Section 4 – Groups

Instructor: Yifan Yang

Fall 2006

Outline

Definition and examples

Definition (4.1)

A group $\langle G, * \rangle$ is a set G, closed under a binary operation $*$, such that

1. $*$ is associative. That is, $(a * b) * c = a * (b * c)$ for all $a, b, c \in G$.
2. There is an identity element $e \in G$ for $*$. That is, there exists $e \in G$ such that $e * x = x * e = x$ for all $x \in G$.
3. Corresponding to each element a of G, there is an inverse a' of a in G such that $a' * a = a * a' = e$.

Examples

1. The binary structure $\langle \mathbb{Z}, + \rangle$ is a group. The identity element is 0, and the inverse a' of $a \in \mathbb{Z}$ is $-a$.
2. The binary structure $\langle \mathbb{Z}, \cdot \rangle$ is not a group because the inverse a' does not exist when $a \neq \pm 1$.
3. The set $\mathbb{Z}_n$ under addition $+_n$ is a group.
4. The set $\mathbb{Z}_n$ under multiplication $\cdot_n$ is not a group since the inverse of $\bar{0}$ does not exist.
5. The set $\mathbb{Z}^+$ under addition is not a group because there is no identity element.
6. The set $\mathbb{Z}^+ \cup \{0\}$ under addition is still not a group. There is an identity element 0, but no inverse for elements $a > 0$.
7. The set of all real-valued functions with domain $\mathbb{R}$ under function addition is a group.
8. The set $M_{m \times n}(\mathbb{R})$ of all $m \times n$ matrices under matrix addition is a group.

Examples

Example

The set $GL(n, \mathbb{R})$ of all invertible $n \times n$ matrices under matrix multiplication is a group. (GL stands for general linear.)

1. Closedness: Recall that an $n \times n$ matrix A is invertible if and only if $\det A \neq 0$. Suppose that A and B are invertible. Then $\det(A), \det(B) \neq 0$, and $\det(AB) = \det(A)\det(B) \neq 0$. Therefore, $A, B \in GL(n, \mathbb{R}) \Rightarrow AB \in GL(n, \mathbb{R})$.
2. Associativity: Property of matrix multiplication.
3. Identity element: The matrix I_n satisfies $AI_n = I_nA = A$ for all $A \in GL(n, \mathbb{R})$.
4. Inverse: Suppose that $A \in GL(n, \mathbb{R})$. Then A^{-1} is also in $GL(n, \mathbb{R})$ since $\det(A^{-1}) = 1/\det(A) \neq 0$.

Remark

In some textbooks, the definition of a group is given as follows.

Definition

A binary structure $\langle G, * \rangle$ is a group if

1. $*$ is associative.
2. There exists a left identity element e in G such that $e * x = x$ for all $x \in G$.
3. For each $a \in G$, there exists a left inverse a' in G such that $a' * a = e$.

It can be shown that this definition is equivalent to the definition given earlier.

In-class exercises

Determine whether the following binary structures are groups.

1. The set $\mathbb{Q}^+$ under the usual multiplication.
2. The set $\mathbb{C}^*$ under the usual multiplication.
3. The set $\mathbb{Q}^+$ with $*$ given by $a * b = ab/2$.
4. The set $\mathbb{R}^+$ with $*$ given by $a * b = \sqrt{ab}$.

Definition

A group G is abelian if its binary operation is commutative.

Remark

Commutative groups are called abelian in honor of the Norwegian mathematician Niels Henrik Abel (1802–1829), who studied the problem when a polynomial equation is solvable by radical. The ideas introduced by him evolved into what we called group theory today.

In 2002, the Norwegian government established the Abel prize, to be awarded annually to mathematicians. The prize comes with a monetary award of roughly $1,000,000 USD.

Examples

The following groups are all abelian.

1. $\langle \mathbb{Z}, + \rangle$, $\langle \mathbb{Q}, + \rangle$, $\langle \mathbb{R}, + \rangle$, and $\langle \mathbb{C}, + \rangle$.
2. $\langle \mathbb{Q}^+, \cdot \rangle$, $\langle \mathbb{R}^*, \cdot \rangle$, and $\langle \mathbb{C}^*, \cdot \rangle$.
3. $\langle \mathbb{Z}_n, +_n \rangle$.
4. The set of $M_{m \times n}(\mathbb{R})$ under addition.
5. The set of all real-valued functions with domain $\mathbb{R}$ under function addition.

The following groups are non-abelian.

1. $GL(n, \mathbb{R})$ under matrix multiplication.
2. The set of all real-valued functions with domain $\mathbb{R}$ under function composition.

Cancellation law

Theorem (4.15)

Let $\langle G, *\rangle$ be a group. Then the left and right cancellation laws hold in G, that is, $a * b = a * c$ implies $b = c$, and $b * a = c * a$ implies $b = c$ for all $a, b, c \in G$.

Remark

Not all binary structures have cancellation laws. For instance,

1. In $M_n(\mathbb{R})$, $AB = AC$ does not imply $B = C$.
2. In $(\mathbb{Z}_n, \cdot_n)$, the cancellation law does not hold either. (In $(\mathbb{Z}_6, \cdot_6)$ we have $\bar{3} \cdot \bar{2} = \bar{0} = \bar{3} \cdot \bar{4}$, but $\bar{2} \neq \bar{4}$.)

