Group Theory

Jaeyi Song and Sophia Hou

Abstract

In the MIT PRIMES Circle (Spring 2022) program, we studied group theory, often following *Contemporary Abstract Algebra* by Joseph Gallian. In this paper, we start by introducing basic ideas relating to group theory such as the definition of a group, cyclic groups, subgroups, and quotient groups. We then introduced the notions of homomorphisms, as well as generators and relations. Finally, we delved into two fun and interesting problems that address generators and relations.

1 Groups

Definition 1.1. A **group** $(G, *)$ is a set G with a binary operation $*$ that has three requirements satisfied:

1. Associativity: $a * (b * c) = (a * b) * c$ for all elements $a, b, c \in G$.
2. Identity: there is an element $e \in G$ in which $a * e = e * a = a$ for all elements of G. The identity for groups under multiplication is 1, under addition it is 0.
3. Inverse: For every element $a \in G$, there is the inverse of a (let's say b) that satisfies $a * b = b * a = e$.

Remark. Usually the group operation $*$ will be multiplication, so we will often just omit writing $*$.

Example 1.2. The group $(\mathbb{Z}/n\mathbb{Z}, +)$, which is the set $\{0, 1, 2, \ldots, n-1\}$ under addition taken modulo n, is a group under addition because it satisfies all 3 requirements. First, it is associative because addition is associative. The identity is 0 and the inverse of x is $n - x$.

Example 1.3. The group $\{1, 3, 7, 9\} \pmod{10}$ is a group under multiplication because it fulfills all the three requirements above. For multiplication the identity is 1, which is included in the set. Associativity is fulfilled since multiplication as an operation itself is associative, and the inverse requirement $a * b = b * a = e$ is also true for all elements.

Example 1.4. The group $\{1, 2, 4, 7, 8, 11, 13, 14\} \pmod{15}$ is a group under multiplication as well, for the same reasons as above.

Example 1.5. The real numbers under addition, denoted by $(\mathbb{R}, +)$ is a group. In this case, the identity would be 0 since the identity for addition is always 0. Under addition, the inverse of an element x is just $-x$.

Example 1.6. The rational numbers under addition, or $(\mathbb{Q}, +)$ is also a group for similar reasons.

Example 1.7. Integers under addition $(\mathbb{Z}, +)$ is a group because it conforms to all group requirements.

Example 1.8. The set $\mathrm{Mat}_2(\mathbb{R})$ is a group under addition because the identity is the zero matrix $\begin{pmatrix} 0 & 0 \\ 0 & 0 \end{pmatrix}$ and the inverse of an element $\begin{pmatrix} a & b \\ c & d \end{pmatrix}$ is $\begin{pmatrix} -a & -b \\ -c & -d \end{pmatrix}$.

Example 1.9. However, $GL(2, \mathbb{R})$ is a group under multiplication because it fulfills all the requirements for groups listed above. Matrix multiplication is associative. The multiplicative matrix identity is $\begin{pmatrix} 1 & 0 \\ 0 & 1 \end{pmatrix}$, which is in $GL(2, \mathbb{R})$. The inverse of a 2 by 2 matrix $\begin{pmatrix} a & b \\ c & d \end{pmatrix}$ is $\frac{1}{ad-bc}\begin{pmatrix} d & -b \\ -c & a \end{pmatrix}$.

Example 1.10. The free group on two elements $\langle a, b \rangle$ consists of all words formed by a, b, a^{-1}, b^{-1}. It is associative because it is essentially concatenation of words. The identity is the empty word, usually denoted e. The inverse of every word can be formed by reversing the order and then taking the inverse of each letter.

Remark. The free group with two elements is not commutative.

Remark. A similar process can be applied to a free group on three elements $\langle a, b, c \rangle$.

Non-example 1.11. However, the natural numbers under multiplication $(\mathbb{N}, \times)$ is not a group because it is not closed for inverses.

Non-example 1.12. The set $\mathrm{Mat}_2(\mathbb{R})$ is not a group under multiplication because not every matrix has an inverse. For example, $\begin{pmatrix} 0 & 0 \\ 0 & 0 \end{pmatrix}$ does not have a multiplicative inverse because the determinant is 0.

Definition 1.13. We define the **order** of G to be the number of elements in G, and write it as $|G|$.

Definition 1.14. The order of an element $g \in G$ is defined to be the smallest positive integer n such that $g^n = e$, the identity in G. We write this as $\mathrm{ord}_G(g)$.

Proposition 1.15. *For any group element a, $a^k = e$ if and only if $ord_G(a)|k$.*

Proposition 1.16. *If a and b are elements of a finite group G and $ab = ba$, $ord_G(ab)$ divides $ord_G(a) \cdot ord_G(b)$.*

Example 1.17. The order of the identity in any group is always 1, because $e^1 = e$ already.

Example 1.18. The order of 1 in $\mathbb{Z}/n\mathbb{Z}$ under addition is n because n is the smallest positive integer k, such that adding k 1's gives you 0.

