§3.1 Definition of a Group

Shaoyun Yi

MATH 546/701I

University of South Carolina

May 13-14, 2020

Review

Review

- Permutation $\sigma \in \mathrm{Sym}(S)$ (or S_n)

Review

- Permutation $\sigma \in \mathrm{Sym}(S)$ (or S_n)
- $|S_n| = n!$

Review

- Permutation $\sigma \in \mathrm{Sym}(S)$ (or S_n)
- $|S_n| = n!$
- Composition (or Product) $\sigma\tau$ & Inverse σ^{-1}

Review

- Permutation $\sigma \in \mathrm{Sym}(S)$ (or S_n)
- $|S_n| = n!$
- Composition (or Product) $\sigma\tau$ & Inverse σ^{-1}
- Cycle of length k: $\sigma = (a_1 a_2 \cdots a_k)$

Review

- Permutation $\sigma \in \mathrm{Sym}(S)$ (or S_n)
- $|S_n| = n!$
- Composition (or Product) $\sigma\tau$ & Inverse σ^{-1}
- Cycle of length k: $\sigma = (a_1 a_2 \cdots a_k)$
- Disjoint cycles are commutative

Review

- Permutation $\sigma \in \mathrm{Sym}(S)$ (or S_n)
- $|S_n| = n!$
- Composition (or Product) $\sigma\tau$ & Inverse σ^{-1}
- Cycle of length k: $\sigma = (a_1 a_2 \cdots a_k)$
- Disjoint cycles are commutative
- $\sigma \in S_n$ can be written as a (unique) product of disjoint cycles.

Review

- Permutation $\sigma \in \mathrm{Sym}(S)$ (or S_n)
- $|S_n| = n!$
- Composition (or Product) $\sigma\tau$ & Inverse σ^{-1}
- Cycle of length k: $\sigma = (a_1 a_2 \cdots a_k)$
- Disjoint cycles are commutative
- $\sigma \in S_n$ can be written as a (unique) product of disjoint cycles.
- A cycle of length m has order m.

Review

- Permutation $\sigma \in \mathrm{Sym}(S)$ (or S_n)
- $|S_n| = n!$
- Composition (or Product) $\sigma\tau$ & Inverse σ^{-1}
- Cycle of length k: $\sigma = (a_1 a_2 \cdots a_k)$
- Disjoint cycles are commutative
- $\sigma \in S_n$ can be written as a (unique) product of disjoint cycles.
- A cycle of length m has order m.
- The order of σ is the **lcm** of the lengths of its disjoint cycles.

Review

- Permutation $\sigma \in \mathrm{Sym}(S)$ (or S_n)
- $|S_n| = n!$
- Composition (or Product) $\sigma\tau$ & Inverse σ^{-1}
- Cycle of length k: $\sigma = (a_1 a_2 \cdots a_k)$
- Disjoint cycles are commutative
- $\sigma \in S_n$ can be written as a (unique) product of disjoint cycles.
- A cycle of length m has order m.
- The order of σ is the **lcm** of the lengths of its disjoint cycles.
- A **transposition** is a cycle $(a_1 a_2)$ of length two.

Review

- Permutation $\sigma \in \mathrm{Sym}(S)$ (or S_n)
- $|S_n| = n!$
- Composition (or Product) $\sigma\tau$ & Inverse σ^{-1}
- Cycle of length k: $\sigma = (a_1 a_2 \cdots a_k)$
- Disjoint cycles are commutative
- $\sigma \in S_n$ can be written as a (unique) product of disjoint cycles.
- A cycle of length m has order m.
- The order of σ is the **lcm** of the lengths of its disjoint cycles.
- A **transposition** is a cycle $(a_1 a_2)$ of length two.
- $\sigma \in S_n$ can be written as a product of transpositions. (NOT unique)

Review

- Permutation $\sigma \in \mathrm{Sym}(S)$ (or S_n)
- $|S_n| = n!$
- Composition (or Product) $\sigma\tau$ & Inverse σ^{-1}
- Cycle of length k: $\sigma = (a_1 a_2 \cdots a_k)$
- Disjoint cycles are commutative
- $\sigma \in S_n$ can be written as a (unique) product of disjoint cycles.
- A cycle of length m has order m.
- The order of σ is the **lcm** of the lengths of its disjoint cycles.
- A **transposition** is a cycle $(a_1 a_2)$ of length two.
- $\sigma \in S_n$ can be written as a product of transpositions. (NOT unique)
- Even permutation vs. Odd permutation

Review

- Permutation $\sigma \in \mathrm{Sym}(S)$ (or S_n)
- $|S_n| = n!$
- Composition (or Product) $\sigma\tau$ & Inverse σ^{-1}
- Cycle of length k: $\sigma = (a_1 a_2 \cdots a_k)$
- Disjoint cycles are commutative
- $\sigma \in S_n$ can be written as a (unique) product of disjoint cycles.
- A cycle of length m has order m.
- The order of σ is the **lcm** of the lengths of its disjoint cycles.
- A **transposition** is a cycle $(a_1 a_2)$ of length two.
- $\sigma \in S_n$ can be written as a product of transpositions. (NOT unique)
- Even permutation vs. Odd permutation
- a cycle of odd length is even and a cycle of even length is odd.

Motivation

Symmetry occurs frequently and in many forms in nature.

Motivation

Symmetry occurs frequently and in many forms in nature.

Example 1

Each coefficient of a poly. is a symmetric function of the poly.'s roots.

$$f(x) = (x - r_1)(x - r_2)(x - r_3) = x^3 + bx^2 + cx + d, \text{ where}$$

$$r_1 + r_2 + r_3 = -b, \quad r_1 r_2 + r_2 r_3 + r_3 r_1 = c, \quad \text{and } r_1 r_2 r_3 = -d.$$

The coefficients remain unchanged under any permutation of the roots.

Motivation

Symmetry occurs frequently and in many forms in nature.

Example 1

Each coefficient of a poly. is a symmetric function of the poly.'s roots.

$$f(x) = (x - r_1)(x - r_2)(x - r_3) = x^3 + bx^2 + cx + d, \text{ where}$$

$$r_1 + r_2 + r_3 = -b, \quad r_1 r_2 + r_2 r_3 + r_3 r_1 = c, \quad \text{and } r_1 r_2 r_3 = -d.$$

The coefficients remain unchanged under any permutation of the roots.

The important feature of symmetry is the way that the shapes (roots) can be changed while the whole figure (the coefficients) remains unchanged.

Motivation

Symmetry occurs frequently and in many forms in nature.

Example 1

Each coefficient of a poly. is a symmetric function of the poly.'s roots.

$$f(x) = (x - r_1)(x - r_2)(x - r_3) = x^3 + bx^2 + cx + d, \text{ where}$$

$$r_1 + r_2 + r_3 = -b, \quad r_1 r_2 + r_2 r_3 + r_3 r_1 = c, \quad \text{and } r_1 r_2 r_3 = -d.$$

The coefficients remain unchanged under any permutation of the roots.

The important feature of symmetry is the way that the shapes (roots) can be changed while the whole figure (the coefficients) remains unchanged.

With respect to symmetry, *geometrically* the important thing is not the position of the points but the **operation** of moving them.
Similarly, with respect to considering *the roots of polynomials*, it is the **operation** of shifting the roots among themselves that is most important and not the roots themselves.

Binary operation

Definition 2

A **binary operation** $*$ on a set S is a function

$$*: S \times S \to S$$

from the set $S \times S$ of all ordered pairs of elements in S into S.

- The operation $*$ is said to be **associative** if

$$a * (b * c) = (a * b) * c \qquad \text{for all } a, b, c \in S.$$

- An element $e \in S$ is called an **identity** element for $*$ if

$$a * e = a \quad \text{and} \quad e * a = a \qquad \text{for all } a \in S.$$

- If $*$ has an identity element e, and $a \in S$, then $b \in S$ is said to be an **inverse** for a if

$$a * b = e \quad \text{and} \quad b * a = e.$$

Binary operation

Definition 2

A **binary operation** $*$ on a set S is a function

$$* : S \times S \to S$$

from the set $S \times S$ of all ordered pairs of elements in S into S.

- The operation $*$ is said to be **associative** if
$$a * (b * c) = (a * b) * c \qquad \text{for all } a, b, c \in S.$$
- An element $e \in S$ is called an **identity** element for $*$ if
$$a * e = a \quad \text{and} \quad e * a = a \qquad \text{for all } a \in S.$$
- If $*$ has an identity element e, and $a \in S$, then $b \in S$ is said to be an **inverse** for a if
$$a * b = e \quad \text{and} \quad b * a = e.$$

A binary operation $*$ permits us to combine only two elements, and so a *priori* $a * b * c$ does not make sense. But $(a * b) * c$ does make sense.

Examples

(i) Multiplication defines a (associative) binary operation on $\mathbf{R}$.

- 1 serves as an identity element.
- Only nonzero element $a \in \mathbf{R}$ has the inverse $1/a$.

Examples

(i) Multiplication defines a (associative) binary operation on $\mathbf{R}$.

- 1 serves as an identity element.
- Only nonzero element $a \in \mathbf{R}$ has the inverse $1/a$.

(ii) Multiplication defines a binary operation on $S = \{x \in \mathbf{R} | x \geq 1\}$.

- 1 serves as an identity element.
- Only 1 has the inverse 1.

Examples

(i) Multiplication defines a (associative) binary operation on $\mathbf{R}$.
- 1 serves as an identity element.
- Only nonzero element $a \in \mathbf{R}$ has the inverse $1/a$.

(ii) Multiplication defines a binary operation on $S = \{x \in \mathbf{R} | x \geq 1\}$.
- 1 serves as an identity element.
- Only 1 has the inverse 1.

If $S = \{x \in \mathbf{R} | x > 1\}$, then S does not have an identity element.

Examples

(i) Multiplication defines a (associative) binary operation on $\mathbf{R}$.

- 1 serves as an identity element.
- Only nonzero element $a \in \mathbf{R}$ has the inverse $1/a$.

(ii) Multiplication defines a binary operation on $S = \{x \in \mathbf{R} | x \geq 1\}$.

- 1 serves as an identity element.
- Only 1 has the inverse 1.

If $S = \{x \in \mathbf{R} | x > 1\}$, then S does not have an identity element.

(iii) If $S = \{x \in \mathbf{R} | x < 0\}$, then multiplication does NOT even define a binary operation on S. (Why?)

