Groups: Definition and Examples

Daniel H. Luecking
MASC

March 29, 2024

What are groups and what are they for?

Over the centuries mathematicians have noticed similarities in many problems. This led to attempts to extract the common properties of these problems and study those properties in isolation.

What are groups and what are they for?

Over the centuries mathematicians have noticed similarities in many problems. This led to attempts to extract the common properties of these problems and study those properties in isolation.

This was especially true for problems that involve symmetry, whether in geometry, theory of equations, or combinatorics. Problems that involved symmetry led to the concept of groups.

What are groups and what are they for?

Over the centuries mathematicians have noticed similarities in many problems. This led to attempts to extract the common properties of these problems and study those properties in isolation.

This was especially true for problems that involve symmetry, whether in geometry, theory of equations, or combinatorics. Problems that involved symmetry led to the concept of groups.

The symmetries in geometry are the kinds you learn about in grade school. If a figure has left-right symmetry, that means you can flip the figure over left-to-right *without changing the figure*.

What are groups and what are they for?

Over the centuries mathematicians have noticed similarities in many problems. This led to attempts to extract the common properties of these problems and study those properties in isolation.

This was especially true for problems that involve symmetry, whether in geometry, theory of equations, or combinatorics. Problems that involved symmetry led to the concept of groups.

The symmetries in geometry are the kinds you learn about in grade school. If a figure has left-right symmetry, that means you can flip the figure over left-to-right *without changing the figure*.

There are is also rotation symmetry, meaning you can rotate the figure around a center point some number of degrees *without changing the figure*.

What are groups and what are they for?

Over the centuries mathematicians have noticed similarities in many problems. This led to attempts to extract the common properties of these problems and study those properties in isolation.

This was especially true for problems that involve symmetry, whether in geometry, theory of equations, or combinatorics. Problems that involved symmetry led to the concept of groups.

The symmetries in geometry are the kinds you learn about in grade school. If a figure has left-right symmetry, that means you can flip the figure over left-to-right *without changing the figure*.

There are is also rotation symmetry, meaning you can rotate the figure around a center point some number of degrees *without changing the figure*. The group involved here is not the figure, but rather the collection of *motions* that do not change the figure.

Invertibility is the key

Invertibility is the key

One property that motions of a symmetric figure have is that they can be combined.

Invertibility is the key

One property that motions of a symmetric figure have is that they can be combined. Another key property is: a motion that doesn't change the figure can be undone by another motion:

Invertibility is the key

One property that motions of a symmetric figure have is that they can be combined. Another key property is: a motion that doesn't change the figure can be undone by another motion: If a figure is flipped over, you can flip it back. If it is rotated, you can rotate it back.

Invertibility is the key

One property that motions of a symmetric figure have is that they can be combined. Another key property is: a motion that doesn't change the figure can be undone by another motion: If a figure is flipped over, you can flip it back. If it is rotated, you can rotate it back.

While symmetry can be obvious in geometry, it is not so obvious in other contexts.

Invertibility is the key

One property that motions of a symmetric figure have is that they can be combined. Another key property is: a motion that doesn't change the figure can be undone by another motion: If a figure is flipped over, you can flip it back. If it is rotated, you can rotate it back.

While symmetry can be obvious in geometry, it is not so obvious in other contexts. Nevertheless it often exists below the surface, and the concept of a group can bring it to light.

What is a group?

A group is a set, together with a binary operation.

What is a group?

A group is a set, together with a binary operation. Depending on the example, the operation could be addition, multiplication, or something like "apply two motions in a row".

What is a group?

A group is a set, together with a binary operation. Depending on the example, the operation could be addition, multiplication, or something like "apply two motions in a row".

If I don't want to specify exactly what the operation is, I will use multiplication-like notation. Here I will assume the operation is called '$*$'.

What is a group?

A group is a set, together with a binary operation. Depending on the example, the operation could be addition, multiplication, or something like "apply two motions in a row".

If I don't want to specify exactly what the operation is, I will use multiplication-like notation. Here I will assume the operation is called '$*$'. Then $(G, *)$ is a group if

C1 For any a, b in G, $a * b$ is in G. (We say G is "closed under $*$".)

What is a group?

A group is a set, together with a binary operation. Depending on the example, the operation could be addition, multiplication, or something like “apply two motions in a row”.