Example 1.19. From Example 1.4, the order of 2 in the group is 4 because 4 is the smallest positive integer k such that $2^k \equiv 1 \pmod{15}$.

Example 1.20. The order of any element in $\langle a, b \rangle$ which is not identity (see Example 1.10) is infinity.

1.1 Cyclic groups

Definition 1.21. Cyclic groups are a special type of group in which every element can be written as iterated copies of a single element a, called a generator of G. For example, if the operation is multiplication, then every element is a power of a. A cyclic group G generated by a is written as $G = \langle a \rangle$.

Proposition 1.22. *Subgroups of cyclic groups are cyclic as well.*

Proposition 1.23. *For any group element $a \in G$, $ord_G(a) = |\langle a \rangle|$.*

Proposition 1.24. *In a finite cyclic group, the order of an element divides the order of a group.*

Remark. Cyclic groups can be finite or infinite, however every cyclic group follows the shape of $\mathbb{Z}/n\mathbb{Z}$, which is infinite if and only if $n = 0$ (so then it looks like $\mathbb{Z}$).

Example 1.25. The group $\mathbb{Z}/6\mathbb{Z} = \{0, 1, 2, 3, 4, 5\} \pmod 6$ is a cyclic group, and cyclic subgroups generated by the following elements are listed below:

- $\langle 1 \rangle = \{1, 2, 3, 4, 5, 0\} = \mathbb{Z}/6\mathbb{Z}$.
- $\langle 2 \rangle = \{2, 4, 0\}$.
- $\langle 3 \rangle = \{3, 0\}$.
- $\langle 4 \rangle = \{4, 2, 0\}$.
- $\langle 5 \rangle = \{5, 4, 3, 2, 1, 0\} = \mathbb{Z}/6\mathbb{Z}$.
- $\langle 0 \rangle = \{0\}$, only has one element.

Remark. Notice that the cyclic subgroups 1 and 5 generate the entire group which means that they are the generators of this group.

Example 1.26. The group $\mathbb{Z}/7\mathbb{Z} = \{0, 1, 2, 3, 4, 5, 6\} \pmod 7$ is a cyclic group for similar reasons. In $\mathbb{Z}/7\mathbb{Z}$ every nonzero element generates the group and thus can be considered a generator.

To generalize the previous two examples, we have the following.

Proposition 1.27. *The group $\mathbb{Z}/n\mathbb{Z}$ is cyclic under addition. The generators of this group are all integers x such that x is relatively prime to n.*

2 Subgroups and Quotient Groups

2.1 Subgroups

Definition 2.1. A **subgroup** is a subset H of a group G that is closed under the operation of G, inverses, and contains the identity. It then becomes a group in its own right. Note that associativity is inherited from the parent group and the other two axioms are verified by definition.

Example 2.2. In $\mathbb{Z}/10\mathbb{Z}$, the subset $\{2, 4, 6, 8, 0\}$ is a subgroup under addition because the identity exists and is 0 and the inverse of 2 is 8 and the inverse of 4 is 6. It is also associative because addition is associative.

Example 2.3. The subset $0, 2, 4, 6 \subset \mathbb{Z}/8\mathbb{Z}$ is a subgroup (under addition) since it has identity, inverse, and associativity. Alternatively, we may use the Finite Subgroup Test, see below.

Example 2.4. The subset $1, 4 \subset (\mathbb{Z}/5\mathbb{Z})^{\times}$ is a subgroup as it fulfills all the requirements.

Example 2.5. Another example similar to the previous one is the subset $1, 5, 7, 11 \subset (\mathbb{Z}/12\mathbb{Z})^{\times}$.

Example 2.6. The subset $\mathbb{Q}_{>0}$, which is the multiplicative group of positive rational numbers, is a subgroup of $(\mathbb{R}_{>0}, \times)$, the multiplicative group of positive real numbers. This is because the identity of $\mathbb{Q}_{>0}$ is 1 and the inverse of $x \in \mathbb{Q}_{>0}$ is $1/x$, which is still a positive rational number. Multiplication is also associative.

Non-example 2.7. The positive integers are not a subgroup of $\mathbb{Z}$, which is the additive group of integers. This is because the inverse of 2 is -2, which is not in the positive integers and thus, every element does not have a inverse.

Non-example 2.8. The set $\begin{pmatrix} a & b \\ c & d \end{pmatrix}$ where a, b, c, and d are all positive real numbers is not a subgroup of $\mathrm{Mat}_2(\mathbb{R})$ because the identity, which is the zero matrix $\begin{pmatrix} 0 & 0 \\ 0 & 0 \end{pmatrix}$ is not in the set.

It turns out that it's easy to check if finite subsets are subgroups.

Proposition 2.9. *The Finite Subgroup Test shows that if H is a nonempty finite subset of a group G and if H is closed under the operation of G, then H is a subgroup of G.*

The idea is that for any element $h \in H$, we may take all of its powers. Since they are all in H but H is finite, they must start repeating, so $h^a = h^b$ for $a \neq b$ and we have that h has finite order and hence an inverse in H.