Examples

(i) Multiplication defines a (associative) binary operation on $\mathbf{R}$.

- 1 serves as an identity element.
- Only nonzero element $a \in \mathbf{R}$ has the inverse $1/a$.

(ii) Multiplication defines a binary operation on $S = \{x \in \mathbf{R} | x \geq 1\}$.

- 1 serves as an identity element.
- Only 1 has the inverse 1.

If $S = \{x \in \mathbf{R} | x > 1\}$, then S does not have an identity element.

(iii) If $S = \{x \in \mathbf{R} | x < 0\}$, then multiplication does NOT even define a binary operation on S. (Why?)

(iv) Division is also NOT a binary operation on $\mathbf{R}$. (Why?)

More Examples

(i) Let $S = \{f | f : A \to A\}$. If $\phi, \theta \in S$, then define $\phi * \theta$ by letting

$$\phi * \theta(a) = \phi(\theta(a)) \qquad \text{for all } a \in A.$$

This defines a binary operation on S.

- composition of functions is **associative**.
- the identity function is an **identity** element.
- the functions that have **inverses** are precisely the ones that are both one-to-one and onto.

More Examples

(i) Let $S = \{f | f : A \to A\}$. If $\phi, \theta \in S$, then define $\phi * \theta$ by letting
$$\phi * \theta(a) = \phi(\theta(a)) \qquad \text{for all } a \in A.$$
This defines a binary operation on S.
- composition of functions is **associative**.
- the identity function is an **identity** element.
- the functions that have **inverses** are precisely the ones that are both one-to-one and onto.

(ii) Matrix multiplication defines a binary operation on $M_n(\mathbf{R})$.
- **associative**: ✓
- the identity matrix serves as an **identity** element.
- a matrix has a multiplicative **inverse** if and only if its determinant is nonzero.

More Examples

(i) Let $S = \{f | f : A \to A\}$. If $\phi, \theta \in S$, then define $\phi * \theta$ by letting

$$\phi * \theta(a) = \phi(\theta(a)) \qquad \text{for all } a \in A.$$

This defines a binary operation on S.

- composition of functions is **associative**.
- the identity function is an **identity** element.
- the functions that have **inverses** are precisely the ones that are both one-to-one and onto.

(ii) Matrix multiplication defines a binary operation on $M_n(\mathbf{R})$.

- **associative**: ✓
- the identity matrix serves as an **identity** element.
- a matrix has a multiplicative **inverse** if and only if its determinant is nonzero.

(iii) Matrix multiplication does NOT define a binary operation on the set of nonzero matrices in $M_n(\mathbf{R})$. (Why?)

More Examples

(i) Let $S = \{f | f : A \to A\}$. If $\phi, \theta \in S$, then define $\phi * \theta$ by letting
$$\phi * \theta(a) = \phi(\theta(a)) \qquad \text{for all } a \in A.$$
This defines a binary operation on S.
- composition of functions is **associative**.
- the identity function is an **identity** element.
- the functions that have **inverses** are precisely the ones that are both one-to-one and onto.

(ii) Matrix multiplication defines a binary operation on $M_n(\mathbf{R})$.
- **associative**: ✓
- the identity matrix serves as an **identity** element.
- a matrix has a multiplicative **inverse** if and only if its determinant is nonzero.

(iii) Matrix multiplication does NOT define a binary operation on the set of nonzero matrices in $M_n(\mathbf{R})$. (Why?)

(iv) Addition of matrices defines an binary operation on $M_n(\mathbf{R})$.
- **associative**: ✓
- the **identity** element is the zero matrix.
- Each matrix has an **inverse**, namely, its negative.

Well-definedness

Since the definition of a binary operation involves a function, we sometimes need to check that a binary operation is well-defined.

Well-definedness

Since the definition of a binary operation involves a function, we sometimes need to check that a binary operation is well-defined.

Example 3

Define multiplication on the set of rational numbers

$$\mathbf{Q} = \left\{ \frac{m}{n} \middle| m, n \in \mathbf{Z} \text{ and } n \neq 0 \right\}$$

where $m/n = p/q$ if $mq = np$. If $a, b \in \mathbf{Q}$ with $a = m/n$ and $b = s/t$, then we define $ab = ms/nt$. Check that the product does not depend on how we choose to represent a and b.

Well-definedness

Since the definition of a binary operation involves a function, we sometimes need to check that a binary operation is well-defined.

Example 3

Define multiplication on the set of rational numbers

$$\mathbf{Q} = \left\{ \frac{m}{n} \middle| m, n \in \mathbf{Z} \text{ and } n \neq 0 \right\}$$

where $m/n = p/q$ if $mq = np$. If $a, b \in \mathbf{Q}$ with $a = m/n$ and $b = s/t$, then we define $ab = ms/nt$. Check that the product does not depend on how we choose to represent a and b.

If we also have $a = p/q$ and $b = u/v$, then we must check $pu/qv = ms/nt$

Well-definedness

Since the definition of a binary operation involves a function, we sometimes need to check that a binary operation is well-defined.

Example 3

Define multiplication on the set of rational numbers

$$\mathbf{Q} = \left\{ \frac{m}{n} \middle| m, n \in \mathbf{Z} \text{ and } n \neq 0 \right\}$$

where $m/n = p/q$ if $mq = np$. If $a, b \in \mathbf{Q}$ with $a = m/n$ and $b = s/t$, then we define $ab = ms/nt$. Check that the product does not depend on how we choose to represent a and b.

If we also have $a = p/q$ and $b = u/v$, then we must check $pu/qv = ms/nt$

Since $m/n = a = p/q$ and $s/t = b = u/v \Rightarrow mq = np$ and $sv = tu$. Thus

$$(ms)(qv) = (nt)(pu).$$

Associative binary operation, I

Proposition 1

Let $*$ be an associative binary operation on a set S.

(a) *The operation $*$ has at most one identity element.*

(b) *If $*$ has an identity element, then any element of S has at most one inverse.*

Associative binary operation, I

Proposition 1

Let $*$ be an associative binary operation on a set S.

(a) *The operation $*$ has at most one identity element.*

(b) *If $*$ has an identity element, then any element of S has at most one inverse.*

(a) Suppose that e and e' are identity elements for $*$. To show: $e = e'$.

Associative binary operation, I

Proposition 1

Let $*$ be an associative binary operation on a set S.

(a) *The operation $*$ has at most one identity element.*

(b) *If $*$ has an identity element, then any element of S has at most one inverse.*

(a) Suppose that e and e' are identity elements for $*$. To show: $e = e'$.
Since e is an identity element, we have $e * e' = e'$, and

Associative binary operation, I

Proposition 1

Let $*$ be an associative binary operation on a set S.

(a) *The operation $*$ has at most one identity element.*

(b) *If $*$ has an identity element, then any element of S has at most one inverse.*

(a) Suppose that e and e' are identity elements for $*$. To show: $e = e'$.
Since e is an identity element, we have $e * e' = e'$, and
since e' is an identity element, we have $e * e' = e$. Thus, $e = e'$. $\square$

Associative binary operation, I

Proposition 1

Let $*$ be an associative binary operation on a set S.

(a) *The operation $*$ has at most one identity element.*

(b) *If $*$ has an identity element, then any element of S has at most one inverse.*

(a) Suppose that e and e' are identity elements for $*$. To show: $e = e'$.
Since e is an identity element, we have $e * e' = e'$, and
since e' is an identity element, we have $e * e' = e$. Thus, $e = e'$. $\square$

(b) Let e be the identity element for S. Let b and b' be inverses for the element a. Then $b * a = e$ and $a * b' = e$. To show: $b = b'$.

Associative binary operation, I

Proposition 1

Let $*$ be an associative binary operation on a set S.

(a) *The operation $*$ has at most one identity element.*

(b) *If $*$ has an identity element, then any element of S has at most one inverse.*

(a) Suppose that e and e' are identity elements for $*$. To show: $e = e'$.
Since e is an identity element, we have $e * e' = e'$, and
since e' is an identity element, we have $e * e' = e$. Thus, $e = e'$. $\square$

(b) Let e be the identity element for S. Let b and b' be inverses for the element a. Then $b * a = e$ and $a * b' = e$. To show: $b = b'$.

$$b' = e * b' = (b * a) * b' = b * (a * b') = b * e = b \quad \text{(associativity)} \quad \square$$

Associative binary operation, I

Proposition 1

Let $*$ be an associative binary operation on a set S.

(a) *The operation $*$ has at most one identity element.*

(b) *If $*$ has an identity element, then any element of S has at most one inverse.*

(a) Suppose that e and e' are identity elements for $*$. To show: $e = e'$.
Since e is an identity element, we have $e * e' = e'$, and
since e' is an identity element, we have $e * e' = e$. Thus, $e = e'$. $\square$

(b) Let e be the identity element for S. Let b and b' be inverses for the element a. Then $b * a = e$ and $a * b' = e$. To show: $b = b'$.

$$b' = e * b' = (b * a) * b' = b * (a * b') = b * e = b \quad \text{(associativity)} \quad \square$$

If $*$ is an associative binary operation on a set S, and $a \in S$ has an inverse, then we will use the notation a^{-1} to denote the **inverse** of a.

Associative binary operation, II

Proposition 2

Let $*$ be an associative binary operation on a set S. If $*$ has an identity element e and $a, b \in S$ have inverses a^{-1} and b^{-1}, respectively, then

(i) *the inverse of a^{-1} exists and is equal to a, and*

(ii) *the inverse of $a * b$ exists and is equal to $b^{-1} * a^{-1}$.*

Associative binary operation, II

Proposition 2

Let $*$ be an associative binary operation on a set S. If $*$ has an identity element e and $a, b \in S$ have inverses a^{-1} and b^{-1}, respectively, then

(i) *the inverse of a^{-1} exists and is equal to a, and*

(ii) *the inverse of $a * b$ exists and is equal to $b^{-1} * a^{-1}$.*

(i) Since a^{-1} is the inverse of a, then $a * a^{-1} = e$ and $a^{-1} * a = e$.

