Q: What's purple and commutes?
A: An abelian grape!
— Anonymous

4 Group Theory

Last lecture, we learned about a combinatorial method for characterizing spaces: using simplicial complexes as triangulations of the spaces. We also showed how the connectivity of compact 2-manifolds is fully characterized by an invariant, the Euler characteristic, that may be computed using any triangulation of the space. In this lecture, we study *Group theory*. This theory is part of the beautiful machinery of *Abstract Algebra*, which is based on abstracting from algebra its core properties, and studying algebra in terms of those properties. Because of this abstraction, group theory is fundamental and applicable to questions in many theoretical fields such as quantum physics and crystallography, as well as questions in practical fields, such as establishing bar codes for products, serial numbers on currency, or solving Rubik's Magic cube. For us, the theory provides powerful tools to define equivalence relations using *homomorphisms* and *factor groups*. These equivalence relations will enable us to partition the space of manifolds into coarser classifications that are computable. We begin with an introduction to groups, their subgroups, and associated cosets. We then look at how we *factor* a group much like the way we divide a composite integer. We end by developing techniques for characterizing a specific type of groups: finitely generated abelian groups.

4.1 Groups

Addition of integers is an operation which assigns another integer to every pair of integers. We begin by extending the concept of addition.

Definition 4.1 (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 S is finite, we may display a binary operation $*$ in a table, listing the elements of the set on the top and side of the table, and stating $a * b$ in row a, column b of the table, as in Table 1. Note that the operation defined by this table

	b	c	b
a	b	a	c
b	a	c	b
c	c	b	a

Table 1. A closed binary operation $*$, defined on the set $\{a, b, c\}$.

depends on the order of the pair, as $a * b \neq b * a$.

Definition 4.2 (properties) Let $*$ be a binary operation on a set S. If $*$ assigns a single element to each pair of elements in S it is *well-defined*. Otherwise, we say it is *not defined* when it assigns zero elements, or *not well-defined* when it assigns more than one element. If it always assigns an element in S to a pair of elements from 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 $a, b \in S$.

If S is finite, the table for a commutative binary operation is symmetric with respect to the upper-left to lower-right diagonal. If a binary operation $*$ is associative, we may write unambiguous long expressions without using parentheses.

The study of groups, as well as the need for new types of numbers, was motivated by solving equations.

Example 4.1 (Solving equations) Suppose we were interested in solving the following three equations:

1. $5 + x = 2$
2. $2x = 3$
3. $x^2 = -1$

The equations imply the need for negative integers $\mathbb{Z}^-$, rational numbers $\mathbb{Q}$, and complex numbers $\mathbb{C}$, respectively. Recalling algebra from 8th grade, I solve equation (1) above, listing the properties needed at each step.

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

We take all the properties we need to solve this equation to define a group.

Definition 4.3 (group) 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) $\exists e \in G$ such that $e * x = x * e = x$ for all $x \in G$. The element e is an *identity* element for $*$ on G.

(c) $\forall a \in G, \exists a' \in G$ such that $a' * a = a * a' = e$. The element a' is an *inverse of a with respect to the operation* $*$.

If G is finite, the *order* of G is $|G|$. We often omit the operation and refer to G as the group.

The identity and inverses are unique in a group. We may easily show, furthermore that $(a*b)' = b' * a'$, for all $a, b \in G$ in group $\langle G, * \rangle$.

Example 4.2 $\langle \mathbb{Z}, + \rangle$, $\langle \mathbb{R}, \cdot \rangle$, $\langle \mathbb{R}, + \rangle$, are all groups. Note that only one operation is allowed for groups, so we choose either multiplication or addition for integers, for example. When we do so, the other operation is not defined.

We are mainly interested in groups with commutative binary operations.

Definition 4.4 (abelian) A group G is *abelian* if its binary operation $*$ is commutative.

We borrow terminology from arithmetic usually for abelian groups, using $+$ or juxtaposition for the operation, 0 or 1 to denote identity, and $-a$ or a^{-1} for inverses. It is easy to list the possible structures for small groups using the following fact, derived from the definition of groups: each element of a finite group must appear once and only once in each row and column of its table. Using this fact, Table 2 shows all possible structures for groups of size 2, 3, and 4 in Table 2. There are, in fact, three possible groups of size 4, but only two unique structures: we get the other one by renaming elements.

