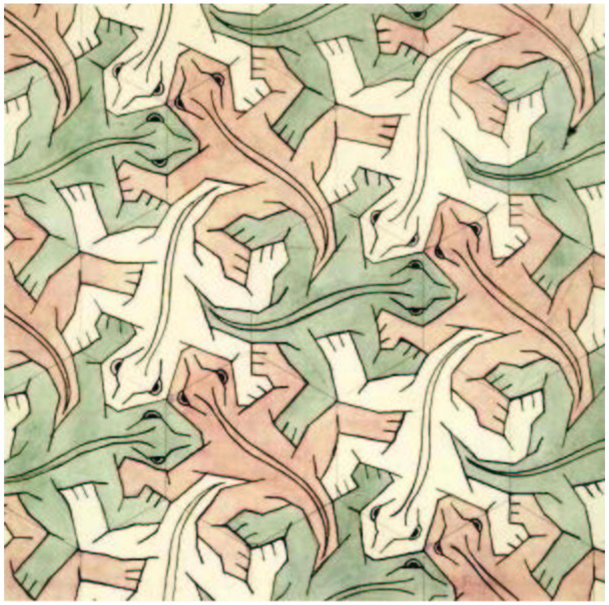
GROUP THEORY



CS 468 – Lecture 4
10/16/2

M. C. ESCHER

I had not yet seen the tile decorations of the Alhambra and never heard of crystallography; so I did not even know that my game was based on rules that have been scientifically investigated.

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

— M. C. Escher

OVERVIEW

- Abstract algebra: studying core properties
- Groups
- Subgroups and Cosets
- Homomorphisms
- Factor groups
- Cyclic groups
- Finitely generated abelian groups

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.
- If $*$ assigns a single element, it is well-defined; if no element, it is not defined; if multiple elements, not well-defined.
- If it always assigns an element in S, it is closed.
- It is associative iff $(a * b) * c = a * (b * c)$ for all $a, b, c \in S$.
- It is commutative iff $a * b = b * a$ for all $a, b \in S$.

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

ABSTRACTION

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

$5 + x$	$=$	2	Given
$-5 + (5 + x)$	$=$	$-5 + 2$	Addition property of equality
$(-5 + 5) + x$	$=$	$-5 + 2$	Associative property of addition
$0 + x$	$=$	$-5 + 2$	Inverse property of addition
x	$=$	$-5 + 2$	Identity property of addition
x	$=$	-3	Addition

GROUPS

- A group $\langle G, * \rangle$ is a set G, together with a binary operation $*$ on G, such that the following axioms are satisfied:
  (a) $*$ is associative.
  (b) G has an identity e element for $*$ such that $e * x = x * e = x$ for all $x \in G$.
  (c) any element a has an inverse a' with respect to the operation $*$, i.e. $\forall a \in G, \exists a' \in G$ such that $a' * a = a * a' = e$.
- If G is finite, the order of G is $|G|$.
- We often omit the operation and refer to G as the group.
- $\langle \mathbb{Z}, + \rangle$, $\langle \mathbb{R}, \cdot \rangle$, $\langle \mathbb{R}, + \rangle$, are all groups.
- A group G is abelian if its binary operation $*$ is commutative.

SMALL GROUPS

(EXAMPLE)

$\mathbb{Z}_2$	e	a
e	e	a
a	a	e

$\mathbb{Z}_3$	e	a	b
e	e	a	b
a	a	b	e
b	b	e	a

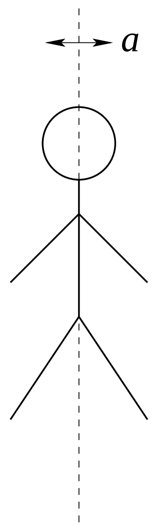
$\mathbb{Z}_4$	0	1	2	3
0	0	1	2	3
1	1	2	3	0
2	2	3	0	1
3	3	0	1	2