Associative binary operation, II

Proposition 2

Let $*$ be an associative binary operation on a set S. If $*$ has an identity element e and $a, b \in S$ have inverses a^{-1} and b^{-1}, respectively, then

(i) *the inverse of a^{-1} exists and is equal to a, and*

(ii) *the inverse of $a * b$ exists and is equal to $b^{-1} * a^{-1}$.*

(i) Since a^{-1} is the inverse of a, then $a * a^{-1} = e$ and $a^{-1} * a = e$. It also show that a is the inverse of a^{-1}. $\square$

Associative binary operation, II

Proposition 2

Let $*$ be an associative binary operation on a set S. If $*$ has an identity element e and $a, b \in S$ have inverses a^{-1} and b^{-1}, respectively, then

(i) *the inverse of a^{-1} exists and is equal to a, and*

(ii) *the inverse of $a * b$ exists and is equal to $b^{-1} * a^{-1}$.*

(i) Since a^{-1} is the inverse of a, then $a * a^{-1} = e$ and $a^{-1} * a = e$. It also show that a is the inverse of a^{-1}. □

(ii) Since $*$ is associative, we have

$$\begin{aligned}(a * b) * (b^{-1} * a^{-1}) =& ((a * b) * b^{-1}) * a^{-1} \\ =& (a * (b * b^{-1})) * a^{-1} \\ =& (a * e) * a^{-1} = a * a^{-1} = e.\end{aligned}$$

Similarly,

Associative binary operation, II

Proposition 2

Let $*$ be an associative binary operation on a set S. If $*$ has an identity element e and $a, b \in S$ have inverses a^{-1} and b^{-1}, respectively, then

(i) *the inverse of a^{-1} exists and is equal to a, and*

(ii) *the inverse of $a * b$ exists and is equal to $b^{-1} * a^{-1}$.*

(i) Since a^{-1} is the inverse of a, then $a * a^{-1} = e$ and $a^{-1} * a = e$. It also show that a is the inverse of a^{-1}. □

(ii) Since $*$ is associative, we have

$$\begin{aligned}(a * b) * (b^{-1} * a^{-1}) =& ((a * b) * b^{-1}) * a^{-1} \\ =& (a * (b * b^{-1})) * a^{-1} \\ =& (a * e) * a^{-1} = a * a^{-1} = e.\end{aligned}$$

Similarly, we also have $(b^{-1} * a^{-1}) * (a * b) = e$. (Check it!) □

Alternative notations for $*$

The general binary operations will normally be denoted multiplicatively; i.e., instead of writing $a * b$ we will just write $a \cdot b$, or simply ab.

Alternative notations for $*$

The general binary operations will normally be denoted multiplicatively; i.e., instead of writing $a * b$ we will just write $a \cdot b$, or simply ab.

Example 4

The previous proposition shows $(ab)^{-1} = b^{-1}a^{-1}$, if a and b have inverses.

Alternative notations for $*$

The general binary operations will normally be denoted multiplicatively; i.e., instead of writing $a * b$ we will just write $a \cdot b$, or simply ab.

Example 4

The previous proposition shows $(ab)^{-1} = b^{-1}a^{-1}$, if a and b have inverses.

Another case, when a binary operation $*$ satisfies the **commutative law**

$$a * b = b * a,$$

it is quite common to use additive notation for the operation.

Group

Definition 5

Let $(G, *)$ denote a nonempty set G together with a binary operation $*$ on G. That is, the following condition must be satisfied.

(i) **Closure**: For all $a, b \in G$, $a * b$ is a well-defined element of G.

Then G is called a **group** if the following properties hold.

(ii) **Associativity**: For all $a, b, c \in G$, we have
$$a * (b * c) = (a * b) * c.$$

(iii) **Identity**: There exists an **identity** element $e \in G$, i.e.,
$$a * e = a \quad \text{and} \quad e * a = a \qquad \text{for all } a \in G.$$

(iv) **Inverses**: For each $a \in G$ there exists an inverse element $a^{-1} \in G$:
$$a * a^{-1} = e \quad \text{and} \quad a^{-1} * a = e.$$

Group

Definition 5

Let $(G, *)$ denote a nonempty set G together with a binary operation $*$ on G. That is, the following condition must be satisfied.

(i) **Closure**: For all $a, b \in G$, $a * b$ is a well-defined element of G.

Then G is called a **group** if the following properties hold.

(ii) **Associativity**: For all $a, b, c \in G$, we have

$$a * (b * c) = (a * b) * c.$$

(iii) **Identity**: There exists an **identity** element $e \in G$, i.e.,

$$a * e = a \quad \text{and} \quad e * a = a \qquad \text{for all } a \in G.$$

(iv) **Inverses**: For each $a \in G$ there exists an inverse element $a^{-1} \in G$:

$$a * a^{-1} = e \quad \text{and} \quad a^{-1} * a = e.$$

- Proposition 1 implies that the identity element e is unique.

Definition 5

Let $(G, *)$ denote a nonempty set G together with a binary operation $*$ on G. That is, the following condition must be satisfied.

(i) **Closure**: For all $a, b \in G$, $a * b$ is a well-defined element of G.

Then G is called a **group** if the following properties hold.

(ii) **Associativity**: For all $a, b, c \in G$, we have

$$a * (b * c) = (a * b) * c.$$

(iii) **Identity**: There exists an **identity** element $e \in G$, i.e.,

$$a * e = a \quad \text{and} \quad e * a = a \qquad \text{for all } a \in G.$$

(iv) **Inverses**: For each $a \in G$ there exists an inverse element $a^{-1} \in G$:

$$a * a^{-1} = e \quad \text{and} \quad a^{-1} * a = e.$$

- Proposition 1 implies that the identity element e is unique.
- Proposition 2 implies that $(a^{-1})^{-1} = a$.

Group

Definition 5

Let $(G, *)$ denote a nonempty set G together with a binary operation $*$ on G. That is, the following condition must be satisfied.

(i) **Closure**: For all $a, b \in G$, $a * b$ is a well-defined element of G.

Then G is called a **group** if the following properties hold.

(ii) **Associativity**: For all $a, b, c \in G$, we have

$$a * (b * c) = (a * b) * c.$$

(iii) **Identity**: There exists an **identity** element $e \in G$, i.e.,

$$a * e = a \quad \text{and} \quad e * a = a \qquad \text{for all } a \in G.$$

(iv) **Inverses**: For each $a \in G$ there exists an inverse element $a^{-1} \in G$:

$$a * a^{-1} = e \quad \text{and} \quad a^{-1} * a = e.$$

- Proposition 1 implies that the identity element e is unique.
- Proposition 2 implies that $(a^{-1})^{-1} = a$. Thus, $a = b \Leftrightarrow a^{-1} = b^{-1}$.

A "Compact" version of the definition of a group

Definition 6 (Restatement of Definition 5)

A group is a nonempty set G with an **associative** binary operation, such that G contains an **identity** element for the operation, and each element of G has an **inverse** in G.

A "Compact" version of the definition of a group

Definition 6 (Restatement of Definition 5)

A group is a nonempty set G with an **associative** binary operation, such that G contains an **identity** element for the operation, and each element of G has an **inverse** in G.

If G is a group and $a \in G$, then for any positive integer n we define a^n to be the product of a with itself n times. (How?) [

A “Compact” version of the definition of a group

Definition 6 (Restatement of Definition 5)

A group is a nonempty set G with an **associative** binary operation, such that G contains an **identity** element for the operation, and each element of G has an **inverse** in G.

If G is a group and $a \in G$, then for any positive integer n we define a^n to be the product of a with itself n times. (How?) [$a^n = a * a^{n-1}$ inductively]

A "Compact" version of the definition of a group

Definition 6 (Restatement of Definition 5)

A group is a nonempty set G with an **associative** binary operation, such that G contains an **identity** element for the operation, and each element of G has an **inverse** in G.

If G is a group and $a \in G$, then for any positive integer n we define a^n to be the product of a with itself n times. (How?) [$a^n = a * a^{n-1}$ inductively] Then the exponential laws must hold for all positive exponents m, n. I.e.,

$$a^m * a^n = a^{m+n} \quad \text{and} \quad (a^m)^n = a^{mn}.$$

A "Compact" version of the definition of a group

Definition 6 (Restatement of Definition 5)

A group is a nonempty set G with an **associative** binary operation, such that G contains an **identity** element for the operation, and each element of G has an **inverse** in G.

If G is a group and $a \in G$, then for any positive integer n we define a^n to be the product of a with itself n times. (How?) [$a^n = a * a^{n-1}$ inductively] Then the exponential laws must hold for all positive exponents m, n. I.e.,

$$a^m * a^n = a^{m+n} \quad \text{and} \quad (a^m)^n = a^{mn}.$$

To extend these laws from positive exponents to all integral exponents,

A "Compact" version of the definition of a group

Definition 6 (Restatement of Definition 5)

A group is a nonempty set G with an **associative** binary operation, such that G contains an **identity** element for the operation, and each element of G has an **inverse** in G.

If G is a group and $a \in G$, then for any positive integer n we define a^n to be the product of a with itself n times. (How?) [$a^n = a * a^{n-1}$ inductively] Then the exponential laws must hold for all positive exponents m, n. I.e.,

$$a^m * a^n = a^{m+n} \quad \text{and} \quad (a^m)^n = a^{mn}.$$

To extend these laws from positive exponents to all integral exponents, we define

$$a^0 = e \quad \text{and} \quad a^{-n} = (a^n)^{-1}.$$

Examples

(1) $\mathbf{R}$ is NOT a group under the standard multiplication $\cdot$.
The first three axioms are satisfied, but the fourth axiom fails. (Why?)

Examples

(1) $\mathbf{R}$ is NOT a group under the standard multiplication $\cdot$.
The first three axioms are satisfied, but the fourth axiom fails. (Why?)

(2) $\mathbf{R}^{\times}$ is a group under the standard multiplication $\cdot$. (Check it!)

- (i) **Closure:** If $a, b \in \mathbf{R}^{\times}$, then $a \cdot b \in \mathbf{R}^{\times}$.
- (ii) **Associativity:** Multiplication of real numbers is associative.
- (iii) **Identity:** 1
- (iv) **Inverses:** $1/a$ gives the inverse of an element $a \in \mathbf{R}^{\times}$.

Examples

(1) $\mathbf{R}$ is NOT a group under the standard multiplication $\cdot$.
The first three axioms are satisfied, but the fourth axiom fails. (Why?)

(2) $\mathbf{R}^\times$ is a group under the standard multiplication $\cdot$. (Check it!)
   (i) **Closure:** If $a, b \in \mathbf{R}^\times$, then $a \cdot b \in \mathbf{R}^\times$.
   (ii) **Associativity:** Multiplication of real numbers is associative.
   (iii) **Identity:** 1
   (iv) **Inverses:** $1/a$ gives the inverse of an element $a \in \mathbf{R}^\times$.