Proposition 2.10. *Let G be a group and let a be any element of G. Then, $\langle a \rangle$ is a subgroup of G.*

Definition 2.11. The **center**, $Z(G)$ of a group G is the subset of elements in G that commute with every element in G:

$$Z(G) = \{a \in G | ax = xa \text{ for all } x \in G\}.$$

Proposition 2.12. *The center of a group G is a subgroup of G.*

Proof. The identity e is in $Z(G)$. In addition, if $a, b \in Z(G)$, then $(ab)x = a(bx) = a(xb) = (ax)b = (xa)b = x(ab)$ for all x in G. Thus, $ab \in Z(G)$. Lastly, if $a \in Z(G)$, then

$$\begin{aligned} xa^{-1} &= exa^{-1}, \\ &= a^{-1}axa^{-1}, \\ &= a^{-1}(ax)a^{-1}, \\ &= a^{-1}(xa)a^{-1}, \\ &= a^{-1}x(aa^{-1}), \\ &= a^{-1}xe, \\ &= a^{-1}x. \end{aligned}$$

Thus, $a^{-1} \in Z(G)$ for all $a \in Z(G)$. □

Somewhat weaker than the condition that an element must commute with *every* element of G, is the condition that it only must commute with some specified element of G.

Definition 2.13. Let a be a fixed element of a group G. The **centralizer** of a in $G, C(a)$, is the set of all elements in G that commute with a. In other terms, $C(a) = \{g \in G \mid ga = ag\}$.

Proposition 2.14. *For all a in a group G, the centralizer of a is a subgroup of G.*

2.2 Cosets

Definition 2.15. Let G be a group and H be a nonempty subset of G. For any $a \in G$, the set $\{ah|h \in H\}$ is denoted by aH and is called the **left coset**; the **right coset** Ha is defined similarly.

Proposition 2.16. *The coset $aH = H$ if and only if $a \in H$.*

Proof. Suppose $aH = H$. Then, $a = ae \in aH = H$. Next, we assume that $a \in H$. $aH \subseteq H$ and $H \supseteq aH$ are both true. The former is true because H is closed. The latter is through the following proof. Let $h \in H$, then $a^{-1}h \in H$ and because $h = eh = (aa^{-1})h = a(a^{-1}h) \in aH$. Thus, $aH = H$. □

Proposition 2.17. *We have that $aH = bH$ if and only if $a \in bH$.*

Proof. If $aH = bH$, then $a = ae \in aH = bH$. If $a \in bH$, then $a = bh$ for some $h \in H$, and therefore, $aH = (bH)H = b(hH) = bH$. □

Proposition 2.18. *The cosets are either disjoint or coincide completely: $aH = bH$ or $aH \cap bH = \emptyset$.*

Proof. If there is an element c in $aH \cap bH$, then $cH = aH$ and $cH = bH$. □

Proposition 2.19. *A coset aH is a subgroup of G if and only if $a \in H$; i.e., the only coset which is a subgroup is the identity coset H.*

Proof. If aH is a subgroup, then it contains e. Thus, $aH \cap eH \neq \emptyset$ and as a result $aH = eH = H$. This means that $a \in H$. If $a \in H$, then $aH = H$. □

Example 2.20. The cosets of $H = \{0, 3, 6\}$ in $\mathbb{Z}/9\mathbb{Z}$ are:

- $0 + H = 3 + H = 6 + H = \{0, 3, 6\}$;
- $1 + H = 4 + H = 7 + H = \{1, 4, 7\}$;
- $2 + H = 5 + H = 8 + H = \{2, 5, 8\}$.

Example 2.21. The cosets of $H = \{\ldots, -4, 0, 4, 8, \ldots\} = 4\mathbb{Z}$ in $(\mathbb{Z}, +)$ are

- $0 + H = \{\ldots, -4, 0, 4, 8, \ldots\}$;
- $1 + H = \{\ldots, -3, 1, 5, 9, \ldots\}$;
- $2 + H = \{\ldots, -2, 2, 6, 10, \ldots\}$;
- $3 + H = \{\ldots, -1, 3, 7, 11, \ldots\}$.

Notice that these cosets act like the group $\mathbb{Z}/4\mathbb{Z}$.

2.3 Lagrange Theorem

One very crucial result in basic group theory is Lagrange's theorem.

Theorem 2.22 (Lagrange)**.** *If G is a finite group and H is a subgroup of G, then:*

1. *$|H|$ divides $|G|$*
2. *The number of distinct left (also, right) cosets of H in G is $|G|/|H|$*

2.4 Normal Subgroups

Definition 2.23. A subgroup H of a group G is called a **normal subgroup** of G if $aH = Ha$ for all a in G. Note that every subgroup in an abelian group is normal!