Proof of Theorem 4.15

Suppose that $a * b = a * c$. Let a' be an inverse of a. Consider the equality

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

By the associativity of $*$, we then have

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

Since a' is an inverse of a, we have $a' * a = e$, and thus,

$$e * b = e * c.$$

Because e is the identity element, it follows that $b = c$. The proof of the assertion that $b * a = c * a$ implies $b = c$ is similar.

The equation $a * x = b$

Theorem (4.16)

Let $\langle G, * \rangle$ be a group. Let a and b be elements in G. Then the equations $a * x = b$ and $y * a = b$ have unique solutions x and y in G.

Remark

Again, there are binary structures where $a * x = b$ may not be solvable for all a and b.

1. In $M_n(\mathbb{R})$ under matrix multiplication, the equation $AX = B$ is not solvable when $\det(A) = 0$ and $\det(B) \neq 0$.
2. In $\langle \mathbb{Z}_8, \cdot_8 \rangle$, the equation $\bar{2} \cdot x = \bar{1}$ is not solvable since $\bar{2} \cdot x$ must be one of $\bar{0}$, $\bar{2}$, $\bar{4}$, and $\bar{6}$.

Proof of Theorem 4.16

Proof.

Let $x = a' * b$. Then

$$a * (a' * b) = (a * a') * b = e * b = b.$$

This shows that the equation $a * x = b$ has at least one solution. To show the uniqueness of the solution, we use the cancellation laws. If x_1 and x_2 are both solutions of $a * x = b$. Then $a * x_1 = a * x_2$. By Theorem 4.15, we therefore have $x_1 = x_2$. The assertion about $y * a = b$ can be proved similarly. $\square$

Uniqueness of identity element and inverse

Theorem (4.17)

Let $\langle G, * \rangle$ be a group. There is only one element e in G such that $e * x = x * e = x$ for all $x \in G$. Likewise, for each $a \in G$, there is only one element a' in G such that $a' * a = a * a' = e$.

Proof.

The uniqueness of identity element is proved in Theorem 3.13. We now prove the uniqueness of inverses. Let $a \in G$. Suppose that a_1 and a_2 satisfy $a * a_1 = a_1 * a = e$ and $a * a_2 = a_2 * a = e$. Then $a * a_1 = a * a_2$. By Theorem 4.15, we have $a_1 = a_2$. $\square$

Uniqueness of identity element and inverse

Corollary (4.18)

Let $\langle G, * \rangle$ be a group. For all $a, b \in G$ we have $(a * b)' = b' * a'$.

Proof.

We have

$$(a * b) * (b' * a') = a * (b * b') * a' = (a * e) * a' = a * a' = e.$$

By Theorem 4.17, the element $b' * a'$ has to be the inverse of $a * b$. $\square$

Case $|G| = 2$

Let G be a group with two element. Since G contains an identity element e, we assume that $G = \{e, a\}$. We now determine the group table. We have

$*$	e	a
e	e	a
a	a	?

It remains to determine $a * a$. The group G contains the inverse of a. From the table, it is clear that $a' \neq e$. Thus, $a' = a$ and we have $a * a = e$. We now check the associativity of $*$.

In theory, we need to check whether

$$(x * y) * z = x * (y * z)$$

for all 8 possible choices of $x, y, z \in G$. Here we notice that the table is isomorphic to that of $\langle \mathbb{Z}_2, +_2 \rangle$.

$*$	e	a
e	e	a
a	a	e

$+_2$	$\bar{0}$	$\bar{1}$
$\bar{0}$	$\bar{0}$	$\bar{1}$
$\bar{1}$	$\bar{1}$	$\bar{0}$

.

Since $\langle \mathbb{Z}_2, +_2 \rangle$ is associative, so is the binary structure we just constructed. Finally, the table is symmetric with respect to the diagonal. In other words, G is abelian ($*$ is commutative).

Case $|G| = 3$

Let G be a group with three element e, a, b. We have

$*$	e	a	b
e	e	a	b
a	a	?	?
b	b	?	?

$*$	e	a	b
e	e	a	b
a	a	?	e
b	b	e	?

$*$	e	a	b
e	e	a	b
a	a	b	e
b	b	e	a

Consider $a * b$. What can it be? If $a * b = a$, then $a * b = a * e$ and $b = e$, which is a contradiction. Likewise, $a * b \neq b$, and we conclude that $a * b = e$, that is, $a' = b$ and

It remains to check associativity. Again, it is tedious to check directly that

$$x * (y * z) = (x * y) * z$$

holds for all $x, y, z \in G$. Instead, we observe that the table is isomorphic to that of $\langle \mathbb{Z}_3, +_3 \rangle$. Thus, $*$ is indeed associative. Note also that $*$ is commutative.

General cases

In general, there are many non-isomorphic groups of a given order (number of elements). For example, there are 2 non-isomorphic groups of order 4, 5 non-isomorphic groups of order 8, 14 non-isomorphic groups of order 16, and $423,164,062$ non-isomorphic groups of order 1024.

In any case, the group table satisfies every element of the group appears in each row/each column exactly once. This is because the equation $a * x = b$ has exactly one solution.

Exercises

In-class exercise

Give all possible group tables for the case $|G| = 4$.

Homework

Do Problems 6, 8, 14, 19, 24, 29, 30, 32, 36, 38 of Section 4.