && \text{Inverse property of addition} \\
x &= -5 + 2 && \text{Identity property of addition} \\
x &= -3 && \text{Addition}
\end{aligned}
$$

BINARY OPERATION

- A binary operation $*$ on a set S is a rule that assigns to each ordered pair (a, b) of elements of S some element in S.
- well-defined: single element
- not defined: no element
- not well-defined: multiple elements
- closed: element in S only
- associative: $(a * b) * c = a * (b * c)$ for all $a, b, c \in S$.
- commutative: $a * b = b * a$ for all $a, b \in S$.

Binary Operation Example

	a	b	c
a	a	c	c
b	a	c	b
c	b	d	c

- $S = \{a, b, c\}$

GROUPS

- A set G
- A binary operation $*$ on G such that:
  (a) $*$ is associative.
  (b) G has an identity e element for $*$:
  $e * x = x * e = x$ for all $x \in G$.
  (c) any element a has an inverse a' wrto $*$:
  $\forall a \in G, \exists a' \in G$, such that $a' * a = a * a' = e$.
- A group $\langle G, * \rangle$. Often, just G.
- If G is finite, the order of G is $|G|$.
- A group G is abelian if its binary operation $*$ is commutative.

EXAMPLE GROUPS

- $\langle \mathbb{Z}, + \rangle$?
- $\langle \mathbb{Z}, \cdot \rangle$?
- $\langle \mathbb{R}, + \rangle$?
- $\langle \mathbb{R}, \cdot \rangle$?

EXAMPLE GROUPS

- $\langle \mathbb{Z}, + \rangle$? Yes!
- $\langle \mathbb{Z}, \cdot \rangle$? No!
- $\langle \mathbb{R}, + \rangle$? Yes!
- $\langle \mathbb{R}, \cdot \rangle$? No (zero has no inverse)

$\mathbb{Z}_n$

- Let n be a fixed positive integer
- Let h and k be any integers.
- The remainder r when $h + k$ is divided by n is $h +_n k$, the sum of h and k modulo n.
- Let $\mathbb{Z}_n = \{0, 1, 2, \ldots, n-1\}$
- $\langle \mathbb{Z}_n, +_n \rangle$ is a group

SMALL GROUPS

	e	a
e	e	a
a	a	e

	e	a	b
e	e	a	b
a	a	b	e
b	b	e	a

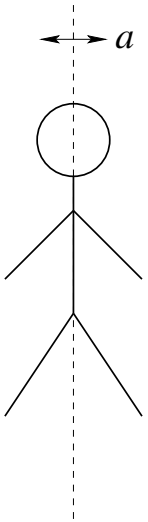
	0	1	2	3
0	0	1	2	3
1	1	2	3	0
2	2	3	0	1
3	3	0	1	2

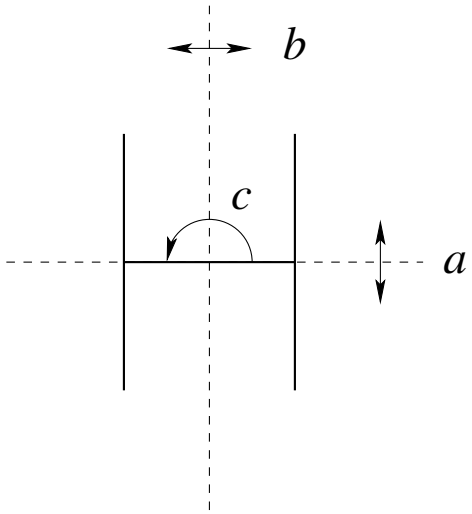
V_4	e	a	b	c
e	e	a	b	c
a	a	e	c	b
b	b	c	e	a
c	c	b	a	e