If I don’t want to specify exactly what the operation is, I will use multiplication-like notation. Here I will assume the operation is called ‘$*$’. Then $(G, *)$ is a group if

- C1 For any a, b in G, $a * b$ is in G. (We say G is “closed under $*$”.)
- G1 For any a, b, c in G, $(a * b) * c = a * (b * c)$. (We say “$*$ is associative”)

What is a group?

A group is a set, together with a binary operation. Depending on the example, the operation could be addition, multiplication, or something like "apply two motions in a row".

If I don't want to specify exactly what the operation is, I will use multiplication-like notation. Here I will assume the operation is called '$*$'. Then $(G, *)$ is a group if

- C1 For any a, b in G, $a * b$ is in G. (We say G is "closed under $*$".)
- G1 For any a, b, c in G, $(a * b) * c = a * (b * c)$. (We say "$*$ is associative")
- G2 There exists an element $e \in G$ such that for every a in G, $e * a = a = a * e$. (e is called the "identity" element. In examples, it could be 0 or 1 or something else entirely.)

What is a group?

A group is a set, together with a binary operation. Depending on the example, the operation could be addition, multiplication, or something like "apply two motions in a row".

If I don't want to specify exactly what the operation is, I will use multiplication-like notation. Here I will assume the operation is called '$*$'. Then $(G, *)$ is a group if

- C1 For any a, b in G, $a * b$ is in G. (We say G is "closed under $*$".)
- G1 For any a, b, c in G, $(a * b) * c = a * (b * c)$. (We say "$*$ is associative")
- G2 There exists an element $e \in G$ such that for every a in G, $e * a = a = a * e$. (e is called the "identity" element. In examples, it could be 0 or 1 or something else entirely.)
- G3 For any a in G there is another element b such that $a * b = e = b * a$ (b is called the "inverse" of a. In examples, b can be written $-a$ or a^{-1}.)

Examples: groups associated with rings

Example 1: The properties that a ring R is required to have (textbook, section 14.1) include the 4 that groups need when '$+$' is the operation, so $(R, +)$ is a group:

Examples: groups associated with rings

Example 1: The properties that a ring R is required to have (textbook, section 14.1) include the 4 that groups need when '$+$' is the operation, so $(R, +)$ is a group:

1. The closure property is required of all rings

Examples: groups associated with rings

Example 1: The properties that a ring R is required to have (textbook, section 14.1) include the 4 that groups need when '$+$' is the operation, so $(R, +)$ is a group:

1. The closure property is required of all rings
2. The associative property: $(a + b) + c = a + (b + c)$.

Examples: groups associated with rings

Example 1: The properties that a ring R is required to have (textbook, section 14.1) include the 4 that groups need when '$+$' is the operation, so $(R, +)$ is a group:

1. The closure property is required of all rings
2. The associative property: $(a + b) + c = a + (b + c)$.
3. The identity element is 0: $a + 0 = a = 0 + a$.

Examples: groups associated with rings

Example 1: The properties that a ring R is required to have (textbook, section 14.1) include the 4 that groups need when '$+$' is the operation, so $(R, +)$ is a group:

1. The closure property is required of all rings
2. The associative property: $(a + b) + c = a + (b + c)$.
3. The identity element is 0: $a + 0 = a = 0 + a$.
4. The inverse of a is $-a$: $a + -a = 0 = -a + a$.

Examples: groups associated with rings

Example 1: The properties that a ring R is required to have (textbook, section 14.1) include the 4 that groups need when '$+$' is the operation, so $(R, +)$ is a group:

1. The closure property is required of all rings
2. The associative property: $(a + b) + c = a + (b + c)$.
3. The identity element is 0: $a + 0 = a = 0 + a$.
4. The inverse of a is $-a$: $a + -a = 0 = -a + a$.

Example 2: If a ring R has a unity, then the set of units $u(R)$ is a group where the operation is multiplication.

Examples: groups associated with rings

Example 1: The properties that a ring R is required to have (textbook, section 14.1) include the 4 that groups need when '$+$' is the operation, so $(R, +)$ is a group:

1. The closure property is required of all rings
2. The associative property: $(a + b) + c = a + (b + c)$.
3. The identity element is 0: $a + 0 = a = 0 + a$.
4. The inverse of a is $-a$: $a + -a = 0 = -a + a$.

Example 2: If a ring R has a unity, then the set of units $u(R)$ is a group where the operation is multiplication.