$\mathbb{Z}_2$	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

Table 2. Structures for groups of size 2, 3, 4.

Example 4.3 (Symmetry groups) An application of group theory is the study of symmetries of geometric figures. An *isometry* is a distance-preserving transformation in a metric space. A *symmetry* is any isometry that leaves the object as a whole unchanged. The symmetries of a figure form a group. A human, abstracted in Figure 1 (a) as a stick figure, has only two symmetries: the identity, and reflection along the vertical line shown. It is immediate, therefore, that a human's group of symmetry is $\mathbb{Z}_2$, as it is the only group of two elements. The letter "H" (b) has three different types of symmetries: reflections along the horizontal and vertical axes, and rotation by 180 degrees. If we write down the table corresponding to compositions of these symmetries, we get the group V_4 in Table 2. Can you draw a figure whose symmetry group is $\mathbb{Z}_4$?

(a) Humans have $\mathbb{Z}_2$ symmetry

(b) The letter “H” has V_4 symmetry

Figure 1. Two figures and their symmetry groups.

4.2 Subgroups and Cosets

As for sets, we may try to understand groups by examining the building blocks they are composed of. We begin by extending the concept of a subset to groups.

Definition 4.5 (induced operation) 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.*

Definition 4.6 (subgroup) 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*.

We can identify subgroups easily, using the following theorem.

Theorem 4.1 *$H \subseteq G$ 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 4.4 The only nontrivial proper subgroup of $\mathbb{Z}_4$ in Table 2 is $\{0, 2\}$. $\{0, 3\}$ is not a subgroup of $\mathbb{Z}_4$ as $3 * 3 = 2 \notin \{0, 3\}$, so the set is not closed under the binary operation stated in the table.

Example 4.5 In the first lecture, we talked about Felix Klein’s unifying definition of geometry and topology as the study of invariant properties under transformation. We may now state his full definition. The set of all transformations of a space forms a group under composition. A *geometry* is the study of those properties of a space that remain invariant under some fixed subgroup of the full transformation group. The set of isometries forms a subgroup of the full transformation group. The *Euclidean geometry* is the study of those properties left invariant under the group of isometries. Similarly, homeomorphisms form a subgroup of the full transformation group, and *topology* is the study of invariants of spaces under this subgroup.

Given a subgroup, we may partition a group into sets, all having the same size as the subgroup. The cosets are basically like the “evil” siblings of the subgroup we use to partition the group.

Theorem 4.2 *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.*

Note that $a^{-1}b \in H \Rightarrow a^{-1}b = h \in H \Rightarrow b = ah$. We use these relations to define cosets.

Definition 4.7 (cosets) 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.

For an abelian subgroup H of G, $ah = ha, \forall a \in G, h \in H$, so left and right cosets match. We may easily show that every left coset and every right coset has the same size by constructing a 1-1 map of H onto a left coset gH of H for a fixed element g of G. If a subgroup's coset match, we say that it is normal.

Definition 4.8 (normal) A subgroup H of a group G is *normal* if its left and right cosets coincide, that is, if $gH = Hg$ for all $g \in G$.

Example 4.6 As we saw in Example 4.4, $\{0, 2\}$ is a subgroup of $\mathbb{Z}_4$. It is normal as $\mathbb{Z}_4$ is abelian. The coset of 1 is $1 + \{0, 2\} = \{1, 3\}$. The sets $\{0, 2\}$ and $\{1, 3\}$ exhaust all of $\mathbb{Z}_4$.

4.3 Factor Groups

Given a normal subgroup, we would like to treat the cosets as individual elements of a smaller group. To do so, we first derive a binary operation from the group operation of G.

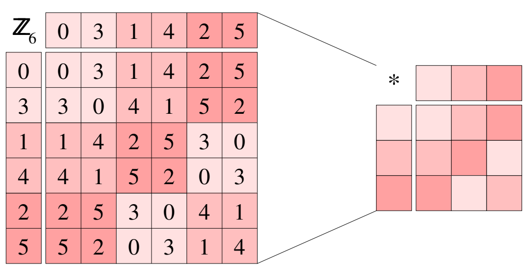
Theorem 4.3 *Let H be a subgroup of a group G. Then, left coset multiplication is well-defined by the equation $(aH)(bH) = (ab)H$, iff left and right cosets coincide.*

We can show that this multiplication is well-defined as it does not depend on the elements a, b chosen from the cosets. Using left coset multiplication as a binary operation, we get new groups.