SYMMETRIES

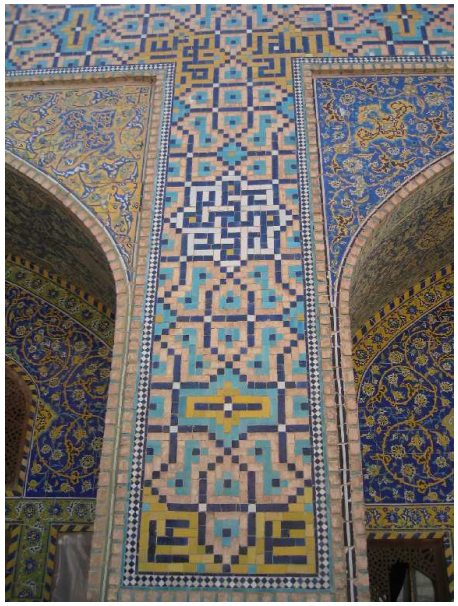
- Metric space with metric d
- φ is an isometry if $d(x, y) = d(\varphi(x), \varphi(y))$
- A symmetry is any isometry that leaves the object as a whole unchanged
- Symmetries form groups!

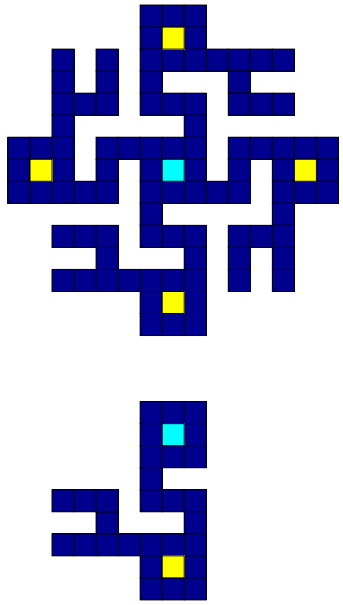
SYMMETRY GROUPS





SYMMETRY GROUPS





SUBGROUPS

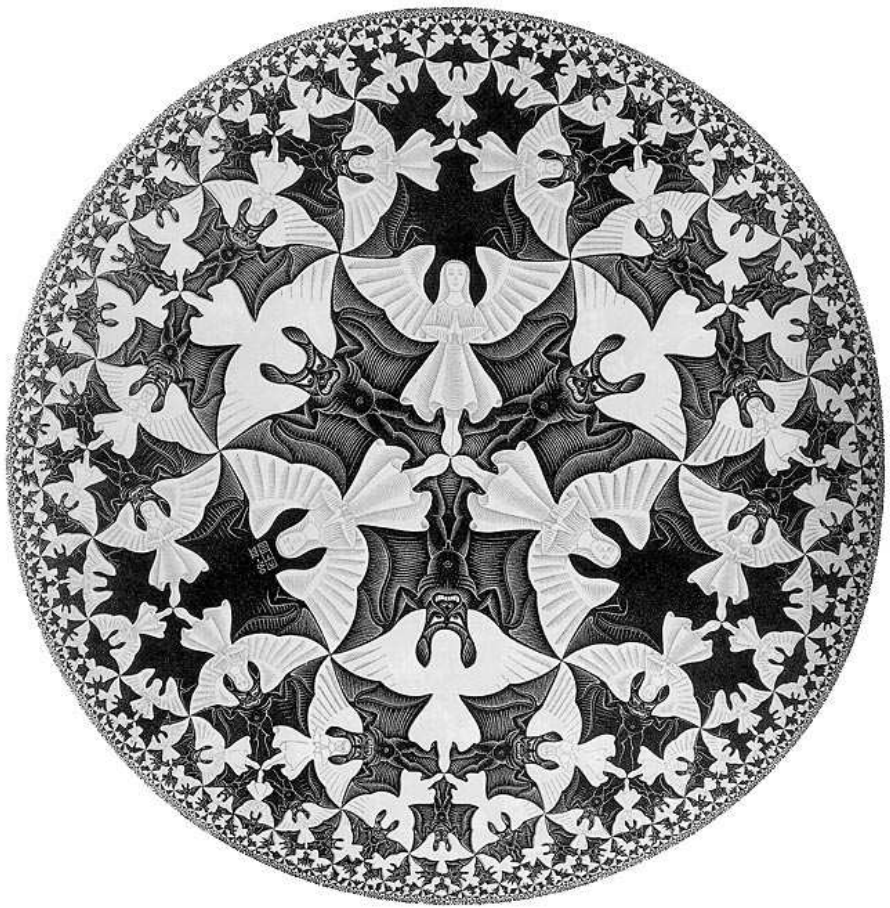
- $\langle G, * \rangle$, a group
- $H \subseteq G$
- $*$ is the induced operation on H from G if S is closed under it
- H is a subgroup of G if H is a group with the induced operation
- $\{e\}$ is the trivial subgroup of G.
- All other subgroups are nontrivial.