Similarly, $\mathbf{Q}^\times$ and $\mathbf{C}^\times$ are groups under the ordinary multiplication.

Examples

(1) $\mathbf{R}$ is NOT a group under the standard multiplication $\cdot$.
The first three axioms are satisfied, but the fourth axiom fails. (Why?)

(2) $\mathbf{R}^{\times}$ is a group under the standard multiplication $\cdot$. (Check it!)

(i) **Closure:** If $a, b \in \mathbf{R}^{\times}$, then $a \cdot b \in \mathbf{R}^{\times}$.
(ii) **Associativity:** Multiplication of real numbers is associative.
(iii) **Identity:** 1
(iv) **Inverses:** $1/a$ gives the inverse of an element $a \in \mathbf{R}^{\times}$.

Similarly, $\mathbf{Q}^{\times}$ and $\mathbf{C}^{\times}$ are groups under the ordinary multiplication.

To form a multiplicative group from the integers $\mathbf{Z}$, we have to restrict ourselves to just ± 1. (Why?)

Symmetric group

Definition 7

The set of all permutations of a set S is denoted by $\mathrm{Sym}(S)$.
The set of all permutations of the set $\{1, 2, \ldots, n\}$ is denoted by S_n.
The group $\mathrm{Sym}(S)$ is called the **symmetric group** on S, and
The group S_n is called the **symmetric group of degree** n.

Symmetric group

Definition 7

The set of all permutations of a set S is denoted by $\mathrm{Sym}(S)$.
The set of all permutations of the set $\{1, 2, \ldots, n\}$ is denoted by S_n.
The group $\mathrm{Sym}(S)$ is called the **symmetric group** on S, and
The group S_n is called the **symmetric group of degree** n.

Proposition 3

If S is any nonempty set, then $\mathrm{Sym}(S)$ is a group under the operation of composition of functions.

Symmetric group

Definition 7

The set of all permutations of a set S is denoted by $\mathrm{Sym}(S)$.
The set of all permutations of the set $\{1, 2, \ldots, n\}$ is denoted by S_n.
The group $\mathrm{Sym}(S)$ is called the **symmetric group** on S, and
The group S_n is called the **symmetric group of degree** n.

Proposition 3

If S is any nonempty set, then $\mathrm{Sym}(S)$ is a group under the operation of composition of functions.

Let $f, g \in \mathrm{Sym}(S)$ be any two one-to-one and onto functions.

Symmetric group

Definition 7

The set of all permutations of a set S is denoted by $\mathrm{Sym}(S)$.
The set of all permutations of the set $\{1, 2, \ldots, n\}$ is denoted by S_n.
The group $\mathrm{Sym}(S)$ is called the **symmetric group** on S, and
The group S_n is called the **symmetric group of degree** n.

Proposition 3

If S is any nonempty set, then $\mathrm{Sym}(S)$ is a group under the operation of composition of functions.

Let $f, g \in \mathrm{Sym}(S)$ be any two one-to-one and onto functions.

(i) **Closure:** $f \circ g \in \mathrm{Sym}(S)$

(ii) **Associativity:** $\circ$ is associative.

(iii) **Identity:** the identity function 1_S

(iv) **Inverses:** a function f is 1-1 and onto $\Leftrightarrow$ it has an inverse function f^{-1}, and f^{-1} is again 1-1 and onto. I.e., $f^{-1} \in \mathrm{Sym}(S)$. $\square$

Example: Multiplication table for S_3

	(1)	(123)	(132)	(12)	(13)	(23)
(1)	(1)	(123)	(132)	(12)	(13)	(23)
(123)	(123)	(132)	(1)	(13)	(23)	(12)
(132)	(132)	(1)	(123)	(23)	(12)	(13)
(12)	(12)	(23)	(13)	(1)	(132)	(123)
(13)	(13)	(12)	(23)	(123)	(1)	(132)
(23)	(23)	(13)	(12)	(132)	(123)	(1)

Example: Multiplication table for S_3

	(1)	(123)	(132)	(12)	(13)	(23)
(1)	(1)	(123)	(132)	(12)	(13)	(23)
(123)	(123)	(132)	(1)	(13)	(23)	(12)
(132)	(132)	(1)	(123)	(23)	(12)	(13)
(12)	(12)	(23)	(13)	(1)	(132)	(123)
(13)	(13)	(12)	(23)	(123)	(1)	(132)
(23)	(23)	(13)	(12)	(132)	(123)	(1)

- In each row, each element of the group occurs exactly once.

Example: Multiplication table for S_3

	(1)	(123)	(132)	(12)	(13)	(23)
(1)	(1)	(123)	(132)	(12)	(13)	(23)
(123)	(123)	(132)	(1)	(13)	(23)	(12)
(132)	(132)	(1)	(123)	(23)	(12)	(13)
(12)	(12)	(23)	(13)	(1)	(132)	(123)
(13)	(13)	(12)	(23)	(123)	(1)	(132)
(23)	(23)	(13)	(12)	(132)	(123)	(1)

- In each row, each element of the group occurs exactly once.
- In each column, each element of the group occurs exactly once.

Example: Multiplication table for S_3

	(1)	(123)	(132)	(12)	(13)	(23)
(1)	(1)	(123)	(132)	(12)	(13)	(23)
(123)	(123)	(132)	(1)	(13)	(23)	(12)
(132)	(132)	(1)	(123)	(23)	(12)	(13)
(12)	(12)	(23)	(13)	(1)	(132)	(123)
(13)	(13)	(12)	(23)	(123)	(1)	(132)
(23)	(23)	(13)	(12)	(132)	(123)	(1)

- In each row, each element of the group occurs exactly once.
- In each column, each element of the group occurs exactly once.

This phenomenon occurs in any such group table. (Why?) [

Example: Multiplication table for S_3

	(1)	(123)	(132)	(12)	(13)	(23)
(1)	(1)	(123)	(132)	(12)	(13)	(23)
(123)	(123)	(132)	(1)	(13)	(23)	(12)
(132)	(132)	(1)	(123)	(23)	(12)	(13)
(12)	(12)	(23)	(13)	(1)	(132)	(123)
(13)	(13)	(12)	(23)	(123)	(1)	(132)
(23)	(23)	(13)	(12)	(132)	(123)	(1)

- In each row, each element of the group occurs exactly once.
- In each column, each element of the group occurs exactly once.

This phenomenon occurs in any such group table. (Why?) [cancellation law]

Cancellation law

Proposition 4 (Cancellation Property for Groups)

Let G be a group, and let $a, b, c \in G$.

(a) *If $ab = ac$, then $b = c$.*

(b) *If $ac = bc$, then $a = b$.*

Note that we drop the notation $a * b$, and simply write ab instead.

Cancellation law

Proposition 4 (Cancellation Property for Groups)

Let G be a group, and let $a, b, c \in G$.

(a) *If $ab = ac$, then $b = c$.*

(b) *If $ac = bc$, then $a = b$.*

Note that we drop the notation $a * b$, and simply write ab instead.

(a)

$$\begin{aligned} ab &= ac \\ a^{-1}(ab) &= a^{-1}(ac) \\ (a^{-1}a)b &= (a^{-1}a)c \\ eb &= ec \\ b &= c \end{aligned}$$

Cancellation law

Proposition 4 (Cancellation Property for Groups)

Let G be a group, and let $a, b, c \in G$.

(a) *If $ab = ac$, then $b = c$.*

(b) *If $ac = bc$, then $a = b$.*

Note that we drop the notation $a * b$, and simply write ab instead.

(a)

$$\begin{aligned} ab =& ac \\ a^{-1}(ab) =& a^{-1}(ac) \\ (a^{-1}a)b =& (a^{-1}a)c \\ eb =& ec \\ b =& c \end{aligned}$$

(b) The proof is similar. (Check it!)

Some motivation for the study of groups

Proposition 5

(a) *If G is a group and $a, b \in G$, then each of the equations*

$$ax = b \quad \text{and} \quad xa = b \qquad \textit{has a unique solution.}$$

(b) *Conversely, if G is a nonempty set with an associative binary operation in which the equations*

$$ax = b \quad \text{and} \quad xa = b \qquad \textit{have solutions for all } a, b \in G,$$

then G is a group.

Some motivation for the study of groups

Proposition 5

(a) *If G is a group and $a, b \in G$, then each of the equations*

$$ax = b \quad \text{and} \quad xa = b \qquad \textit{has a unique solution.}$$

(b) *Conversely, if G is a nonempty set with an associative binary operation in which the equations*

$$ax = b \quad \text{and} \quad xa = b \qquad \textit{have solutions for all } a, b \in G,$$

then G is a group.

(a) Existence:

Some motivation for the study of groups

Proposition 5

(a) *If G is a group and $a, b \in G$, then each of the equations*

$$ax = b \quad \text{and} \quad xa = b \qquad \textit{has a unique solution.}$$

(b) *Conversely, if G is a nonempty set with an associative binary operation in which the equations*

$$ax = b \quad \text{and} \quad xa = b \qquad \textit{have solutions for all } a, b \in G,$$

then G is a group.

(a) Existence: $x = a^{-1}b$ plugs in $ax = b$. ✓(Check it!)
Uniqueness:

Some motivation for the study of groups

Proposition 5

(a) *If G is a group and $a, b \in G$, then each of the equations*

$$ax = b \quad \text{and} \quad xa = b \qquad \textit{has a unique solution.}$$

(b) *Conversely, if G is a nonempty set with an associative binary operation in which the equations*

$$ax = b \quad \text{and} \quad xa = b \qquad \textit{have solutions for all } a, b \in G,$$

then G is a group.

(a) Existence: $x = a^{-1}b$ plugs in $ax = b$. ✓(Check it!)
Uniqueness: If s, t are solutions of $ax = b$, then $as = b = at \Rightarrow s = t$.

Some motivation for the study of groups

Proposition 5

(a) *If G is a group and $a, b \in G$, then each of the equations*

$$ax = b \quad \text{and} \quad xa = b \qquad \textit{has a unique solution.}$$

(b) *Conversely, if G is a nonempty set with an associative binary operation in which the equations*

$$ax = b \quad \text{and} \quad xa = b \qquad \textit{have solutions for all } a, b \in G,$$

then G is a group.