Proposition 2.24. *The following conditions are equivalent:*

1. *H is a normal subgroup of G.*
2. *$gHg^{-1} \subseteq H$ for all $g \in G$.*
3. *The normalizer of H in G (the set of elements whose conjugation action preserves H) is G, i.e. $N_G(H) = G$.*
4. *There exists a homomorphism φ from G to another group such that $H = \ker(\varphi)$.*

Example 2.25. Let $H = 1$. Then by (2) the trivial subgroup is always a normal subgroup of any group G. This is because gHg^{-1} will be $\{g1g^{-1}\} = \{1\} = H$, which is a subset of H.

Example 2.26. Let $H = G$. Then by (2) the whole group is always a normal subgroup of any group G. This is shown by $gHg^{-1} = gGg^{-1} = G = H$.

Example 2.27. The group $SL(2, \mathbb{R})$ of 2×2 matrices with determinant 1 is a normal subgroup of $GL(2, \mathbb{R})$ (the group of 2×2 matrices with nonzero determinants). If $x \in GL(2, \mathbb{R})$ and $h \in SL(2, \mathbb{R})$, then $\det(xhx^{-1}) = (\det x)(\det h)(\det x)^{-1} = (\det x)(\det x)^{-1} = 1$. Thus, $xhx^{-1} \in H$ and therefore, $xHx^{-1} \subseteq H$.

Example 2.28. The center $Z(G)$ of a group is a normal subgroup because for every $a \in G$ and $h \in Z(G)$, $ah = ha$ (by definition).

Example 2.29. The alternating group A_n of even permutations is a normal subgroup of S_n.

2.5 Quotient Subgroups

Definition 2.30. Let G be a group and let H be a normal subgroup of G. The set $G/H = \{aH | a \in G\}$ is a group under the operation $(aH)(bH) = abH$.

Remark. Note that this is note true if H is not normal!

Example 2.31. Let $4\mathbb{Z} = \{0, \pm 4, \pm 8, ...\} \subset \mathbb{Z}$, as in Example 2.21. The quotient group consists of the cosets of $4\mathbb{Z}$ in $\mathbb{Z}$, which in turn behave like the elements $0, 1, 2, 3$ modulo 4. The quotient group is $\mathbb{Z}/4\mathbb{Z}$, which matches our usual description of this group.

Example 2.32. Let $n\mathbb{Z} = \{0, \pm n, \pm 2n, ...\} \subset \mathbb{Z}$. Then the quotient group $\mathbb{Z}/n\mathbb{Z}$ is $\{0 + n\mathbb{Z}, 1 + n\mathbb{Z}, 2 + n\mathbb{Z}, 3 + n\mathbb{Z}, ..., n - 1 + n\mathbb{Z}\} = \{0, 1, 2, \ldots, n - 1\}$ taken modulo n.

Example 2.33. Let S_n be the permutation group and $A_n \subseteq S_n$ be the alternating group (of even permutations). Then $S_n/A_n \cong \{\pm 1\} \cong \mathbb{Z}/2\mathbb{Z}$ with the identification given by the sign of the permutation.

3 Group Homomorphisms

Definition 3.1. A **homomorphism** ϕ from group G to a group G' is a function that preserves the group's operation. The following requirements must be satisfied:

1. $\phi(ab) = \phi(a)\phi(b)$ and for all $a, b \in G$.
2. The identity maps to identity, i.e. $\phi(e_G) = e_{G'}$.

Definition 3.2. The **kernel** of a homomorphism ϕ from group G to a group G' (with identity e) is the set

$$\{g \in G \mid \phi(g) = e\}.$$

Remark. For subgroups as well, many of its original features are preserved under the image of a homomorphism. For instance, if H is abelian, then $\phi(H)$ is also abelian. If H is normal in G, then $\phi(H)$ is also normal inside $\phi(G)$.

Proposition 3.3. *If ϕ is a group homomorphism from G to G' then $\ker \phi$ is a normal subgroup for G. Conversely, every normal subgroup is the kernel of some group homomorphism from G (to varying targets).*

Proof. We want to show that $axa^{-1} \in \ker \phi$, i.e. that $\phi(axa^{-1}) = e$, for $x \in \ker \phi$ and any $a \in G$. But we have $\phi(axa^{-1}) = \phi(a)\phi(x)\phi(a^{-1}) = \phi(a)e\phi(a)^{-1} = e$, so $\ker \phi$ is a normal subgroup.

Conversely, a normal subgroup N of G satisfies the condition that the cosets G/N form a group. Therefore in the canonical map $G \to G/N$, the kernel is N, so N is indeed the kernel of some homomorphism. □

We now list some properties of groups under homomorphisms.