CHARACTERIZING SUBGROUPS

- (Theorem)$H \subseteq G$ of a group $\langle G, * \rangle$ is a subgroup of G iff:
  1. H is closed under $*$,
  2. the identity e of G is in H,
  3. for all $a \in H$, $a^{-1} \in H$.
- Example: subgroups of $\mathbb{Z}_4$

$\mathbb{Z}_4$	0	1	2	3
0	0	1	2	3
1	1	2	3	0
2	2	3	0	1
3	3	0	1	2

STORYTIME



COSETS

- H, a subgroup of G.
- Let the relation $\sim_L$ be defined on G by:

$$a \sim_L b \text{ iff } a^{-1}b \in H.$$

- Let $\sim_R$ be defined by:

$$a \sim_R b \text{ iff } ab^{-1} \in H.$$

  Then $\sim_L$ and $\sim_R$ are both equivalence relations on G.

- Let H be a subgroup of group G. For $a \in G$, the subset $aH = \{ah \mid h \in H\}$ of G is the left coset of H containing a, and $Ha = \{ha \mid h \in H\}$ is the right coset of H containing a.

NORMAL SUBGROUPS

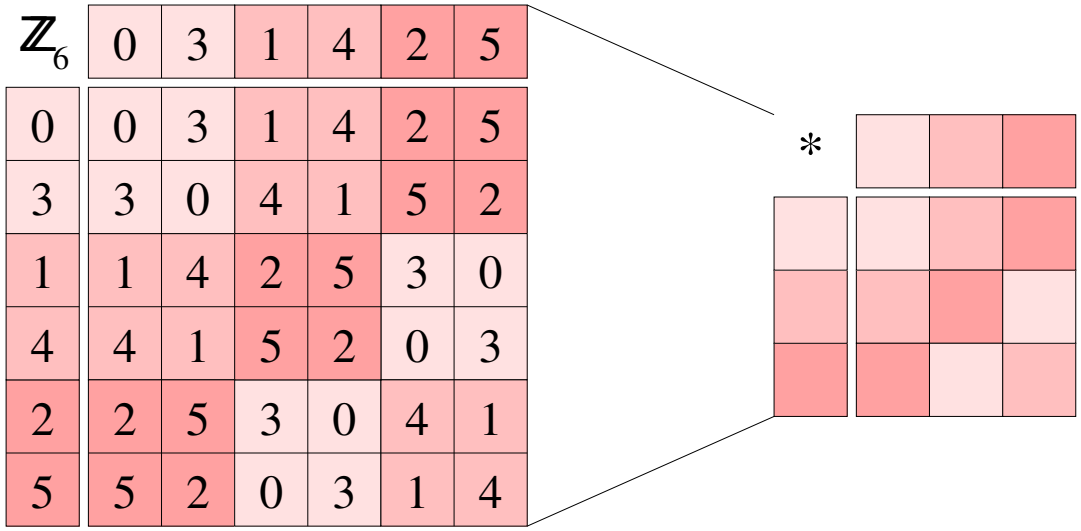
- If left and right cosets match, the subgroup is normal.
- All subgroups H of an abelian group G are normal, as $ah = ha, \forall a \in G, h \in H$
- $\{0, 2\}$ is a subgroup of $\mathbb{Z}_4$. It is normal. The coset of 1 is $1 + \{0, 2\} = \{1, 3\}$.
- Plan:
  - Treat elements in a subgroup as equal
  - Breaks group into cosets
  - Treat cosets as *elements* of a smaller group!

FACTOR GROUPS

- Let H be a normal subgroup of group G.
- Let $\{aH \mid a \in G\}$ be the set of cosets.
- Left coset multiplication is well-defined by the equation $(aH)(bH) = (ab)H$
- The cosets of H form a group G/H under left multiplication
- G/H is the factor group (or quotient group) of G modulo H.
- The elements in the same coset of H are congruent modulo H.