Corollary 4.1 *Let H be a subgroup of G whose left and right cosets coincide. Then, the cosets of H form a group G/H under the binary operation $(aH)(bH) = (ab)H$.*

Definition 4.9 (factor group) The group G/H in Corollary 4.1 is the *factor group* (or *quotient group*) *of G modulo H*. The elements in the same coset of H are said to be *congruent modulo H*.

Example 4.7 (Factoring $\mathbb{Z}_6$) The cyclic group $\mathbb{Z}_6$, on the left, has $\{0, 3\}$ as a subgroup. As $\mathbb{Z}_6$ is abelian, $\{0, 3\}$ is normal, so we may factor $\mathbb{Z}_6$ using this subgroup, getting cosets $\{0, 3\}$, $\{1, 4\}$, and $\{2, 5\}$. Figure 2 shows the table for $\mathbb{Z}_6$, ordered and colored according to the cosets. The color pattern gives rise to a smaller group, shown on the



$\mathbb{Z}_6$	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

Figure 2. $\mathbb{Z}_6/\{0, 3\}$ is isomorphic to $\mathbb{Z}_3$.

right, where each coset is collapsed to a single element. Comparing this new group to the structures in Table 2, we observe that it is isomorphic to $\mathbb{Z}_3$, the only group of order 3. Therefore, $\mathbb{Z}_6/\{0, 3\} \cong \mathbb{Z}_3$. Moreover, $\{0, 3\}$ with binary operation $+_6$ is isomorphic to $\mathbb{Z}_2$, as one may see from the top left corner of the table for $\mathbb{Z}_6$. So, we have $\mathbb{Z}_6/\mathbb{Z}_2 \cong \mathbb{Z}_3$. Similarly, $\mathbb{Z}_6/\mathbb{Z}_3 \cong \mathbb{Z}_2$, as shown in Figure 3.

For a beginner, factor groups seem to be of the hardest concepts in group theory. Given a factor group G/H, the key idea to remember is that each *element* of the factor group has the form aH: it is a set, a coset of H. Now, we could represent each element of a factor group with a representative from the coset. For example, the element 4 could represent the coset $\{1, 4\}$ for factor group $\mathbb{Z}_6/\{0, 3\}$. However, don't forget that this element is congruent to 1 modulo $\{0, 3\}$.

$\mathbb{Z}_6$	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

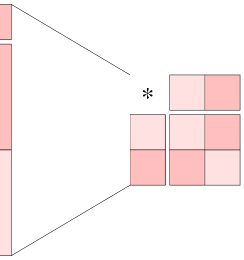


Figure 3. $\mathbb{Z}_6/\{0, 2, 4\}$ is isomorphic to $\mathbb{Z}_2$.

4.4 Homomorphisms

Having defined groups, a natural question that arises is to characterize groups: how many "different" groups are there? This is yet another classification problem and it is the fundamental question studied in group theory. Since we are interested in characterizing the structure of groups, we define maps between groups to relate their structures.

Definition 4.10 (homomorphism) A map φ of a group G into a group G' is a *homomorphism* if $\varphi(ab) = \varphi(a)\varphi(b)$ for all $a, b \in G$. For any groups G and G', there's always at least one homomorphism $\varphi : G \to G'$, namely the *trivial homomorphism* defined by $\varphi(g) = e'$ for all $g \in G$, where e' is the identity in G'.

Analogs of injections, surjections, and bijections exist for maps between groups. They have their own special names, however.

Definition 4.11 (mono-, epi-, iso-morphism) 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.

Isomorphisms between groups are like homeomorphisms between topological spaces. We may use isomorphisms to define an equivalence relationship between groups, formalizing our notion for similar structures for groups.

Theorem 4.4 *Let $\mathcal{G}$ be any collection of groups. Then $\cong$ is an equivalence relation on $\mathcal{G}$.*

All groups of order 4, for example, are isomorphic to one of the two 4 by 4 tables in Table 2, so the classification problem is fully solved for that order. We need smarter techniques, however, to settle this question for higher orders.