Proposition 3.4. *Let ϕ be a homomorphism from a group G to a group G' and let g be an element of G. Then the following statements are true.*

1. *ϕ carries the identity of G to the identity of G'.*
2. *$\phi(g^n) = \phi(g))^n$ for all n in $\mathbb{Z}$.*
3. *If $|g|$ is finite, then $|\phi(g)|$ divides $|g|$. If $|G|$ is finite, then $|\phi(g)|$ divides $|g|$ and $|\phi(G)|$.*
4. *$\ker\phi$ is a normal subgroup of G*
5. *$\phi(a) = \phi(b)$ if and only if $ab^{-1} \in \ker\phi$.*
6. *If $\phi(g) = g'$, then $\phi^{-1}(g') = \{x \in G \mid \phi(x) = g'\} = g\ker\phi$.*

We have some additional properties of subgroups under homomorphisms.

Proposition 3.5. *Let ϕ be a homomorphism from a group G to a group G' and let H be a subgroup of G. Then the following statements are true.*

1. *$\phi(H) = \{\phi(h) \mid h \in H\}$ is a subgroup of G'.*
2. *If H is cyclic, then $\phi(H)$ is cyclic.*
3. *If H is abelian, then $\phi(H)$ is abelian.*
4. *If H is normal in G, then $\phi(H)$ is normal in $\phi(G)$ (but not necessarily G'!).*
5. *If $|\ker\phi| = n$, then ϕ is an n to 1 mapping from G onto $\phi(G)$.*
6. *If H is finite, then $|\phi(H)|$ divides $|H|$.*
7. *$\phi(Z(G))$ is a subgroup of $Z(\phi(G))$.*
8. *If K' is a subgroup of G' then $\phi^{-1}(K') = \{k \in G \mid \phi(k) \in K'\}$ is a subgroup of G.*
9. *If K' is a normal subgroup of G', then $\phi^{-1}(K') = \{k \in G \mid \phi(k) \in K'\}$ is a normal subgroup of G .*
10. *If ϕ is onto and $\ker\phi = \{e\}$, then ϕ is an isomorphism from G to G'.*

Example 3.6. The function $f : G \to H$ defined by $f(g) = 1$ for all $g \in G$ is a homomorphism. This is also called the "trivial homomorphism," and it shows that G is a normal subgroup of G.

Example 3.7. An example of a homomorphism is the mod 3 map $\mathbb{Z} \to \mathbb{Z}/3\mathbb{Z}$. This can be seen since $x + y \pmod 3 = x \pmod 3 + y \pmod 3$; for instance, $5 + 2 \pmod 3 = 1$ and $5 \pmod 3 + 2 \pmod 3 = 1$ as well. Clearly, identity maps to identity since 0 maps to $0 \pmod 3 = 0$.

Example 3.8. The determinant map $\det : GL(2,\mathbb{R}) \to \mathbb{R}^\times$, where matrix $A \mapsto \det A$ is a homomorphism because the identity matrix $\begin{pmatrix} 1 & 0 \\ 0 & 1 \end{pmatrix}$ maps to 1 and $\det(A)\det(B) = \det(AB)$.

Example 3.9. The nth power map $f : \mathbb{Q}^\times \to \mathbb{Q}^\times$ defined by $f(x) = x^n$ is a group homomorphism because $1 \mapsto 1$ and $f(xy) = (xy)^n = x^n y^n = f(x)f(y)$.

Example 3.10. The absolute value function $f : \mathbb{C}^* \to \mathbb{R}_{>0}$ is a homomorphism for similar reasons.

Non-example 3.11. The function $f : \mathbb{Z} \to \mathbb{Z}$ defined by $f(x) = x + 1$ is not a group homomorphism since $f(x + y) = x + y + 1 \neq f(x) + f(y) = x + y + 2$.

Non-example 3.12. The function $f : \mathbb{Q}^\times \to \mathbb{Q}^\times$ is defined by $f(x) = 3x$ is not a group homomorphism because $f(xy) = 3xy \neq f(x) \cdot f(y) = 9xy$.

Non-example 3.13. The function $f : \mathbb{Z} \to \mathbb{Z}$ is defined by $f(x) = x^2$ is not a group homomorphism because $f(x+y) = (x+y)^2 = x^2+2xy+y^2 \neq x^2+y^2 = f(x)+f(y)$.

Non-example 3.14. The function $f : GL(2,\mathbb{R}) \to \mathbb{R}^\times$ sending $\begin{pmatrix} a & b \\ c & d \end{pmatrix} \mapsto b$ is not a group homomorphism because the identity matrix, $\begin{pmatrix} 1 & 0 \\ 0 & 1 \end{pmatrix} \mapsto 0$, but the identity of $\mathbb{R}^\times$ is 1, so the identity does not map to the identity. Furthermore, 0 does not even exist in the group $\mathbb{R}^\times$.

3.1 Group Isomorphisms

Definition 3.15. An **isomorphism** is a group homomorphism that is bijective. For such a homomorphism $G \to G'$, we say that G and G' are **isomorphic**.

Generally, a group G can be proven to be isomorphic to group G' through the following three steps:

(1) Mapping: Determine a candidate for the isomorphism; define a homomorphism ϕ from group G to group G'.