1. The closure property follows from the fact that if a, b are in $u(R)$ then $(ab)^{-1} = b^{-1}a^{-1}$ so ab is also a unit.

Examples: groups associated with rings

Example 1: The properties that a ring R is required to have (textbook, section 14.1) include the 4 that groups need when '$+$' is the operation, so $(R, +)$ is a group:

1. The closure property is required of all rings
2. The associative property: $(a + b) + c = a + (b + c)$.
3. The identity element is 0: $a + 0 = a = 0 + a$.
4. The inverse of a is $-a$: $a + -a = 0 = -a + a$.

Example 2: If a ring R has a unity, then the set of units $u(R)$ is a group where the operation is multiplication.

1. The closure property follows from the fact that if a, b are in $u(R)$ then $(ab)^{-1} = b^{-1}a^{-1}$ so ab is also a unit.
2. The associative property $(ab)c = a(bc)$ a basic condition for rings.

Examples: groups associated with rings

Example 1: The properties that a ring R is required to have (textbook, section 14.1) include the 4 that groups need when '$+$' is the operation, so $(R, +)$ is a group:

1. The closure property is required of all rings
2. The associative property: $(a + b) + c = a + (b + c)$.
3. The identity element is 0: $a + 0 = a = 0 + a$.
4. The inverse of a is $-a$: $a + -a = 0 = -a + a$.

Example 2: If a ring R has a unity, then the set of units $u(R)$ is a group where the operation is multiplication.

1. The closure property follows from the fact that if a, b are in $u(R)$ then $(ab)^{-1} = b^{-1}a^{-1}$ so ab is also a unit.
2. The associative property $(ab)c = a(bc)$ a basic condition for rings.
3. The identity element is the unity u: $a \cdot u = a = u \cdot a$.

Examples: groups associated with rings

Example 1: The properties that a ring R is required to have (textbook, section 14.1) include the 4 that groups need when '$+$' is the operation, so $(R, +)$ is a group:

1. The closure property is required of all rings
2. The associative property: $(a + b) + c = a + (b + c)$.
3. The identity element is 0: $a + 0 = a = 0 + a$.
4. The inverse of a is $-a$: $a + -a = 0 = -a + a$.

Example 2: If a ring R has a unity, then the set of units $u(R)$ is a group where the operation is multiplication.

1. The closure property follows from the fact that if a, b are in $u(R)$ then $(ab)^{-1} = b^{-1}a^{-1}$ so ab is also a unit.
2. The associative property $(ab)c = a(bc)$ a basic condition for rings.
3. The identity element is the unity u: $a \cdot u = a = u \cdot a$.
4. The inverse of a is a^{-1}. It is also a unit.

Permutations

The permutations of a finite set A, can be viewed as one-to-one functions from the set of possible positions to the set A.

Permutations

The permutations of a finite set A, can be viewed as one-to-one functions from the set of possible positions to the set A. But we've seen that 'positions' are not required for permutations. We can consider all one-to-one functions from any set X to A and count them as permutations.

Permutations

The permutations of a finite set A, can be viewed as one-to-one functions from the set of possible positions to the set A. But we've seen that 'positions' are not required for permutations. We can consider all one-to-one functions from any set X to A and count them as permutations.

To get a group out of this we need one-to-one functions from A to A.

Permutations

The permutations of a finite set A, can be viewed as one-to-one functions from the set of possible positions to the set A. But we've seen that 'positions' are not required for permutations. We can consider all one-to-one functions from any set X to A and count them as permutations.

To get a group out of this we need one-to-one functions from A to A. If A has n elements we call S_n the set of all one-to-one functions from A to A, with the operation of composition (denoted $f \circ g$, defined by $(f \circ g)(x) = f(g(x))$).

Permutations

The permutations of a finite set A, can be viewed as one-to-one functions from the set of possible positions to the set A. But we've seen that 'positions' are not required for permutations. We can consider all one-to-one functions from any set X to A and count them as permutations.

To get a group out of this we need one-to-one functions from A to A. If A has n elements we call S_n the set of all one-to-one functions from A to A, with the operation of composition (denoted $f \circ g$, defined by $(f \circ g)(x) = f(g(x))$). We call S_n *the symmetric group on n objects*. It has $n!$ elements.

Permutations

The permutations of a finite set A, can be viewed as one-to-one functions from the set of possible positions to the set A. But we've seen that 'positions' are not required for permutations. We can consider all one-to-one functions from any set X to A and count them as permutations.