FACTOR GROUPS

(EXAMPLE)

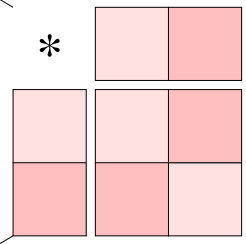


- $\{0, 3\}$ is a normal subgroup
- Cosets $\{0, 3\}$, $\{1, 4\}$, and $\{2, 5\}$
- $\mathbb{Z}_6/\{0, 3\}$ looks like $\mathbb{Z}_3$

FACTOR GROUPS

(EXAMPLE)

$\mathbb{Z}_6$	0	2	4	1	3	5
0	0	2	4	1	3	5
2	2	4	0	3	5	1
4	4	0	2	5	1	3
1	1	3	5	2	4	0
3	3	5	1	4	0	2
5	5	1	3	0	2	4



- $\{0, 2, 4\}$ is a normal subgroup
- Cosets $\{0, 2, 4\}$, $\{1, 3, 5\}$
- $\mathbb{Z}_6/\{0, 2, 4\}$ looks like $\mathbb{Z}_2$

HOMOMORPHISMS

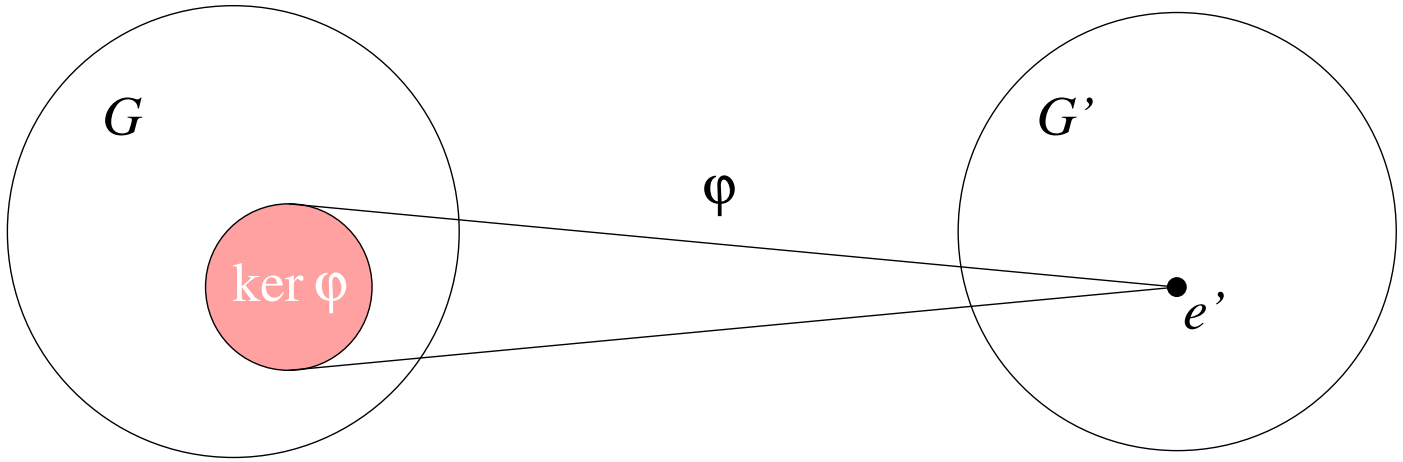
- Given groups G, G'
- $\varphi : G \to G'$
- φ is a homomorphism if it is *linear*: for all $a, b \in G$,

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

- Trivial homomorphism defined by $\varphi(g) = e'$ for all $g \in G$
- A 1-1 homomorphism is an monomorphism.
- A homomorphism that is onto is an epimorphism.
- A homomorphism that is 1-1 and onto is an isomorphism $\cong$.
- (Theorem) Let $\mathcal{G}$ be any collection of groups. Then $\cong$ is an equivalence relation on $\mathcal{G}$.

PROPERTIES OF HOMOMORPHISMS

- If e is the identity in G, then $\varphi(e)$ is the identity e' in G'.
- If $a \in G$, then $\varphi(a^{-1}) = \varphi(a)^{-1}$.
- If H is a subgroup of G, then $\varphi(H)$ is a subgroup of G'.
- If K' is a subgroup of G', then $\varphi^{-1}(K')$ is a subgroup of G.
- The normal subgroup $\ker \varphi = \varphi^{-1}(\{e'\}) \subseteq G$, is the kernel of φ.