(2) Injective: Prove ϕ is injective, so that no two elements map to the same element in G'.

(3) Surjective: Prove that ϕ is surjective, so that for any element g' in G, we can find an element g in G such that $\phi(g) = g'$.

Theorem 3.16 (First Isomorphism Theorem)**.** *Let ϕ be a group homomorphism from G to G'. Then the mapping from $G/\ker\phi$ to $\phi(G)$, given by $g\ker\phi \mapsto \phi(g)$ is an isomorphism.*

Corollary 3.17. *If ϕ is a homomorphism from a finite group G to G', then $|G|/|\ker\phi| = |\phi(G)|$.*

Corollary 3.18. *If ϕ is a homomorphism from a finite group G to G', then $|\phi(G)|$ divides $|G|$ and $|G'|$.*

Proposition 3.19. *Let $\phi : G \to G'$ be an isomorphism. Then the following statements are true.*

1. *ϕ carries the identity of G to the identity of G'.*
2. *For every integer n and for every group element a in G, $\phi(a^n) = [\phi(a)]^n$, or in the additive form, $\phi(na) = n\phi(a)$.*
3. *For any elements a and b in G, a and b commute if and only if $\phi(a)$ and $\phi(b)$ commute as well.*
4. *$G = \langle a \rangle$ if and only if $G' = \langle \phi(a) \rangle$.*
5. *Isomorphisms preserve orders, as $ord_G(a) = ord_{G'}(\phi(a))$ for all a in G.*
6. *For a fixed integer k and a fixed group element b in G, $x^k = b$ has the same number of solutions in G as $x^k = \phi(b)$ has in G'.*
7. *If G is finite, then G and G' have exactly the same number of elements of every order.*
8. *ϕ^{-1} is an isomorphism from G' to G.*
9. *G is abelian if and only if G' is abelian.*
10. *G is cyclic if and only if G' is cyclic.*
11. *If K is a subgroup of G then $\phi(K) = \{\phi(k) \mid k \in K\}$ is a subgroup of G'.*
12. *If K' is a subgroup of G' then $\phi^{-1}(K') = \{g \in G \mid \phi(g) \in K'\}$ is a subgroup of G.*
13. *$\phi(Z(G)) = Z(G')$.*

In other words, if two groups G and G' are isomorphic, *we can really think about them as the same group*, with the identification given by the isomorphism.

Definition 3.20. An automorphism of G is an isomorphism from a group G to itself.

Definition 3.21. Let G be a group and let $a \in G$. Then, the function ϕ_a defined by $\phi_a(x) = axa^{-1}$ for all x in G is called the *inner automorphism of G induced by a*, and is an automorphism of G.

Proposition 3.22. *The set of automorphisms of a group $Aut(G)$ forms a group (under the operation of function composition), and the set of inner automorphisms of a group $Inn(G)$ forms a subgroup of this group.*

Remark. The group $\mathrm{Aut}(G)$ was first studied by O. Holder in 1893 and also independently by E.H. Moore in 1894.

Proposition 3.23. *For every positive integer n, $Aut(\mathbb{Z}/n\mathbb{Z})$ is isomorphic to $(\mathbb{Z}/n\mathbb{Z})^\times$.*

Theorem 3.24 (Cayley 1854)**.** *Every finite group is isomorphic to a subgroup of a permutation group.*

Example 3.25. Let G be real numbers under addition $(\mathbb{R}, +)$ and let G' be the positive real numbers under multiplication, $(\mathbb{R}_{>0}, \times)$. Then G and G' are isomorphic under the mapping $f(x) = e^x$. It is one-to-one since $e^x = e^y \to \log e^x = \log e^y$, thus $x = y$. To prove onto, we must find a value such that $f(x) = y$ will be fulfilled. This value is $\log y$. Finally, it is operation preserving since $f(x + y) = e^(x + y) = e^x \cdot e^y = f(x)f(y)$. Thus, it is an isomorphism.

Non-example 3.26. The mapping from R under addition to itself mapped by $f(x) = x^3$ is not an isomorphism since it is not operation preserving. In other words, $(x + y)^3 \neq x^3 + y^3$ for certain values of x and y.

4 Generators and Relations

Definition 4.1. Let S be some (finite, for now) set of symbols. The **words** formed by S are just finite-length concatenations of s and s^{-1} for all $s \in S$.

Example 4.2. Suppose $S = \{x\}$. Then some examples of words are $xx^{-1}x$, x, and x^{-4}.

Example 4.3. Suppose $S = \{a, b\}$. Then some examples of words are $abaa^{-1}b$, $aba^{-1}ab^{-1}$, and $a^3b^{-5}a^{-2}$.

There's one minor problem with words: xx^{-1} should not be any different that the empty word. We'll remedy that by putting the following equivalence relation of words.

Definition 4.4. For any words u, v of S, we say that $u \sim v$ if v can be obtained from u by a finite sequence of insertions or deletions of words of the form xx^-1 or $x^{-1}x$ where $x \in S$.