To get a group out of this we need one-to-one functions from A to A. If A has n elements we call S_n the set of all one-to-one functions from A to A, with the operation of composition (denoted $f \circ g$, defined by $(f \circ g)(x) = f(g(x))$). We call S_n *the symmetric group on n objects*. It has $n!$ elements.

1. The composition of two one-to-one functions in S_n is also one-to-one.

Permutations

The permutations of a finite set A, can be viewed as one-to-one functions from the set of possible positions to the set A. But we've seen that 'positions' are not required for permutations. We can consider all one-to-one functions from any set X to A and count them as permutations.

To get a group out of this we need one-to-one functions from A to A. If A has n elements we call S_n the set of all one-to-one functions from A to A, with the operation of composition (denoted $f \circ g$, defined by $(f \circ g)(x) = f(g(x))$). We call S_n *the symmetric group on n objects*. It has $n!$ elements.

1. The composition of two one-to-one functions in S_n is also one-to-one.
2. The associative property $f \circ (g \circ h) = (f \circ g) \circ h$ comes from the fact that when applied to some element x both ultimately equal $f(g(h(x)))$.

Permutations

The permutations of a finite set A, can be viewed as one-to-one functions from the set of possible positions to the set A. But we've seen that 'positions' are not required for permutations. We can consider all one-to-one functions from any set X to A and count them as permutations.

To get a group out of this we need one-to-one functions from A to A. If A has n elements we call S_n the set of all one-to-one functions from A to A, with the operation of composition (denoted $f \circ g$, defined by $(f \circ g)(x) = f(g(x))$). We call S_n *the symmetric group on n objects*. It has $n!$ elements.

1. The composition of two one-to-one functions in S_n is also one-to-one.
2. The associative property $f \circ (g \circ h) = (f \circ g) \circ h$ comes from the fact that when applied to some element x both ultimately equal $f(g(h(x)))$.
3. The identity element is the identity function: $\mathrm{id}(x) = x$.

Permutations

The permutations of a finite set A, can be viewed as one-to-one functions from the set of possible positions to the set A. But we've seen that 'positions' are not required for permutations. We can consider all one-to-one functions from any set X to A and count them as permutations.

To get a group out of this we need one-to-one functions from A to A. If A has n elements we call S_n the set of all one-to-one functions from A to A, with the operation of composition (denoted $f \circ g$, defined by $(f \circ g)(x) = f(g(x))$). We call S_n *the symmetric group on n objects*. It has $n!$ elements.

1. The composition of two one-to-one functions in S_n is also one-to-one.
2. The associative property $f \circ (g \circ h) = (f \circ g) \circ h$ comes from the fact that when applied to some element x both ultimately equal $f(g(h(x)))$.
3. The identity element is the identity function: $\mathrm{id}(x) = x$.
4. The inverse of f in S_n is the inverse function.

Properties of groups

If it is not specified what group G we are dealing with, we will always use the same notation as if the operation is multiplication.

Properties of groups

If it is not specified what group G we are dealing with, we will always use the same notation as if the operation is multiplication. That is, writing ab or $a \cdot b$ instead of something like $a * b$.

Properties of groups

If it is not specified what group G we are dealing with, we will always use the same notation as if the operation is multiplication. That is, writing ab or $a \cdot b$ instead of something like $a * b$.

- The cancellation properties: if $ab = ac$ then $b = c$. This is because we can "multiply" both sides by a^{-1} to get $a^{-1}(ab) = a^{-1}(ac)$ then regroup to $(a^{-1}a)b = (a^{-1}a)c$. This is $eb = ec$ which says $b = c$. Similarly, if $ba = ca$ then $b = c$.

Properties of groups

If it is not specified what group G we are dealing with, we will always use the same notation as if the operation is multiplication. That is, writing ab or $a \cdot b$ instead of something like $a * b$.

- The cancellation properties: if $ab = ac$ then $b = c$. This is because we can "multiply" both sides by a^{-1} to get $a^{-1}(ab) = a^{-1}(ac)$ then regroup to $(a^{-1}a)b = (a^{-1}a)c$. This is $eb = ec$ which says $b = c$. Similarly, if $ba = ca$ then $b = c$.
- The identity is unique: if $ba = a$ write this as $ba = ea$ and then cancellation gives $b = e$.

Properties of groups

If it is not specified what group G we are dealing with, we will always use the same notation as if the operation is multiplication. That is, writing ab or $a \cdot b$ instead of something like $a * b$.