CYCLIC GROUPS

- Let G be a group and let $a \in G$
- $H = \{a^n \mid n \in \mathbb{Z}\}$ is a subgroup of G
- It is the smallest subgroup of G that contains a
- H is the cyclic subgroup of G generated by a denoted $\langle a \rangle$
- If $\langle a \rangle$ is finite, the order of a is $|\langle a \rangle|$
- $a \in G$ generates G and is a generator for G if $\langle a \rangle = G$
- A group G is cyclic if it has a generator

CLASSIFICATION OF CYCLIC GROUPS

- $\langle \mathbb{Z}, + \rangle = \langle 1 \rangle$
- $\langle \mathbb{Z}_n, +_n \rangle = \langle 1 \rangle$
- (Theorem) Any infinite cyclic group is isomorphic to $\langle \mathbb{Z}, + \rangle$. Any finite cyclic group of order n is isomorphic to $\langle \mathbb{Z}_n, +_n \rangle$.

SMALL GROUPS (REVISITED)

	e	a
e	e	a
a	a	e

	e	a	b
e	e	a	b
a	a	b	e
b	b	e	a

	0	1	2	3
0	0	1	2	3
1	1	2	3	0
2	2	3	0	1
3	3	0	1	2

V_4	e	a	b	c
e	e	a	b	c
a	a	e	c	b
b	b	c	e	a
c	c	b	a	e

FINITELY GENERATED GROUPS

- (Theorem) The intersection of subgroups is a subgroup.
- Let G be a group and let $a_i \in G$ for $i \in I$
- We can take the intersection of all subgroups containing all a_i to obtain a subgroup H
- H is the smallest subgroup containing all a_i
- H is the subgroup generated by $\{a_i \mid i \in I\}$
- If H is G, then $\{a_i \mid i \in I\}$ generates G and the a_i are the generators of G
- If there is a finite set $\{a_i \mid i \in I\}$ that generates G, then G is finitely generated

DIRECT PRODUCTS

- Let $G_1, G_2, \ldots, G_n$ be groups.
- The set is $\prod_{i=1}^{n} G_i$ (Cartesian product)
- Binary operation:
  $(a_1, a_2, \ldots, a_n) \times (b_1, b_2, \ldots, b_n) = (a_1 b_1, a_2 b_2, \ldots, a_n b_n)$.
- Then $\langle \prod_{i=1}^{n} G_i, \times \rangle$ is a group.
- We call it the direct product of the groups G_i.
- Sometimes called direct sum with $\oplus$.
- Example: $\mathbb{Z}_2 \times \mathbb{Z}$, $\mathbb{Z} \times \mathbb{Z}$

FUNDAMENTAL THEOREM

- (Theorem) Every finitely generated abelian group is isomorphic to product of cyclic groups of the form

$$\mathbb{Z}_{m_1} \times \mathbb{Z}_{m_2} \times \ldots \times \mathbb{Z}_{m_r} \times \mathbb{Z} \times \mathbb{Z} \times \ldots \times \mathbb{Z},$$

  where m_i divides m_{i+1} for $i = 1, \ldots, r-1$.

- The direct product is unique: the number of factors of $\mathbb{Z}$ is unique and the cyclic group orders m_i are unique.
- Free: vector space, basis, rank
- Torsion: module
- The number of factors of $\mathbb{Z}$ is the Betti number $\beta(G)$ of G.
- The orders of the finite cyclic groups are the torsion coefficients of G.

GROUP PRESENTATIONS

- For each generator, we have a letter in an alphabet
- Any symbol of the form $a^n = aaaa \cdots a$ (a string of $n \in \mathbb{Z}$ a's) is a syllable
- A finite string of syllables is a word
- The empty word 1 does not have any syllables
- We may replace $a^m a^n$ by a^{m+n} using elementary contractions
- Relations are equations of form $r = 1$ (torsion)
- Notation: (letters : relations)
- Example: $\mathbb{Z}_6 =?$

SYMMETRY WORK 70