Homomorphisms preserve the identity, inverses, and subgroups in the following sense.

Theorem 4.5 *Let φ be a homomorphism of a group G into a group G'.*

1. *If e is the identity in G, then $\varphi(e)$ is the identity e' in G'.*
2. *If $a \in G$, then $\varphi(a^{-1}) = \varphi(a)^{-1}$.*
3. *If H is a subgroup of G, then $\varphi(H)$ is a subgroup of G'.*
4. *If K' is a subgroup of G', then $\varphi^{-1}(K')$ is a subgroup of G.*

Homomorphisms also define a special subgroup in their domain.

Definition 4.12 (kernel) Let $\varphi : G \to G'$ be a homomorphism. The subgroup $\varphi^{-1}(\{e'\}) \subseteq G$, consisting of all elements of G mapped by φ into the identity e' of G', is the *kernel of φ*, denoted by $\ker\varphi$, as shown in Figure **??**.

Note that $\ker\varphi$ is a subgroup by an application of Theorem 4.5 to the fact that $\{e'\}$ is the trivial subgroup of G'. So, we may use it to partition G into cosets.

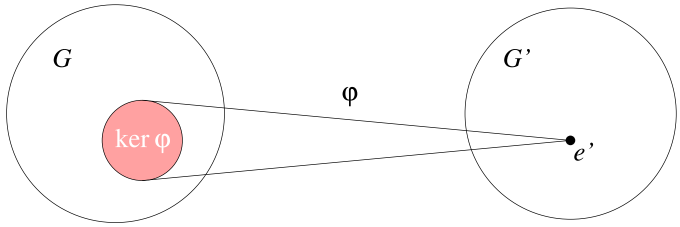


Figure 4. A homomorphism $\varphi : G \to G'$ and its kernel.

Theorem 4.6 *Let $\varphi : G \to G'$ be a homomorphism, and let $H = \ker \varphi$. Let $a \in G$. Then the set*

$$\varphi^{-1}\{\varphi(a)\} = \{x \in G \mid \varphi(x) = \varphi(a)\}$$

is the left coset aH of H, and is also the right coset Ha of H.

The two partitions of G into left cosets and into right cosets of $\ker \varphi$ are the same, according to the theorem. That is, the kernel is normal.

4.5 Finitely Generated Abelian Groups

We are primarily interested in *finitely generated abelian groups*. These groups will arise as descriptions of the connectivity of topological spaces. To understand the structure of these groups, we utilize our usual approach: understand simple structures first, and try to construct complicated structures from these building blocks. We begin with cyclic groups, the simplest group there is.

Theorem 4.7 *Let G be a group and let $a \in G$. Then, $H = \{a^n \mid n \in \mathbb{Z}\}$ is a subgroup of G and is the smallest subgroup of G that contains a, that is, every subgroup containing a contains H.*

Definition 4.13 (cyclic group) The group H of Theorem 4.7 is the *cyclic subgroup of G generated by a*, and will be denoted by $\langle a \rangle$. If $\langle a \rangle$ is finite, then the *order of a* is $|\langle a \rangle|$. An element a of a group G *generates* G and is a *generator for G* if $\langle a \rangle = G$. A group G is *cyclic* if it has a generator.

For example, $\mathbb{Z} = \langle 1 \rangle$ under addition, and is therefore cyclic. We can also define finite cyclic groups using a new binary operation.

Definition 4.14 (modulo) Let n be a fixed positive integer and let h and k be any integers. The remainder r when $h + k$ is divided by n is the *sum of h and k modulo n*.

Definition 4.15 ($\mathbb{Z}_n$) The set $\{0, 1, 2, \ldots, n-1\}$ is a cyclic group $\mathbb{Z}_n$ of elements under addition modulo n.

We may fully classify cyclic groups, using the theorem below.

Theorem 4.8 (Classification of cyclic groups) *Any infinite cyclic group is isomorphic to $\mathbb{Z}$ under addition. Any finite cyclic group of order n is isomorphic to $\mathbb{Z}_n$ under addition modulo n.*

Consequently, we may use $\mathbb{Z}$ and $\mathbb{Z}_n$ as the prototypical cyclic groups.