Proposition 4.5 (Equivalence classes form a group)**.** *Let S be a set of distinct symbols. For any word u, let W_u denote the set of all words on S equivalent to u. Then the set of all equivalence classes of elements is a group under the operation $u' * v' = uv'$. This is called the **free group on** S.*

To state it again:

Definition 4.6. The free group on elements $\{x_1, \dots, x_n\}$, denoted by $\langle x_1, x_2, ..., x_n \rangle$, consists of all finite-length words formed by $x_1, x_2, ..., x_n, x_1^{-1}, x_2^{-1}, ..., x_n^{-1}$ under the equivalence class described above.

Proposition 4.7. *The free group on one element is $\mathbb{Z}$.*

Example 4.8. For an example of a free group with two elements, see example 1.10.

Example 4.9. A free group with three elements would be $\langle a, b, c \rangle$.

Definition 4.10. Consider the free group on n elements, $x_1, x_2, ..., x_n$. Let $r_1, r_2, ..., r_m$ be elements in this group (these are just words). The group $\langle x_1, x_2, ..., x_n \mid r_1, r_2, ..., r_m \rangle$ is the quotient we get by setting each r_i equal to identity. Simply put, the presentation of a group, G, is an expression of G in terms of generators and relations.

Remark. We can also describe the prior group by considering the smallest normal subgroup N containing $r_1, \dots, r_m$. Then

$$\langle x_1, x_2, ..., x_n \mid r_1, r_2, ..., r_m \rangle \cong \langle x_1, \dots, x_n \rangle / N.$$

Theorem 4.11. *Every group is a homomorphic image of a free group. In other words, every group has a presentation in terms of generators and relations.*

Proof. Every group has presentation $\langle \{x_g \mid g \in G\} \mid x_g x_{g'} = x_{gg'} \forall g, g' \in G \rangle$. (Note that the number of generators and relations may be infinite). We are essentially taking a generator for every element of G, as we don't know which elements generate G. In addition, we impose a relation among the generators for every relation between elements of G. □

Remark. The construction above results in a large amount of relations to check by hands. Generators and relations are important because they allow us to determine how many homomorphisms exist between two groups without checking all necessary relations between all elements.

Proposition 4.12 (Dyck)**.** *Let $G = \langle a_1, a_2, ..., a_n | w_1 = w_2 = ... = w_t = e \rangle$ and let $G' = \langle a_1, a_2, ..., a_n | w_1 = w_2 = ... = w_t = w_{t+1} = ... = w_{t+k} = e \rangle$. Then G' is a homomorphic image of G.*

In other words, we can really think about generators and relations as taking elements which generate a group, *subject to conditions/relations that the generators must satisfy.* Dyck's theorem tells us that by imposing more relations, we get a quotient group! (So if we want more elements to be zero, we just have to quotient them out.)

Example 4.13. The group $\mathbb{Z}/3\mathbb{Z}$ has a presentation $\langle x \mid x^3 = e \rangle$. The x represents the element 1, so $x^3 = e$ just means that $1 + 1 + 1 = 0 \pmod 3$.

Example 4.14. The group $\mathbb{Z}^2$ has a presentation $\langle x, y \mid xy = yx \rangle$. The x and y represent elements $(1, 0)$ and $(0, 1)$, and the relation $xy = yx$ just means that x and y commute, i.e. that $(1, 0) + (0, 1) = (0, 1) + (1, 0)$.

Example 4.15. The symmetric group S_4 has presentation $\langle x_1, x_2, x_3 \mid x_1^2 = x_2^2 = x_3^2 = (x_1 x_2)^3 = (x_2 x_3)^3 = (x_1 x_3)^2 = e \rangle$. The x_i represents the transpositions $(i, i + 1)$.

Notice how these presentations are much simpler than in the constructive proof of Theorem 4.11!

5 Interesting Problems

Lastly, we'll consider two interesting problems.

5.1 Homophones

Let's consider the free group generated by 26 generators, say $a, b, c, d, ..., x, y, z$. Now impose the relations of homophones: that is, for every pair of words which are homophones, set them equal (i.e. read and red, so $read = red$, where the generators are being multiplied). What is this group?

Answer: There are many ways to arrive at the same answer. Here is one plausible solution.