(a) Existence: $x = a^{-1}b$ plugs in $ax = b$. ✓(Check it!)
Uniqueness: If s, t are solutions of $ax = b$, then $as = b = at \Rightarrow s = t$.
The proof for the second equation is similar. (Check it!) [

Some motivation for the study of groups

Proposition 5

(a) *If G is a group and $a, b \in G$, then each of the equations*

$$ax = b \quad \text{and} \quad xa = b \qquad \textit{has a unique solution.}$$

(b) *Conversely, if G is a nonempty set with an associative binary operation in which the equations*

$$ax = b \quad \text{and} \quad xa = b \qquad \textit{have solutions for all } a, b \in G,$$

then G is a group.

(a) Existence: $x = a^{-1}b$ plugs in $ax = b$. ✓(Check it!)
Uniqueness: If s, t are solutions of $ax = b$, then $as = b = at \Rightarrow s = t$.
The proof for the second equation is similar. (Check it!) [$x = ba^{-1}$]

Some motivation for the study of groups

Proposition 5

(a) *If G is a group and $a, b \in G$, then each of the equations*

$$ax = b \quad \text{and} \quad xa = b \qquad \text{has a unique solution.}$$

(b) *Conversely, if G is a nonempty set with an associative binary operation in which the equations*

$$ax = b \quad \text{and} \quad xa = b \qquad \text{have solutions for all } a, b \in G,$$

then G is a group.

(a) Existence: $x = a^{-1}b$ plugs in $ax = b$. ✓(Check it!)
Uniqueness: If s, t are solutions of $ax = b$, then $as = b = at \Rightarrow s = t$.
The proof for the second equation is similar. (Check it!) [$x = ba^{-1}$]

(b) We still need to show that the following two axioms are satisfied.
   (i) **Identity:**
   (ii) **Inverses:**

Continued on next page . . .

Proof of Proposition 5 (b)

If G is a nonempty set with an associative binary operation in which $ax = b$ and $xa = b$ have solutions for all $a, b \in G$, then G is a group.

(i) **Identity:** Let e be a solution of $ax = a$. To show $be = b, \forall b \in G$.

Proof of Proposition 5 (b)

If G is a nonempty set with an associative binary operation in which $ax = b$ and $xa = b$ have solutions for all $a, b \in G$, then G is a group.

(i) **Identity:** Let e be a solution of $ax = a$. To show $be = b, \forall b \in G$.
Let $b \in G$ be given. Let c be a solution to $xa = b$, so $ca = b$.

Proof of Proposition 5 (b)

If G is a nonempty set with an associative binary operation in which $ax = b$ and $xa = b$ have solutions for all $a, b \in G$, then G is a group.

(i) **Identity:** Let e be a solution of $ax = a$. To show $be = b, \forall b \in G$. Let $b \in G$ be given. Let c be a solution to $xa = b$, so $ca = b$. Then

$$be = (ca)e = c(ae) = ca = b.$$

Proof of Proposition 5 (b)

If G is a nonempty set with an associative binary operation in which $ax = b$ and $xa = b$ have solutions for all $a, b \in G$, then G is a group.

(i) **Identity:** Let e be a solution of $ax = a$. To show $be = b, \forall b \in G$.
Let $b \in G$ be given. Let c be a solution to $xa = b$, so $ca = b$. Then
$$be = (ca)e = c(ae) = ca = b.$$
Similarly, there exists $e' \in G$ such that $e'b = b, \forall b \in G$. (Check it!)
To show $e = e'$:

Proof of Proposition 5 (b)

If G is a nonempty set with an associative binary operation in which $ax = b$ and $xa = b$ have solutions for all $a, b \in G$, then G is a group.

(i) **Identity:** Let e be a solution of $ax = a$. To show $be = b, \forall b \in G$. Let $b \in G$ be given. Let c be a solution to $xa = b$, so $ca = b$. Then

$$be = (ca)e = c(ae) = ca = b.$$

Similarly, there exists $e' \in G$ such that $e'b = b, \forall b \in G$. (Check it!) To show $e = e'$: $e'e = e'$ and $e'e = e$. (Why?) $\square$

(ii) **Inverses:** Given any element $b \in G$, we must find an inverse for b.

Proof of Proposition 5 (b)

If G is a nonempty set with an associative binary operation in which $ax = b$ and $xa = b$ have solutions for all $a, b \in G$, then G is a group.

(i) **Identity:** Let e be a solution of $ax = a$. To show $be = b, \forall b \in G$.
Let $b \in G$ be given. Let c be a solution to $xa = b$, so $ca = b$. Then

$$be = (ca)e = c(ae) = ca = b.$$

Similarly, there exists $e' \in G$ such that $e'b = b, \forall b \in G$. (Check it!)
To show $e = e'$: $e'e = e'$ and $e'e = e$. (Why?) $\square$

(ii) **Inverses:** Given any element $b \in G$, we must find an inverse for b.
Let c be a solution to $bx = e$ and let d be a solution to $xb = e$.

Proof of Proposition 5 (b)

If G is a nonempty set with an associative binary operation in which $ax = b$ and $xa = b$ have solutions for all $a, b \in G$, then G is a group.

(i) **Identity:** Let e be a solution of $ax = a$. To show $be = b, \forall b \in G$.
Let $b \in G$ be given. Let c be a solution to $xa = b$, so $ca = b$. Then

$$be = (ca)e = c(ae) = ca = b.$$

Similarly, there exists $e' \in G$ such that $e'b = b, \forall b \in G$. (Check it!)
To show $e = e'$: $e'e = e'$ and $e'e = e$. (Why?) $\square$

(ii) **Inverses:** Given any element $b \in G$, we must find an inverse for b.
Let c be a solution to $bx = e$ and let d be a solution to $xb = e$. Then

$$d = de = d(bc) = (db)c = ec = c.$$

Proof of Proposition 5 (b)

If G is a nonempty set with an associative binary operation in which $ax = b$ and $xa = b$ have solutions for all $a, b \in G$, then G is a group.

(i) **Identity:** Let e be a solution of $ax = a$. To show $be = b, \forall b \in G$. Let $b \in G$ be given. Let c be a solution to $xa = b$, so $ca = b$. Then

$$be = (ca)e = c(ae) = ca = b.$$

Similarly, there exists $e' \in G$ such that $e'b = b, \forall b \in G$. (Check it!) To show $e = e'$: $e'e = e'$ and $e'e = e$. (Why?) $\square$

(ii) **Inverses:** Given any element $b \in G$, we must find an inverse for b. Let c be a solution to $bx = e$ and let d be a solution to $xb = e$. Then

$$d = de = d(bc) = (db)c = ec = c.$$

Thus $bc = e$ and $cb = e$, and so c is an inverse for b. $\square$

Example

- Remember that the elements in groups may not commute.

Example

- Remember that the elements in groups may not commute.
- The associative law for the operation in a group effectively says that we do not need to worry about parentheses, but sometimes they are helpful in emphasizing the crucial parts of an argument.

Example

- Remember that the elements in groups may not commute.
- The associative law for the operation in a group effectively says that we do not need to worry about parentheses, but sometimes they are helpful in emphasizing the crucial parts of an argument.

Example 8

Let G be a group and $a, b \in G$.Then $(ab)^2 = a^2b^2$ if and only if $ba = ab$.

Example

- Remember that the elements in groups may not commute.
- The associative law for the operation in a group effectively says that we do not need to worry about parentheses, but sometimes they are helpful in emphasizing the crucial parts of an argument.

Example 8

Let G be a group and $a, b \in G$.Then $(ab)^2 = a^2b^2$ if and only if $ba = ab$.

Proof.

Example

- Remember that the elements in groups may not commute.
- The associative law for the operation in a group effectively says that we do not need to worry about parentheses, but sometimes they are helpful in emphasizing the crucial parts of an argument.

Example 8

Let G be a group and $a, b \in G$. Then $(ab)^2 = a^2b^2$ if and only if $ba = ab$.

Proof.

$(\Leftarrow)$ $(ab)^2 = (ab)(ab) = a(b(ab)) = a((ba)b)$

Example

- Remember that the elements in groups may not commute.
- The associative law for the operation in a group effectively says that we do not need to worry about parentheses, but sometimes they are helpful in emphasizing the crucial parts of an argument.

Example 8

Let G be a group and $a, b \in G$. Then $(ab)^2 = a^2b^2$ if and only if $ba = ab$.

Proof.

$(\Leftarrow)$ $(ab)^2 = (ab)(ab) = a(b(ab)) = a((ba)b) \stackrel{!}{=} a((ab)b) = a(a(bb)) = (aa)(bb)$

Example

- Remember that the elements in groups may not commute.
- The associative law for the operation in a group effectively says that we do not need to worry about parentheses, but sometimes they are helpful in emphasizing the crucial parts of an argument.

Example 8

Let G be a group and $a, b \in G$.Then $(ab)^2 = a^2b^2$ if and only if $ba = ab$.

Proof.

$(\Leftarrow)$ $(ab)^2 = (ab)(ab) = a(b(ab)) = a((ba)b) \overset{!}{=} a((ab)b) = a(a(bb)) = (aa)(bb)$

$(\Rightarrow)$ Since $(ab)^2 = (ab)(ab)$ and $a^2b^2 = (aa)(bb)$,

Example

- Remember that the elements in groups may not commute.
- The associative law for the operation in a group effectively says that we do not need to worry about parentheses, but sometimes they are helpful in emphasizing the crucial parts of an argument.

Example 8

Let G be a group and $a, b \in G$.Then $(ab)^2 = a^2 b^2$ if and only if $ba = ab$.

Proof.

$(\Leftarrow)$ $(ab)^2 = (ab)(ab) = a(b(ab)) = a((ba)b) \overset{!}{=} a((ab)b) = a(a(bb)) = (aa)(bb)$

$(\Rightarrow)$ Since $(ab)^2 = (ab)(ab)$ and $a^2 b^2 = (aa)(bb)$, then

$$\begin{aligned} (ab)(ab) &= (aa)(bb) \\ a(b(ab)) &= a(a(bb)) \\ bab &= abb && \text{[We exclude the parentheses]} \\ ba &= ab && \text{(Why?)} \end{aligned}$$

$\square$

Abelian group

Definition 9

A group G is said to be **abelian** if $ab = ba$ for all $a, b \in G$.

Abelian group

Definition 9

A group G is said to be **abelian** if $ab = ba$ for all $a, b \in G$.

In an abelian group G, the operation is very often denoted additively.

Abelian group

Definition 9

A group G is said to be **abelian** if $ab = ba$ for all $a, b \in G$.