- The cancellation properties: if $ab = ac$ then $b = c$. This is because we can "multiply" both sides by a^{-1} to get $a^{-1}(ab) = a^{-1}(ac)$ then regroup to $(a^{-1}a)b = (a^{-1}a)c$. This is $eb = ec$ which says $b = c$. Similarly, if $ba = ca$ then $b = c$.
- The identity is unique: if $ba = a$ write this as $ba = ea$ and then cancellation gives $b = e$.
- The inverse is unique: if b and c are inverses of a, so that $ab = e = ac$, use cancellation to get $b = c$.

Order of a group

It is traditional to call the size of a group G its 'order'. For example the order of $\mathbb{Z}_n$ (a group with addition) is n.

Order of a group

It is traditional to call the size of a group G its 'order'. For example the order of $\mathbb{Z}_n$ (a group with addition) is n.

The order of $u(\mathbb{Z}_n)$ (the group of units of the ring $\mathbb{Z}_n$) is $\phi(n)$ (because that is the number of units in $\mathbb{Z}_n$).

Order of a group

It is traditional to call the size of a group G its ‘order’. For example the order of $\mathbb{Z}_n$ (a group with addition) is n.

The order of $u(\mathbb{Z}_n)$ (the group of units of the ring $\mathbb{Z}_n$) is $\phi(n)$ (because that is the number of units in $\mathbb{Z}_n$).

The order of S_n is $n!$.

Order of a group

It is traditional to call the size of a group G its 'order'. For example the order of $\mathbb{Z}_n$ (a group with addition) is n.

The order of $u(\mathbb{Z}_n)$ (the group of units of the ring $\mathbb{Z}_n$) is $\phi(n)$ (because that is the number of units in $\mathbb{Z}_n$).

The order of S_n is $n!$.

Going back to the idea of motions of a symmetric figure, the set of motions of a square has order 8:

Order of a group

It is traditional to call the size of a group G its 'order'. For example the order of $\mathbb{Z}_n$ (a group with addition) is n.

The order of $u(\mathbb{Z}_n)$ (the group of units of the ring $\mathbb{Z}_n$) is $\phi(n)$ (because that is the number of units in $\mathbb{Z}_n$).

The order of S_n is $n!$.

Going back to the idea of motions of a symmetric figure, the set of motions of a square has order 8: 4 lines of symmetry (vertical, horizontal and 2 diagonals) give 4 'flipping over' motions.

Order of a group

It is traditional to call the size of a group G its 'order'. For example the order of $\mathbb{Z}_n$ (a group with addition) is n.

The order of $u(\mathbb{Z}_n)$ (the group of units of the ring $\mathbb{Z}_n$) is $\phi(n)$ (because that is the number of units in $\mathbb{Z}_n$).

The order of S_n is $n!$.

Going back to the idea of motions of a symmetric figure, the set of motions of a square has order 8: 4 lines of symmetry (vertical, horizontal and 2 diagonals) give 4 'flipping over' motions. There are four rotations (by 0°, 90°, 180° and 270°). We'll have more to say about these kinds of groups later in the chapter.

A further look at examples

First a definition. A group G is called *Abelian* (or *abelian*) if $ab = ba$ for all a, b in G. (Named after the mathematician Niels Henrik Abel.)

A further look at examples

First a definition. A group G is called *Abelian* (or *abelian*) if $ab = ba$ for all a, b in G. (Named after the mathematician Niels Henrik Abel.)

A ring with addition is Abelian: $a + b = b + a$ is one of the requirements for rings.

A further look at examples

First a definition. A group G is called *Abelian* (or *abelian*) if $ab = ba$ for all a, b in G. (Named after the mathematician Niels Henrik Abel.)

A ring with addition is Abelian: $a + b = b + a$ is one of the requirements for rings.

The group of units of a ring may not be Abelian, but if R is a commutative ring then it is. In particular, $u(\mathbb{Z}_n)$ is Abelian.

A further look at examples

First a definition. A group G is called *Abelian* (or *abelian*) if $ab = ba$ for all a, b in G. (Named after the mathematician Niels Henrik Abel.)

A ring with addition is Abelian: $a + b = b + a$ is one of the requirements for rings.

The group of units of a ring may not be Abelian, but if R is a commutative ring then it is. In particular, $u(\mathbb{Z}_n)$ is Abelian.