(1) $by = bye \implies e = 1$

(2) $see = sea \implies a = 1$

(3) $buy = by \implies u = 1$

(4) $fir = fur \implies i = 1$

(5) $whole = hole \implies w = 1$

(6) $hour = our \implies h = 1$

(7) $in = inn \implies n = 1$

(8) $knot = not \implies k = 1$

(9) $die = dye \implies y = 1$

(10) $ad = add \implies d = 1$

(11) $all = awl \implies l = 1$

(12) $arc = ark \implies c = 1$

(13) $ate = eight \implies g = 1$

(14) $base = bass \implies s = 1$

(15) $berry = bury \implies r = 1$

(16) $boos = booze \implies s = 1$

(17) $bat = batt \implies t = 1$

(18) $check = cheque \implies q = 1$

(19) $idle = idol \implies o = 1$

(20) $lam = lamb \implies b = 1$

(21) $coo = coup \implies p = 1$

(22) $faze = phase \implies f = 1$

(23) $genes = jeans \implies j = 1$

(24) $flex = flecks \implies x = 1$

(25) $gamma = gama \implies m = 1$

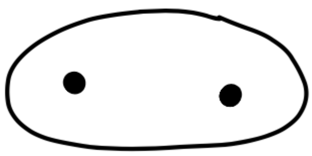
All letters except v are identity. According to Merriam Webster, there are also no relations in v, so it turns out the quotient group is just $\langle v \rangle \cong \mathbb{Z}$.

Remark. According to Prof. Etingof, there is a paper which claims that there is a homophone which also uses v, which then implies that the group is actually trivial. You can ask similar questions about alphabets in other languages as well.

5.2 Unraveling a string

Suppose we have two (infinitely tall) telephone poles. Pavel is a man of chaos and takes a very strong metal chain and loops it around these telephone poles, then fuses the two ends together. He needs a configuration so that you cannot simply pull the chains away from the poles and drag them away; as is, they are knotted around the poles.

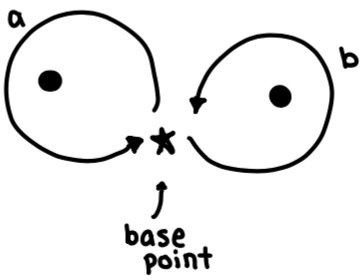
This can be done with the following configuration:



However, he is nice and allows that if they remove a single pole - any pole! - the chain will fall away and can simply be removed from the remaining pole with no problems. Can you find such a configuration? What about 3 poles? What about n poles?

For two poles:

A loop (beginning and ending at this base point) going counterclockwise around the left pole is denoted as a and a loop going counterclockwise around the right pole is denoted as b.

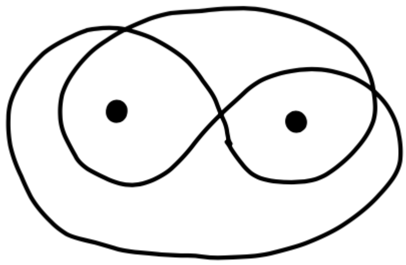


Loops (beginning and ending at the base point, up to homotopy) form a group by concatenation, with inverse being the reverse direction of the loop. This is called the fundamental group: in this case, the group is $\langle a, b \rangle$. The inverse is given by reversing the direction of the loop; for example, a^{-1} is a clockwise motion around the right pole and b^{-1} is a clockwise motion around the left pole.

Let us reformulate the question in terms of group theory.

- A loop is an element of this group $\langle a, b \rangle$.
- A loop that is entangled around the poles and cannot be removed is an element that is not the identity.
- Removing the left pole is the same as setting a to be the identity element. Similarly, removing the right pole is the same as setting b to be the identity element.
- We must find an element $x \in \langle a, b \rangle$ that is not identity, but when either a or b is set to identity, x becomes the identity.

One element that satisfies these conditions is $aba^{-1}b^{-1}$, shown below.



The expression $aba^{-1}b^{-1}$ represents a configuration that follows the requirments of the problem. In the current state with two poles, the chain cannot be taken out. However, when the pole on the right is removed, the expression becomes bb^{-1}, which can be simplified to 1. The same can be said about the other pole.

For three poles:

The concept is very similar, but we now have motion c, which is around the third pole counterclockwise. The expression

$$(aba^{-1}b^{-1})c(aba^{-1}b^{-1})^{-1}c^{-1}$$

is the configuration for 3 poles. By taking out any one of the three poles, we see that the expression reduced to just 1.

For n poles:

Let $a_1, a_2, \ldots, a_n$ be the generators of the fundamental group, where a_i is the counterclockwise loop around the ith pole.

Let x_{n-1} be the solution representing $n-1$ poles. The element $x_{n-1}a_nx_{n-1}^{-1}a_n^{-1}$ represents the solution for n poles.

Why? When either one of the poles from 1 to $n-1$ are removed, x_{n-1} becomes the identity and the element becomes $a_na_n^{-1}$, which is identity. If the nth pole is removed, the element becomes $x_{n-1}x_{n-1}^{-1}$, which is also identity.

Try drawing this out for $n > 3$: you will find it very hard to have discovered by hand! Maybe group theory is quite useful after all.

Acknowledgements

We would like to thank the MIT math department, the PRIMES program at MIT, Pavel Etingof and Slava Gerovitch, who are the organizers and founders of PRIMES, Marisa Gaetz and Mary Stelow who helped organize and manage the PRIMES Circle program and for their feedback on this paper, and our mentor Merrick Cai for his continuous help and support.