In an abelian group G, the operation is very often denoted additively.

(i) **Associativity:** $a + (b + c) = (a + b) + c$ for all $a, b, c \in G$.

(ii) **Identity:** The identity element is 0 and is called a **zero** element.

$$0 + a = a + 0 = a$$

(iii) **Inverses:** The additive inverse of a is denoted by $-a$, and satisfies

$$a + (-a) = (-a) + a = 0.$$

Abelian group

Definition 9

A group G is said to be **abelian** if $ab = ba$ for all $a, b \in G$.

In an abelian group G, the operation is very often denoted additively.

(i) **Associativity:** $a + (b + c) = (a + b) + c$ for all $a, b, c \in G$.

(ii) **Identity:** The identity element is 0 and is called a **zero** element.

$$0 + a = a + 0 = a$$

(iii) **Inverses:** The additive inverse of a is denoted by $-a$, and satisfies

$$a + (-a) = (-a) + a = 0.$$

Example 10

$\mathbf{Z}$ is an abelian group under the ordinary addition.

Abelian group

Definition 9

A group G is said to be **abelian** if $ab = ba$ for all $a, b \in G$.

In an abelian group G, the operation is very often denoted additively.

(i) **Associativity:** $a + (b + c) = (a + b) + c$ for all $a, b, c \in G$.

(ii) **Identity:** The identity element is 0 and is called a **zero** element.

$$0 + a = a + 0 = a$$

(iii) **Inverses:** The additive inverse of a is denoted by $-a$, and satisfies

$$a + (-a) = (-a) + a = 0.$$

Example 10

$\mathbf{Z}$ is an abelian group under the ordinary addition.
Similarly, $\mathbf{Q}, \mathbf{R}, \mathbf{C}$ are abelian groups under the ordinary addition.

Revisit Propositions 4 and 5 in additive notation

(Cancellation law) Let G be an abelian group, and let $a, b, c \in G$.

(a) $a + b = a + c \Longrightarrow b = c$

(b) $a + c = b + c \Longrightarrow a = b$ (No any additional information about G.)

Revisit Propositions 4 and 5 in additive notation

(Cancellation law) Let G be an abelian group, and let $a, b, c \in G$.

(a) $a + b = a + c \Longrightarrow b = c$

(b) $a + c = b + c \Longrightarrow a = b$ (No any additional information about G.)

Proposition 5 just becomes $a + x = x + a = b$ has a unique solution.

Revisit Propositions 4 and 5 in additive notation

(Cancellation law) Let G be an abelian group, and let $a, b, c \in G$.

(a) $a + b = a + c \Longrightarrow b = c$

(b) $a + c = b + c \Longrightarrow a = b$ (No any additional information about G.)

Proposition 5 just becomes $a + x = x + a = b$ has a unique solution.

Let G be an abelian group, and let $a \in G$. For a positive integer n,

$$na := \underbrace{a + \cdots + a}_{n \text{ times}}.$$

In additive notation, this replaces the exponential notation a^n.

Revisit Propositions 4 and 5 in additive notation

(Cancellation law) Let G be an abelian group, and let $a, b, c \in G$.

(a) $a + b = a + c \Longrightarrow b = c$

(b) $a + c = b + c \Longrightarrow a = b$ (No any additional information about G.)

Proposition 5 just becomes $a + x = x + a = b$ has a unique solution.

Let G be an abelian group, and let $a \in G$. For a positive integer n,

$$na := \underbrace{a + \cdots + a}_{n \text{ times}}.$$

In additive notation, this replaces the exponential notation a^n.
Note that this is not a multiplication in G, since n is not an element of G.

Revisit Propositions 4 and 5 in additive notation

(Cancellation law) Let G be an abelian group, and let $a, b, c \in G$.

(a) $a + b = a + c \Longrightarrow b = c$

(b) $a + c = b + c \Longrightarrow a = b$ (No any additional information about G.)

Proposition 5 just becomes $a + x = x + a = b$ has a unique solution.

Let G be an abelian group, and let $a \in G$. For a positive integer n,

$$na := \underbrace{a + \cdots + a}_{n \text{ times}}.$$

In additive notation, this replaces the exponential notation a^n.
Note that this is not a multiplication in G, since n is not an element of G.
Similarly, we define

$$0a = 0 \quad \text{and } (-n)a = -(na)$$

to make the (extended) standard laws of exponents expressed as

$$ma + na = (m + n)a \quad \text{and} \quad m(na) = (mn)a \text{ for all } a \in G \text{ and all } m, n \in \mathbf{Z}.$$

Finite group vs. Infinite group

Definition 11

A group G is said to be a **finite group** if the set G has a finite number of elements.

Finite group vs. Infinite group

Definition 11

A group G is said to be a **finite group** if the set G has a finite number of elements. In this case, the number of elements is called the **order** of G, denoted by $|G|$.

Finite group vs. Infinite group

Definition 11

A group G is said to be a **finite group** if the set G has a finite number of elements. In this case, the number of elements is called the **order** of G, denoted by $|G|$. If G is not finite, it is said to be an **infinite group**.

Finite group vs. Infinite group

Definition 11

A group G is said to be a **finite group** if the set G has a finite number of elements. In this case, the number of elements is called the **order** of G, denoted by $|G|$. If G is not finite, it is said to be an **infinite group**.

Recall that the *modulus* n is a positive integer, and then two integers

$$a, b \text{ are } \textit{congruent modulo } \text{n, written } a \equiv b \pmod{n},$$

if a and b have the same remainder when divided by n.

Finite group vs. Infinite group

Definition 11

A group G is said to be a **finite group** if the set G has a finite number of elements. In this case, the number of elements is called the **order** of G, denoted by $|G|$. If G is not finite, it is said to be an **infinite group**.

Recall that the *modulus* n is a positive integer, and then two integers

$$a, b \text{ are } \textit{congruent modulo } \text{n, written } a \equiv b \pmod{n},$$

if a and b have the same remainder when divided by n.
Let $[a]_n$ denote the set of all integers that are congruent to a modulo n.
Given $[a]_n$ and $[b]_n$ we define

$$[a]_n + [b]_n = [a+b]_n.$$

Finite group vs. Infinite group

Definition 11

A group G is said to be a **finite group** if the set G has a finite number of elements. In this case, the number of elements is called the **order** of G, denoted by $|G|$. If G is not finite, it is said to be an **infinite group**.

Recall that the *modulus* n is a positive integer, and then two integers

$$a, b \text{ are } \textit{congruent modulo } \text{n, written } a \equiv b \pmod{n},$$

if a and b have the same remainder when divided by n.
Let $[a]_n$ denote the set of all integers that are congruent to a modulo n.
Given $[a]_n$ and $[b]_n$ we define

$$[a]_n + [b]_n = [a+b]_n.$$

Question 1

Does it define a binary operation? Is it really well-defined?

Finite group vs. Infinite group

Definition 11

A group G is said to be a **finite group** if the set G has a finite number of elements. In this case, the number of elements is called the **order** of G, denoted by $|G|$. If G is not finite, it is said to be an **infinite group**.

Recall that the *modulus* n is a positive integer, and then two integers

$$a, b \text{ are } \textit{congruent modulo } \text{n, written } a \equiv b \pmod{n},$$

if a and b have the same remainder when divided by n.
Let $[a]_n$ denote the set of all integers that are congruent to a modulo n.
Given $[a]_n$ and $[b]_n$ we define

$$[a]_n + [b]_n = [a+b]_n.$$

Question 1

Does it define a binary operation? Is it really well-defined?

Yes! (Why?) [

Finite group vs. Infinite group

Definition 11

A group G is said to be a **finite group** if the set G has a finite number of elements. In this case, the number of elements is called the **order** of G, denoted by $|G|$. If G is not finite, it is said to be an **infinite group**.

Recall that the *modulus* n is a positive integer, and then two integers

a, b are *congruent modulo* n, written $a \equiv b \pmod{n}$,

if a and b have the same remainder when divided by n.
Let $[a]_n$ denote the set of all integers that are congruent to a modulo n.
Given $[a]_n$ and $[b]_n$ we define

$$[a]_n + [b]_n = [a+b]_n.$$

Question 1

Does it define a binary operation? Is it really well-defined?

Yes! (Why?) $[a_1 \equiv a_2 \pmod{n}, b_1 \equiv b_2 \pmod{n} \Rightarrow a_1 + b_1 \equiv a_2 + b_2 \pmod{n}]$

$\mathbf{Z}_n$: Group of integers modulo n

Proposition 6

$\mathbf{Z}_n$ is an abelian group under addition of congruence classes for $n \in \mathbf{Z}_{>0}$. The group $\mathbf{Z}_n$ is finite and $|\mathbf{Z}_n| = n$.

$\mathbf{Z}_n$: Group of integers modulo n

Proposition 6

$\mathbf{Z}_n$ is an abelian group under addition of congruence classes for $n \in \mathbf{Z}_{>0}$. The group $\mathbf{Z}_n$ is finite and $|\mathbf{Z}_n| = n$.

(i) **Closure:** well-defined ✓

(ii) **Associative:** ✓ (Check it!)

(iii) **Commutative:** $[a]_n + [b]_n = [a+b]_n = [b+a]_n = [b]_n + [a]_n$.

(iv) **Identity:** $[a]_n + [0]_n = [a+0]_n = [a]_n$.

(v) **Inverses:** $[a]_n + [-a]_n = [a-a]_n = [0]_n$.

$\mathbf{Z}_n$: Group of integers modulo n

Proposition 6

$\mathbf{Z}_n$ is an abelian group under addition of congruence classes for $n \in \mathbf{Z}_{>0}$. The group $\mathbf{Z}_n$ is finite and $|\mathbf{Z}_n| = n$.

(i) **Closure:** well-defined ✓

(ii) **Associative:** ✓ (Check it!)

(iii) **Commutative:** $[a]_n + [b]_n = [a+b]_n = [b+a]_n = [b]_n + [a]_n$.

(iv) **Identity:** $[a]_n + [0]_n = [a+0]_n = [a]_n$.

(v) **Inverses:** $[a]_n + [-a]_n = [a-a]_n = [0]_n$.

For each $a \in \mathbf{Z}$, $[a]_n = [r]_n$ for a unique $r \in \mathbf{Z}$ with $0 \leq r < n$. $\Rightarrow |\mathbf{Z}_n| = n$

$\mathbf{Z}_n$: Group of integers modulo n

Proposition 6

$\mathbf{Z}_n$ is an abelian group under addition of congruence classes for $n \in \mathbf{Z}_{>0}$. The group $\mathbf{Z}_n$ is finite and $|\mathbf{Z}_n| = n$.