Some other groups associated with integers:

- The group of units of the ring $\mathbb{Z}$ is $\{1, -1\}$ with multiplication for the operation.

A further look at examples

First a definition. A group G is called *Abelian* (or *abelian*) if $ab = ba$ for all a, b in G. (Named after the mathematician Niels Henrik Abel.)

A ring with addition is Abelian: $a + b = b + a$ is one of the requirements for rings.

The group of units of a ring may not be Abelian, but if R is a commutative ring then it is. In particular, $u(\mathbb{Z}_n)$ is Abelian.

Some other groups associated with integers:

- The group of units of the ring $\mathbb{Z}$ is $\{1, -1\}$ with multiplication for the operation.
- The additive group of $\mathbb{Z}_2$ is $\{0, 1\}$ with addition mod 2.

A further look at examples

First a definition. A group G is called *Abelian* (or *abelian*) if $ab = ba$ for all a, b in G. (Named after the mathematician Niels Henrik Abel.)

A ring with addition is Abelian: $a + b = b + a$ is one of the requirements for rings.

The group of units of a ring may not be Abelian, but if R is a commutative ring then it is. In particular, $u(\mathbb{Z}_n)$ is Abelian.

Some other groups associated with integers:

- The group of units of the ring $\mathbb{Z}$ is $\{1, -1\}$ with multiplication for the operation.
- The additive group of $\mathbb{Z}_2$ is $\{0, 1\}$ with addition mod 2.
- The additive group of $\mathbb{Z}_2^n$ consists of strings of bits with length n. The operation is bitwise addition mod 2 (i.e., the bitwise $\textsc{xor}$).

More on permutations

Consider S_4, the permutations of a set A with 4 elements. The set doesn't really matter, so let's use $A = \{1, 2, 3, 4\}$.

More on permutations

Consider S_4, the permutations of a set A with 4 elements. The set doesn't really matter, so let's use $A = \{1, 2, 3, 4\}$.

We need a notation that allows us to quickly define permutations. We use one based on defining a function with a table of values.

More on permutations

Consider S_4, the permutations of a set A with 4 elements. The set doesn't really matter, so let's use $A = \{1, 2, 3, 4\}$.

We need a notation that allows us to quickly define permutations. We use one based on defining a function with a table of values. For example, the table

$$\begin{array}{r|cccc} x & 1 & 2 & 3 & 4 \\ \hline f(x) & 2 & 3 & 1 & 4 \end{array}$$

defines a function f whose values are obtained by looking up x in the first row and reading off the value $f(x)$ below it.

More on permutations

Consider S_4, the permutations of a set A with 4 elements. The set doesn't really matter, so let's use $A = \{1, 2, 3, 4\}$.

We need a notation that allows us to quickly define permutations. We use one based on defining a function with a table of values. For example, the table

x	1	2	3	4
$f(x)$	2	3	1	4

defines a function f whose values are obtained by looking up x in the first row and reading off the value $f(x)$ below it. Notice that the second row is a permutation of the first row. Every different permutation will produce a different one-to-one function. This is in part why we simply call these functions permutations.

Permutation notation

It is traditional to name permutations with Greek letters. It is also traditional to write the composition of two permutation, say α and β, by $\alpha\beta$.

Permutation notation

It is traditional to name permutations with Greek letters. It is also traditional to write the composition of two permutation, say α and β, by $\alpha\beta$. This is interpreted as 'first α then β'. [In function notation this would be $\beta(\alpha(x))$ because we evaluate innermost parentheses first.].

Permutation notation

It is traditional to name permutations with Greek letters. It is also traditional to write the composition of two permutation, say α and β, by $\alpha\beta$. This is interpreted as 'first α then β'. [In function notation this would be $\beta(\alpha(x))$ because we evaluate innermost parentheses first.]. We abbreviate the table on the previous page as $\alpha = \begin{pmatrix} 1 & 2 & 3 & 4 \\ 2 & 3 & 1 & 4 \end{pmatrix}$, which defines α to be the same function as f.

Permutation notation

It is traditional to name permutations with Greek letters. It is also traditional to write the composition of two permutation, say α and β, by $\alpha\beta$. This is interpreted as 'first α then β'. [In function notation this would be $\beta(\alpha(x))$ because we evaluate innermost parentheses first.]. We abbreviate the table on the previous page as $\alpha = \begin{pmatrix} 1 & 2 & 3 & 4 \\ 2 & 3 & 1 & 4 \end{pmatrix}$, which defines α to be the same function as f.