We next extend the idea of a generator to multiple generators for a group. Each generator generates some portion of the elements. We put them together using intersection of groups.

Theorem 4.9 *The intersection of subgroups H_i of a group G for $i \in I$ is again a subgroup of G.*

Let G be a group and let $a_i \in G$ for $i \in I$. There is at least one subgroup of G containing all the elements a_i, namely G, itself. Theorem 4.9 allows us to take the intersection of all the subgroups of G containing all a_i to obtain a subgroup H of G. Clearly, H is the smallest subgroup containing all a_i.

Definition 4.16 (finitely generated) Let G be a group and let $a_i \in G$ for $i \in I$. The smallest subgroup of G containing $\{a_i \mid i \in I\}$ is the *subgroup generated by* $\{a_i \mid i \in I\}$. If this subgroup is all of 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.*

Having defined what we mean by finitely generated groups, we may look at a complete description of their structure.

Theorem 4.10 (direct products) *Let $G_1, G_2, \ldots, G_n$ be groups. For $(a_1, a_2, \ldots, a_n)$ and $(b_1, b_2, \ldots, b_n)$ in $\prod_{i=1}^n G_i$, define $(a_1, a_2, \ldots, a_n)(b_1, b_2, \ldots, b_n)$ to be $(a_1 b_1, a_2 b_2, \ldots, a_n b_n)$. Then $\prod_{i=1}^n G_i$ is a group, the* direct product of the groups G_i*, under this binary operation.*

The direct product is often written with the symbol $\otimes$ to distinguish it from the binary operation of the group (which may be indicated as a product. Sometimes, it is called the *direct sum*, indicated by a $\oplus$. Although these symbols seem to be designed to scare non-specialists away, the do help to keep the distinction between different operations clear, especially when we have additional operations in advanced algebra.

The following theorem gives a complete characterization of the structure of finitely generated abelian groups as the direct product of cyclic groups.

Theorem 4.11 (Fundamental Theorem of Finitely Generated Abelian Groups) *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; that is, the number of factors of $\mathbb{Z}$ is unique and the cyclic group orders m_i are unique.

Note how the product is composed of a number of infinite and finite cyclic group factors. Intuitively, the infinite part captures those generators that are "free" to generate as many elements as they wish. This portion of the group is a *free group* that acts like a vector space. The group may be given a *basis* of generators from which we may generate the group. The number of generators is called the *rank* of the free group. The finite or "torsion" part, on the other hand, captures generators with finite order. This portion is like a strange vector space that does not allow us to move freely in every dimension. In fact, this portion is called a *module*. We do not have enough time in this course to discuss these structures in detail.

Definition 4.17 (Betti number, torsion) The number of factors of $\mathbb{Z}$ in Theorem 4.11 is the *Betti number* $\beta(G)$ of G. The orders of the finite cyclic groups are the *torsion coefficients of* G.

4.6 Group Presentations

We end this lecture with a short and informal treatment of *group presentations*: a method for specifying finitely generated groups. We think of each generator of the group as 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* and a finite string of syllables is a *word*. The *empty word* 1 does not have any syllables. We modify words naturally using *elementary contractions*, replacing $a^m a^n$ by a^{m+n}. The torsional part of the group also gives us *relations*, equations of form $r = 1$. A presentation allows us to write all possible strings that correspond to the elements of the presented groups. Formally, we show an isomorphism between the set of strings and the group.

For example, the cyclic group $\mathbb{Z}_6$ may be presented by a single generator a and the relation $a^6 = 1$. We use $(a : a^6)$ for denoting this presentation. Another presentation for $\mathbb{Z}_6$ is $(a, b : a^2, b^3, aba^{-1}b^{-1})$. This presentation describes the underlying structure of $\mathbb{Z}_6$ as $\mathbb{Z}_2 \times \mathbb{Z}_3$. The last relation captures the commutativity of the group.

Acknowledgments

Most of this lecture is from Fraleigh's magnificent introductory book on abstract algebra [1]. Another excellent book is Gallian [2].

References

[1] Fraleigh, J. B. *A First Course in Abstract Algebra*, sixth ed. Addison-Wesley, Reading, MA, 1998.

[2] Gallian, J. A. *Contemporary Abstract Algebra*, fifth ed. Houghton Mifflin College, Boston, Massachusetts, 2002.