(i) **Closure:** well-defined ✓

(ii) **Associative:** ✓ (Check it!)

(iii) **Commutative:** $[a]_n + [b]_n = [a+b]_n = [b+a]_n = [b]_n + [a]_n$.

(iv) **Identity:** $[a]_n + [0]_n = [a+0]_n = [a]_n$.

(v) **Inverses:** $[a]_n + [-a]_n = [a-a]_n = [0]_n$.

For each $a \in \mathbf{Z}$, $[a]_n = [r]_n$ for a unique $r \in \mathbf{Z}$ with $0 \leq r < n$. $\Rightarrow |\mathbf{Z}_n| = n$

Question 2

Is the result true for multiplication? I.e., is $\mathbf{Z}_n$ an abelian group under $\cdot$?

$\mathbf{Z}_n$: Group of integers modulo n

Proposition 6

$\mathbf{Z}_n$ is an abelian group under addition of congruence classes for $n \in \mathbf{Z}_{>0}$. The group $\mathbf{Z}_n$ is finite and $|\mathbf{Z}_n| = n$.

(i) **Closure:** well-defined ✓

(ii) **Associative:** ✓ (Check it!)

(iii) **Commutative:** $[a]_n + [b]_n = [a+b]_n = [b+a]_n = [b]_n + [a]_n$.

(iv) **Identity:** $[a]_n + [0]_n = [a+0]_n = [a]_n$.

(v) **Inverses:** $[a]_n + [-a]_n = [a-a]_n = [0]_n$.

For each $a \in \mathbf{Z}$, $[a]_n = [r]_n$ for a unique $r \in \mathbf{Z}$ with $0 \leq r < n$. $\Rightarrow |\mathbf{Z}_n| = n$

Question 2

Is the result true for multiplication? I.e., is $\mathbf{Z}_n$ an abelian group under $\cdot$?

No! (Why?) [

$\mathbf{Z}_n$: Group of integers modulo n

Proposition 6

$\mathbf{Z}_n$ is an abelian group under addition of congruence classes for $n \in \mathbf{Z}_{>0}$. The group $\mathbf{Z}_n$ is finite and $|\mathbf{Z}_n| = n$.

(i) **Closure:** well-defined ✓

(ii) **Associative:** ✓ (Check it!)

(iii) **Commutative:** $[a]_n + [b]_n = [a+b]_n = [b+a]_n = [b]_n + [a]_n$.

(iv) **Identity:** $[a]_n + [0]_n = [a+0]_n = [a]_n$.

(v) **Inverses:** $[a]_n + [-a]_n = [a-a]_n = [0]_n$.

For each $a \in \mathbf{Z}$, $[a]_n = [r]_n$ for a unique $r \in \mathbf{Z}$ with $0 \leq r < n$. $\Rightarrow |\mathbf{Z}_n| = n$

Question 2

Is the result true for multiplication? I.e., is $\mathbf{Z}_n$ an abelian group under $\cdot$?

No! (Why?) [In fact, $\mathbf{Z}_n$ is NOT even a group under multiplication.]

$\mathbf{Z}_n^\times$: Group of units modulo n

Proposition 7

$\mathbf{Z}_n^\times$ is an abelian group under multiplication of congruence classes for $n \in \mathbf{Z}_{>0}$. The group $\mathbf{Z}_n^\times$ is finite and $|\mathbf{Z}_n^\times| = \varphi(n)$.

$\mathbf{Z}_n^\times$: Group of units modulo n

Proposition 7

$\mathbf{Z}_n^\times$ is an abelian group under multiplication of congruence classes for $n \in \mathbf{Z}_{>0}$. The group $\mathbf{Z}_n^\times$ is finite and $|\mathbf{Z}_n^\times| = \varphi(n)$.

(i) **Closure:** $[a]_n, [b]_n \in \mathbf{Z}_n^\times \Rightarrow [a]_n \cdot [b]_n \in \mathbf{Z}_n^\times$ (Check it!)
Well-defined: $a_1 \equiv a_2 \pmod{n}, b_1 \equiv b_2 \pmod{n} \Rightarrow a_1 b_1 \equiv a_2 b_2 \pmod{n}$

(ii) **Associative:** ✓ (Check it!)

(iii) **Commutative:** $[a]_n \cdot [b]_n = [a \cdot b]_n = [b \cdot a]_n = [b]_n \cdot [a]_n$.

(iv) **Identity:** $[a]_n \cdot [1]_n = [a \cdot 1]_n = [a]_n$.

(v) **Inverses:** $\mathbf{Z}_n^\times := \{[a]_n \big| (a, n) = 1\}$ & multiplicative inverses belong to $\mathbf{Z}_n^\times$.

$\mathbf{Z}_n^\times$: Group of units modulo n

Proposition 7

$\mathbf{Z}_n^\times$ is an abelian group under multiplication of congruence classes for $n \in \mathbf{Z}_{>0}$. The group $\mathbf{Z}_n^\times$ is finite and $|\mathbf{Z}_n^\times| = \varphi(n)$.

(i) **Closure:** $[a]_n, [b]_n \in \mathbf{Z}_n^\times \Rightarrow [a]_n \cdot [b]_n \in \mathbf{Z}_n^\times$ (Check it!)
Well-defined: $a_1 \equiv a_2 \pmod{n}, b_1 \equiv b_2 \pmod{n} \Rightarrow a_1 b_1 \equiv a_2 b_2 \pmod{n}$

(ii) **Associative:** ✓ (Check it!)

(iii) **Commutative:** $[a]_n \cdot [b]_n = [a \cdot b]_n = [b \cdot a]_n = [b]_n \cdot [a]_n$.

(iv) **Identity:** $[a]_n \cdot [1]_n = [a \cdot 1]_n = [a]_n$.

(v) **Inverses:** $\mathbf{Z}_n^\times := \{[a]_n \big| (a, n) = 1\}$ & multiplicative inverses belong to $\mathbf{Z}_n^\times$.

We have seen $|\mathbf{Z}_n^\times| = \varphi(n)$ before, where $\varphi(n)$ is the Euler φ-function. □

Example: Multiplication table of $\mathbf{Z}_8^\times$

	[1]	[3]	[5]	[7]
[1]	[1]	[3]	[5]	[7]
[3]	[3]	[1]	[7]	[5]
[5]	[5]	[7]	[1]	[3]
[7]	[7]	[5]	[3]	[1]

Example: Multiplication table of $\mathbf{Z}_8^\times$

	[1]	[3]	[5]	[7]
[1]	[1]	[3]	[5]	[7]
[3]	[3]	[1]	[7]	[5]
[5]	[5]	[7]	[1]	[3]
[7]	[7]	[5]	[3]	[1]

Again,

- in each row, each element of the group occurs exactly once.
- in each column, each element of the group occurs exactly once.

Examples from Matrices

Example 12

$M_n(\mathbf{R})$ forms a group under matrix addition.

(i) Closure: (Check it!)

(ii) Associativity: (Check it!)

(iii) Identity: zero matrix

(iv) Inverses: its negative

Examples from Matrices

Example 12

$M_n(\mathbf{R})$ forms a group under matrix addition.

(i) Closure: (Check it!)

(ii) Associativity: (Check it!)

(iii) Identity: zero matrix

(iv) Inverses: its negative

Q: Is there a matrix group under matrix multiplication?

Examples from Matrices

Example 12

$M_n(\mathbf{R})$ forms a group under matrix addition.

(i) Closure: (Check it!)

(ii) Associativity: (Check it!)

(iii) Identity: zero matrix

(iv) Inverses: its negative

Q: Is there a matrix group under matrix multiplication? **Yes!**

Definition 13

The set of all invertible $n \times n$ matrices with entries in $\mathbf{R}$ is called the **general linear group of degree n over the real numbers**, and is denoted by $\mathrm{GL}_n(\mathbf{R})$.

Examples from Matrices

Example 12

$M_n(\mathbf{R})$ forms a group under matrix addition.

(i) Closure: (Check it!)

(ii) Associativity: (Check it!)

(iii) Identity: zero matrix

(iv) Inverses: its negative

Q: Is there a matrix group under matrix multiplication? **Yes!**

Definition 13

The set of all invertible $n \times n$ matrices with entries in $\mathbf{R}$ is called the **general linear group of degree n over the real numbers**, and is denoted by $\mathrm{GL}_n(\mathbf{R})$.

Proposition 8

$\mathrm{GL}_n(\mathbf{R})$ *forms a group under matrix multiplication.*

Proof of Proposition 8

Recall that

$$\begin{bmatrix} a_{11} & a_{12} \\ a_{21} & a_{22} \end{bmatrix} \begin{bmatrix} b_{11} & b_{12} \\ b_{21} & b_{22} \end{bmatrix} = \begin{bmatrix} a_{11}b_{11}+a_{12}b_{21} & a_{11}b_{12}+a_{12}b_{22} \\ a_{21}b_{11}+a_{22}b_{21} & a_{21}b_{12}+a_{22}b_{22} \end{bmatrix}.$$

Proof of Proposition 8

Recall that

$$\begin{bmatrix} a_{11} & a_{12} \\ a_{21} & a_{22} \end{bmatrix} \begin{bmatrix} b_{11} & b_{12} \\ b_{21} & b_{22} \end{bmatrix} = \begin{bmatrix} a_{11}b_{11}+a_{12}b_{21} & a_{11}b_{12}+a_{12}b_{22} \\ a_{21}b_{11}+a_{22}b_{21} & a_{21}b_{12}+a_{22}b_{22} \end{bmatrix}.$$

A matrix $A = \begin{bmatrix} a & b \\ c & d \end{bmatrix}$ has an inverse if and only if its determinant $\det(A) = ad - bc$ is nonzero, and

Proof of Proposition 8

Recall that

$$\begin{bmatrix} a_{11} & a_{12} \\ a_{21} & a_{22} \end{bmatrix} \begin{bmatrix} b_{11} & b_{12} \\ b_{21} & b_{22} \end{bmatrix} = \begin{bmatrix} a_{11}b_{11}+a_{12}b_{21} & a_{11}b_{12}+a_{12}b_{22} \\ a_{21}b_{11}+a_{22}b_{21} & a_{21}b_{12}+a_{22}b_{22} \end{bmatrix}.$$

A matrix $A = \begin{bmatrix} a & b \\ c & d \end{bmatrix}$ has an inverse if and only if its determinant $\det(A) = ad - bc$ is nonzero, and the inverse $A^{-1} = \frac{1}{ad-bc} \begin{bmatrix} d & -b \\ -c & a \end{bmatrix}$.