If $\beta = \begin{pmatrix} 1 & 2 & 3 & 4 \\ 3 & 4 & 1 & 2 \end{pmatrix}$ then $\alpha\beta = \begin{pmatrix} 1 & 2 & 3 & 4 \\ 4 & 1 & 3 & 2 \end{pmatrix}$. The following diagrams can help to see this.

Permutation notation

It is traditional to name permutations with Greek letters. It is also traditional to write the composition of two permutation, say α and β, by $\alpha\beta$. This is interpreted as 'first α then β'. [In function notation this would be $\beta(\alpha(x))$ because we evaluate innermost parentheses first.]. We abbreviate the table on the previous page as $\alpha = \begin{pmatrix} 1 & 2 & 3 & 4 \\ 2 & 3 & 1 & 4 \end{pmatrix}$, which defines α to be the same function as f.

If $\beta = \begin{pmatrix} 1 & 2 & 3 & 4 \\ 3 & 4 & 1 & 2 \end{pmatrix}$ then $\alpha\beta = \begin{pmatrix} 1 & 2 & 3 & 4 \\ 4 & 1 & 3 & 2 \end{pmatrix}$. The following diagrams can help to see this.

We can visualize functions using arrows.

Permutation notation

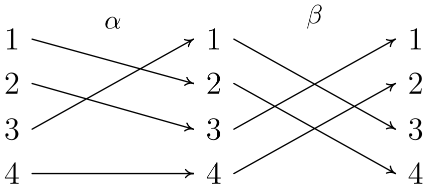
It is traditional to name permutations with Greek letters. It is also traditional to write the composition of two permutation, say α and β, by $\alpha\beta$. This is interpreted as 'first α then β'. [In function notation this would be $\beta(\alpha(x))$ because we evaluate innermost parentheses first.]. We abbreviate the table on the previous page as $\alpha = \begin{pmatrix} 1 & 2 & 3 & 4 \\ 2 & 3 & 1 & 4 \end{pmatrix}$, which defines α to be the same function as f.

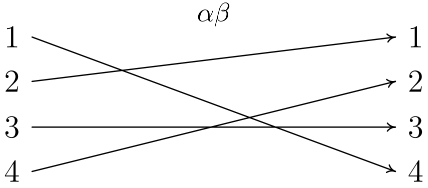
If $\beta = \begin{pmatrix} 1 & 2 & 3 & 4 \\ 3 & 4 & 1 & 2 \end{pmatrix}$ then $\alpha\beta = \begin{pmatrix} 1 & 2 & 3 & 4 \\ 4 & 1 & 3 & 2 \end{pmatrix}$. The following diagrams can help to see this.

We can visualize functions using arrows. On the next slide we see arrows used to represent α and β, as well as $\alpha\beta$

Aids in composing permutation

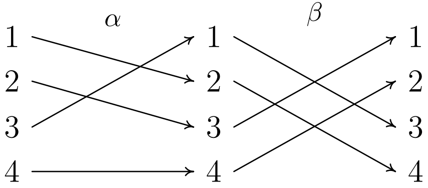
Below $\alpha = \begin{pmatrix} 1 & 2 & 3 & 4 \\ 2 & 3 & 1 & 4 \end{pmatrix}$, $\beta = \begin{pmatrix} 1 & 2 & 3 & 4 \\ 3 & 4 & 1 & 2 \end{pmatrix}$, and $\alpha\beta = \begin{pmatrix} 1 & 2 & 3 & 4 \\ 4 & 1 & 3 & 2 \end{pmatrix}$.

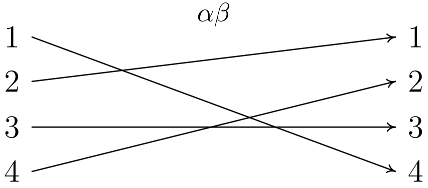




Aids in composing permutation

Below $\alpha = \begin{pmatrix} 1 & 2 & 3 & 4 \\ 2 & 3 & 1 & 4 \end{pmatrix}$, $\beta = \begin{pmatrix} 1 & 2 & 3 & 4 \\ 3 & 4 & 1 & 2 \end{pmatrix}$, and $\alpha\beta = \begin{pmatrix} 1 & 2 & 3 & 4 \\ 4 & 1 & 3 & 2 \end{pmatrix}$.