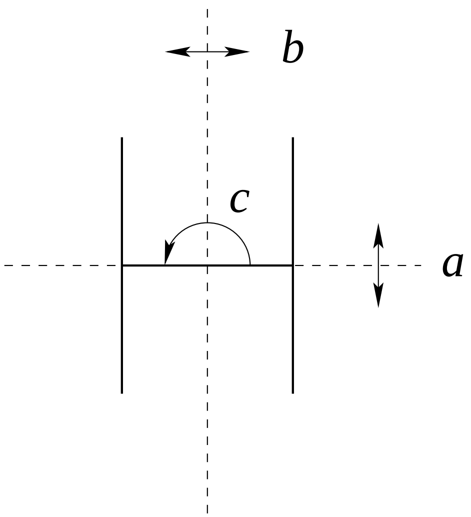
V_4	e	a	b	c
e	e	a	b	c
a	a	e	c	b
b	b	c	e	a
c	c	b	a	e

SYMMETRY GROUPS

(EXAMPLE)

- If the space has a metric d, a transformation ϕ is an isometry if $d(x, y) = d(\phi(x), \phi(y))$, that is, if ϕ preserves distance.
- A symmetry is any isometry that leaves the object as a whole unchanged. Symmetries form groups!





SUBGROUPS

- Let $\langle G, * \rangle$ be a group and $S \subseteq G$. If S is closed under $*$, then $*$ is the induced operation on S from G.
- A subset $H \subseteq G$ of group $\langle G, * \rangle$ is a subgroup of G if H is a group and is closed under $*$. The subgroup consisting of the identity element of G, $\{e\}$ is the trivial subgroup of G. All other subgroups are nontrivial.
- (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 $\mathbb{Z}_4$

COSETS

- Let H be a subgroup of G. Let the relation $\sim_L$ be defined on G by: $a \sim_L b$ iff $a^{-1}b \in H$. Let $\sim_R$ be defined by: $a \sim_R b$ 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.
- 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 $1 + \{0, 2\} = \{1, 3\}$. That's all folks!

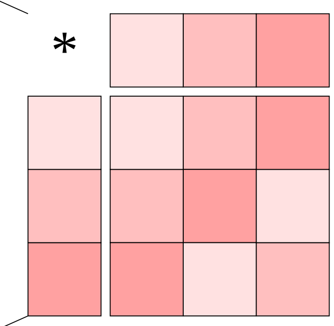
Factor Groups

- Let H be a normal subgroup of group G.
- 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)

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

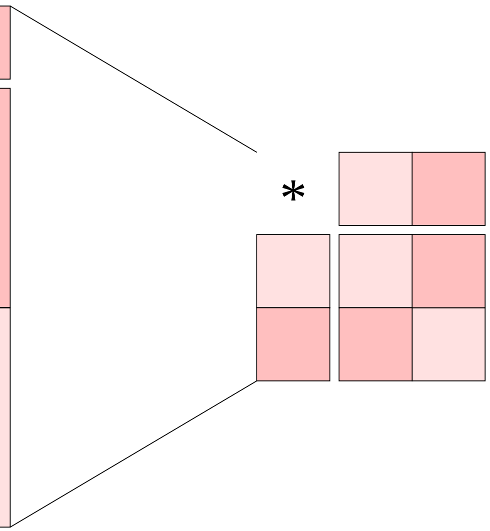


- $\{0, 3\}$ is a normal subgroup
- Cosets $\{0, 3\}$, $\{1, 4\}$, and $\{2, 5\}$
- $\mathbb{Z}_6/\{0, 3\} \cong \mathbb{Z}_3$