To show: $\mathrm{GL}_n(\mathbf{R})$ forms a group under matrix multiplication.

Proof of Proposition 8

Recall that

$$\begin{bmatrix} a_{11} & a_{12} \\ a_{21} & a_{22} \end{bmatrix} \begin{bmatrix} b_{11} & b_{12} \\ b_{21} & b_{22} \end{bmatrix} = \begin{bmatrix} a_{11}b_{11}+a_{12}b_{21} & a_{11}b_{12}+a_{12}b_{22} \\ a_{21}b_{11}+a_{22}b_{21} & a_{21}b_{12}+a_{22}b_{22} \end{bmatrix}.$$

A matrix $A = \begin{bmatrix} a & b \\ c & d \end{bmatrix}$ has an inverse if and only if its determinant $\det(A) = ad - bc$ is nonzero, and the inverse $A^{-1} = \frac{1}{ad-bc}\begin{bmatrix} d & -b \\ -c & a \end{bmatrix}$.

To show: $\mathrm{GL}_n(\mathbf{R})$ forms a group under matrix multiplication.

(i) **Closure:**

Proof of Proposition 8

Recall that

$$\begin{bmatrix} a_{11} & a_{12} \\ a_{21} & a_{22} \end{bmatrix} \begin{bmatrix} b_{11} & b_{12} \\ b_{21} & b_{22} \end{bmatrix} = \begin{bmatrix} a_{11}b_{11}+a_{12}b_{21} & a_{11}b_{12}+a_{12}b_{22} \\ a_{21}b_{11}+a_{22}b_{21} & a_{21}b_{12}+a_{22}b_{22} \end{bmatrix}.$$

A matrix $A = \begin{bmatrix} a & b \\ c & d \end{bmatrix}$ has an inverse if and only if its determinant $\det(A) = ad - bc$ is nonzero, and the inverse $A^{-1} = \frac{1}{ad-bc}\begin{bmatrix} d & -b \\ -c & a \end{bmatrix}$.

To show: $\mathrm{GL}_n(\mathbf{R})$ forms a group under matrix multiplication.

(i) **Closure:** If (a_{ij}) and (b_{ij}) are $n \times n$ matrices, then the product (c_{ij}) with (i, j)-entries $c_{ij} = \sum_{k=1}^{n} a_{ik} b_{kj}$. This shows the well-definedness.

Proof of Proposition 8

Recall that

$$\begin{bmatrix} a_{11} & a_{12} \\ a_{21} & a_{22} \end{bmatrix} \begin{bmatrix} b_{11} & b_{12} \\ b_{21} & b_{22} \end{bmatrix} = \begin{bmatrix} a_{11}b_{11}+a_{12}b_{21} & a_{11}b_{12}+a_{12}b_{22} \\ a_{21}b_{11}+a_{22}b_{21} & a_{21}b_{12}+a_{22}b_{22} \end{bmatrix}.$$

A matrix $A = \begin{bmatrix} a & b \\ c & d \end{bmatrix}$ has an inverse if and only if its determinant $\det(A) = ad - bc$ is nonzero, and the inverse $A^{-1} = \frac{1}{ad-bc}\begin{bmatrix} d & -b \\ -c & a \end{bmatrix}$.

To show: $\mathrm{GL}_n(\mathbf{R})$ forms a group under matrix multiplication.

(i) **Closure:** If (a_{ij}) and (b_{ij}) are $n \times n$ matrices, then the product (c_{ij}) with (i, j)-entries $c_{ij} = \sum_{k=1}^{n} a_{ik} b_{kj}$. This shows the well-definedness.

If A and B are invertible matrices in $\mathrm{GL}_n(\mathbf{R})$, then

$\det(AB) = \det(A)\det(B) \neq 0$. Closed under matrix multiplication.

Proof of Proposition 8

Recall that

$$\begin{bmatrix} a_{11} & a_{12} \\ a_{21} & a_{22} \end{bmatrix} \begin{bmatrix} b_{11} & b_{12} \\ b_{21} & b_{22} \end{bmatrix} = \begin{bmatrix} a_{11}b_{11}+a_{12}b_{21} & a_{11}b_{12}+a_{12}b_{22} \\ a_{21}b_{11}+a_{22}b_{21} & a_{21}b_{12}+a_{22}b_{22} \end{bmatrix}.$$

A matrix $A = \begin{bmatrix} a & b \\ c & d \end{bmatrix}$ has an inverse if and only if its determinant $\det(A) = ad - bc$ is nonzero, and the inverse $A^{-1} = \frac{1}{ad-bc}\begin{bmatrix} d & -b \\ -c & a \end{bmatrix}$.

To show: $\mathrm{GL}_n(\mathbf{R})$ forms a group under matrix multiplication.

(i) **Closure:** If (a_{ij}) and (b_{ij}) are $n \times n$ matrices, then the product (c_{ij})

with (i,j)-entries $c_{ij} = \sum_{k=1}^{n} a_{ik}b_{kj}$. This shows the well-definedness.

If A and B are invertible matrices in $\mathrm{GL}_n(\mathbf{R})$, then

$\det(AB) = \det(A)\det(B) \neq 0$. Closed under matrix multiplication.

(ii) **Associativity:** *You should see the proof in linear algebra course.*

(iii) **Identity:** The identity matrix I_n

(iv) **Inverses:** $A^{-1}, \forall A \in \mathrm{GL}_n(\mathbf{R})$. (definition of invertible matrix)

Conjugacy

Definition 14

R is an **equivalence relation** if and only if for all $a, b, c \in S$ we have

(1) [Reflexive law] $a \sim a$;

(2) [Symmetric law] if $a \sim b$, then $b \sim a$;

(3) [Transitive law] if $a \sim b$ and $b \sim c$, then $a \sim c$.

Conjugacy

Definition 14

R is an **equivalence relation** if and only if for all $a, b, c \in S$ we have

(1) [Reflexive law] $a \sim a$;

(2) [Symmetric law] if $a \sim b$, then $b \sim a$;

(3) [Transitive law] if $a \sim b$ and $b \sim c$, then $a \sim c$.

Definition 15

Let G be a group and let $x, y \in G$. Write $x \sim y$ if there exists an element $a \in G$ such that $y = axa^{-1}$. In this case we say that y is a **conjugate** of x.

Conjugacy

Definition 14

R is an **equivalence relation** if and only if for all $a, b, c \in S$ we have

(1) [Reflexive law] $a \sim a$;

(2) [Symmetric law] if $a \sim b$, then $b \sim a$;

(3) [Transitive law] if $a \sim b$ and $b \sim c$, then $a \sim c$.

Definition 15

Let G be a group and let $x, y \in G$. Write $x \sim y$ if there exists an element $a \in G$ such that $y = axa^{-1}$. In this case we say that y is a **conjugate** of x.

Proposition 9

The above relation $\sim$ defines an equivalence relation on G.

Conjugacy

Definition 14

R is an **equivalence relation** if and only if for all $a, b, c \in S$ we have

(1) [Reflexive law] $a \sim a$;

(2) [Symmetric law] if $a \sim b$, then $b \sim a$;

(3) [Transitive law] if $a \sim b$ and $b \sim c$, then $a \sim c$.

Definition 15

Let G be a group and let $x, y \in G$. Write $x \sim y$ if there exists an element $a \in G$ such that $y = axa^{-1}$. In this case we say that y is a **conjugate** of x.

Proposition 9

The above relation $\sim$ defines an equivalence relation on G.

(1) [Reflexive law]:

Conjugacy

Definition 14

R is an **equivalence relation** if and only if for all $a, b, c \in S$ we have

(1) [Reflexive law] $a \sim a$;

(2) [Symmetric law] if $a \sim b$, then $b \sim a$;

(3) [Transitive law] if $a \sim b$ and $b \sim c$, then $a \sim c$.

Definition 15

Let G be a group and let $x, y \in G$. Write $x \sim y$ if there exists an element $a \in G$ such that $y = axa^{-1}$. In this case we say that y is a **conjugate** of x.

Proposition 9

The above relation $\sim$ defines an equivalence relation on G.

(1) [Reflexive law]: $x = exe^{-1}$ for all $x \in G$.

(2) [Symmetric law]: $y = axa^{-1} \Rightarrow$

Conjugacy

Definition 14

R is an **equivalence relation** if and only if for all $a, b, c \in S$ we have

(1) [Reflexive law] $a \sim a$;

(2) [Symmetric law] if $a \sim b$, then $b \sim a$;

(3) [Transitive law] if $a \sim b$ and $b \sim c$, then $a \sim c$.

Definition 15

Let G be a group and let $x, y \in G$. Write $x \sim y$ if there exists an element $a \in G$ such that $y = axa^{-1}$. In this case we say that y is a **conjugate** of x.

Proposition 9

The above relation $\sim$ defines an equivalence relation on G.

(1) [Reflexive law]: $x = exe^{-1}$ for all $x \in G$.

(2) [Symmetric law]: $y = axa^{-1} \Rightarrow x = a^{-1}y(a^{-1})^{-1}$. (Check it!)

(3) [Transitive law]: $y = axa^{-1}, z = byb^{-1} \Rightarrow$

Conjugacy

Definition 14

R is an **equivalence relation** if and only if for all $a, b, c \in S$ we have

(1) [Reflexive law] $a \sim a$;

(2) [Symmetric law] if $a \sim b$, then $b \sim a$;

(3) [Transitive law] if $a \sim b$ and $b \sim c$, then $a \sim c$.

Definition 15

Let G be a group and let $x, y \in G$. Write $x \sim y$ if there exists an element $a \in G$ such that $y = axa^{-1}$. In this case we say that y is a **conjugate** of x.

Proposition 9

The above relation $\sim$ defines an equivalence relation on G.

(1) [Reflexive law]: $x = exe^{-1}$ for all $x \in G$.

(2) [Symmetric law]: $y = axa^{-1} \Rightarrow x = a^{-1}y(a^{-1})^{-1}$. (Check it!)

(3) [Transitive law]: $y = axa^{-1}, z = byb^{-1} \Rightarrow z = (ba)x(ba)^{-1}$. (Why?)