To get the second figure from the first, connect the head of an α-arrow to the tail of the β-arrow and straighten it out.

Aids in visualizing permutations

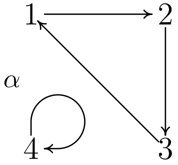
We can imagine permutations as representing motions. If $1, 2, 3,$ and 4 label four points in a plane (or in space) we can imagine a permutation as moving one point to another.

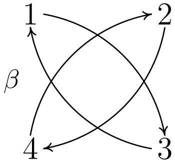
Aids in visualizing permutations

We can imagine permutations as representing motions. If $1, 2, 3$, and 4 label four points in a plane (or in space) we can imagine a permutation as moving one point to another. For example, α from before moves 1 to 2, 2 to 3, and 3 to 1 while leaving 4 where it is.

Aids in visualizing permutations

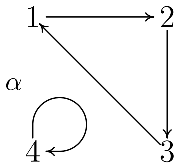
We can imagine permutations as representing motions. If $1, 2, 3,$ and 4 label four points in a plane (or in space) we can imagine a permutation as moving one point to another. For example, α from before moves 1 to 2, 2 to 3, and 3 to 1 while leaving 4 where it is. We can represent this with arrows connecting the points. This is done below for α and β

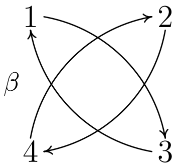




Aids in visualizing permutations

We can imagine permutations as representing motions. If $1, 2, 3$, and 4 label four points in a plane (or in space) we can imagine a permutation as moving one point to another. For example, α from before moves 1 to 2, 2 to 3, and 3 to 1 while leaving 4 where it is. We can represent this with arrows connecting the points. This is done below for α and β

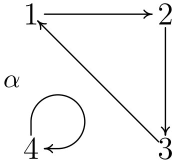


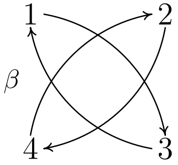


This can be used to compute $\alpha\alpha$. Just follow two arrows.

Aids in visualizing permutations

We can imagine permutations as representing motions. If $1, 2, 3$, and 4 label four points in a plane (or in space) we can imagine a permutation as moving one point to another. For example, α from before moves 1 to 2, 2 to 3, and 3 to 1 while leaving 4 where it is. We can represent this with arrows connecting the points. This is done below for α and β

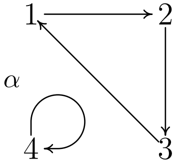


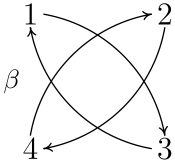


This can be used to compute $\alpha\alpha$. Just follow two arrows. For example starting from 1, the arrows go to 2 then 3, so we see that $\alpha\alpha$ moves 1 to 3.

Aids in visualizing permutations

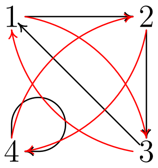
We can imagine permutations as representing motions. If $1, 2, 3$, and 4 label four points in a plane (or in space) we can imagine a permutation as moving one point to another. For example, α from before moves 1 to 2, 2 to 3, and 3 to 1 while leaving 4 where it is. We can represent this with arrows connecting the points. This is done below for α and β



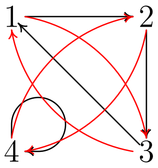


This can be used to compute $\alpha\alpha$. Just follow two arrows. For example starting from 1, the arrows go to 2 then 3, so we see that $\alpha\alpha$ moves 1 to 3. It is not so useful for computing $\alpha\beta$. One can do that by drawing both permutations in the same figure, with different colored arrows. See the figure on the next page.

Composing permutations as motions

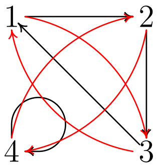


Composing permutations as motions

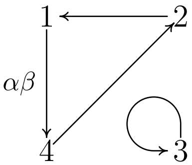


We can then follow the black arrow from 1 to 2 and then the red arrow from 2 to 4 to see that $\alpha\beta$ moves 1 to 4.

Composing permutations as motions



We can then follow the black arrow from 1 to 2 and then the red arrow from 2 to 4 to see that $\alpha\beta$ moves 1 to 4. This gives



From this we can read off $\alpha\beta = \begin{pmatrix} 1 & 2 & 3 & 4 \\ 4 & 1 & 3 & 2 \end{pmatrix}$.