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



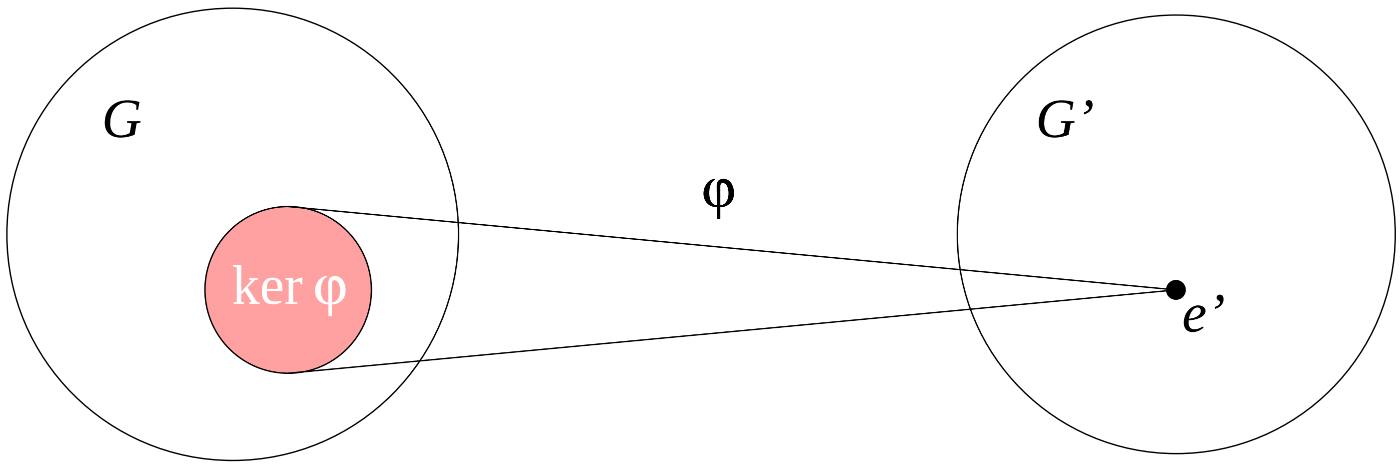
- $\{0, 2, 4\}$ is a normal subgroup
- Cosets $\{0, 2, 4\}$, $\{1, 3, 5\}$
- $\mathbb{Z}_6/\{0, 2, 4\} \cong \mathbb{Z}_2$

HOMOMORPHISMS

- A map φ of a group G into a group G' is a *homomorphism* if $\varphi(ab) = \varphi(a)\varphi(b)$ for all $a, b \in G$.
- Trivial homomorphism defined by $\varphi(g) = e'$ for all $g \in G$, where e' is the identity 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.
- We use $\cong$ for isomorphisms.
- (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
- Is $\mathbb{Z}_m$ cyclic? Is V_4?

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 $\oplus$.

Fundamental Theorem

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

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

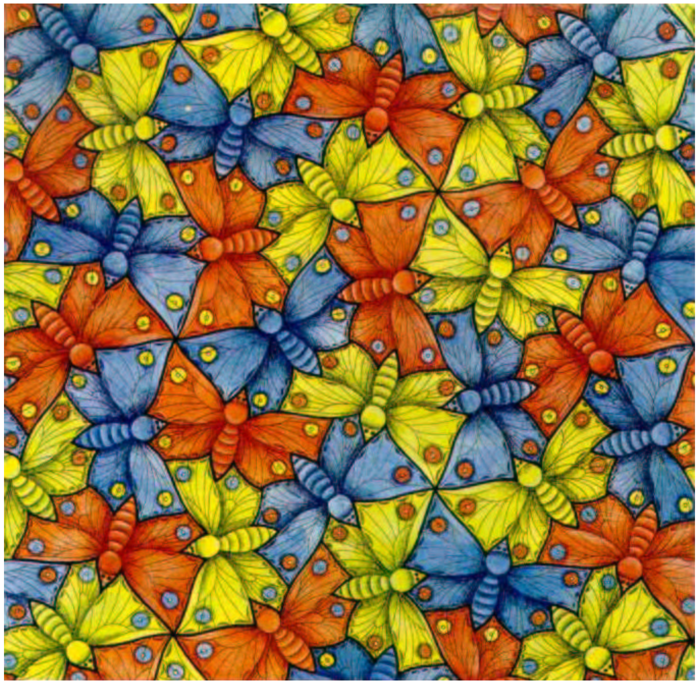
  where m_i divides m_{i+1} for $i = 1, \ldots, r-1$.

- The direct product is unique: the number of factors of $\mathbb{Z}$ is unique and the cyclic group orders m_i are unique.
- Free: basis, rank, vector space
- 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)

SYMMETRY WORK 70



Ladies and gentlemen, herewith I have come to the end of this talk. I hope that I have not tried your patience too much, and I thank you very much for the attention you have so kindly given to my fancies.

— M. C. Escher