Abstract algebra

Fundamentals

Jesús García Díaz

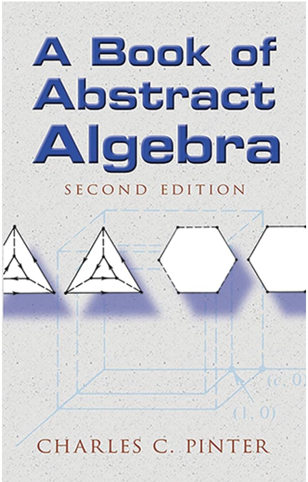
CONAHCYT
INAOE

July 9 2024

Contents

1. A bit of history
2. Algebraic structures
3. Groups
4. Rings
5. Fields
6. Vector spaces
7. Ending

Bibliography



A bit of history

A bit of history

The word “algebra” is derived from the Arabic word *al-gebr*, meaning reunion of broken parts. During the 11th century, it was perhaps the Islamic world that represented the most mathematically sophisticated civilization. However, there was no algebraic manipulation of the kind seen in modern texts, and medieval mathematical writing was rethorical, with everything being described in words. This “algebra” is the algebra of real numbers, which for millenia was explicitly defined as the *science of solving equations*.

A bit of history

Most of the major ancient civilizations, the Babylonian, Egyptian, Chinese, and Hindu, dealt with the solution of polynomial equations, mainly linear and quadratic equations. The Babylonians (c. 1700 BC) were particularly proficient algebraists. They were able to solve quadratic equations by methods similar to ours.

A bit of history

It is the Rennaisance (XVI century). After thousands of years of ignoring the formula for cubic equations, in 1535, Tartaglia announced he had found a formula for cubic equations of the form $x2 + ax2 = b$ (that is, without the x term). Soon, he was challenged by Antonio Fior, a pupil of Scipio del Ferro, who had already found a formula for solving cubic equations of the form $x^3 + ax = b$ (that is, without the x^2 term). A few days before the contest, Tartaglia found the formula for general cubic equations.

Nicolo de Fontana (Tartaglia)

A bit of history

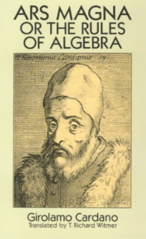
For some time, Tartaglia kept his method to himself. However, Girolamo Cardano persuaded him to share his secret (Tartaglia asked Cardano never to reveal his secret, and Cardano promised to help him become an artillery adviser to the Spanish army).

A bit of history

For some time, Tartaglia kept his method to himself. However, Girolamo Cardano persuaded him to share his secret (Tartaglia asked Cardano never to reveal his secret, and Cardano promised to help him become an artillery adviser to the Spanish army).

A few years later, Cardano published *Ars Magna*, in which he presented the algebraic knowledge of his time, including Tartaglia's method.

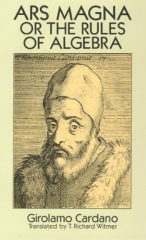
Nicolo de Fontana (Tartaglia)



Girolamo Cardano

A bit of history

The next great step in the progress of algebra was made by Cardano's personal servant, Ludovico Ferrari, who found the general method for solving quartic equations ($x^4 + ax^3 + bx^2 + cx = d$).



ARS MAGNA
OR THE RULES
OF ALGEBRA

Girolamo Cardano
Translated by T. Richard Witmer

Girolamo Cardano

Ludovico Ferrari

A bit of history

Now the challenge was clear: to find a formula for the roots of equations of degree 5 or higher. During the next centuries, there was hardly a mathematician of distinction who did not try to solve this problem.

A bit of history

Now the challenge was clear: to find a formula for the roots of equations of degree 5 or higher. During the next centuries, there was hardly a mathematician of distinction who did not try to solve this problem.

It was a great surprise when, in 1824, a young Niels Abel showed that such a formula do not exist. This discovery opened the doors to new directions in mathematics.

Niels Abel

A bit of history

Around those days (XIX century), different characters started playing around with *new algebras*. To date, hundreds of algebras have been invented (discovered?).

Évariste Galois

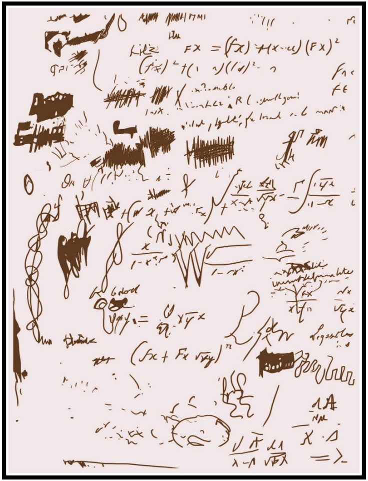
Carl Friedrich Gauss

A bit of history

Évariste Galois

- His father committed suicide.
- He was twice refused admittance to the École Polytechnique.
- He showed his work to Cauchy, Fouries, and Poisson.
  - they lost it,
  - died,
  - or did not get it.
- He was accepted to the École Normale, but was soon rejected.
- He was jailed twice.
- He died in 1832 at the age of 20 at a duel.
- The night before the duel, he collected his findings and sent them to a friend.
  - His works were published 15 years after his death.

A bit of history



Algebraic structures

Algebraic structures

So, what is algebra?

Algebraic structures

So, what is algebra?

Nowadays, algebra is defined as the **the study of algebraic structures**, which are sets of objects and a set of certain operations over such sets.

Algebraic structures

So, what is algebra?

Nowadays, algebra is defined as the **the study of algebraic structures**, which are sets of objects and a set of certain operations over such sets.

+ mix

+ chords

Algebraic structures

So, what is algebra?

Nowadays, algebra is defined as the **the study of algebraic structures**, which are sets of objects and a set of certain operations over such sets.

$+$ mix

$+$ chords

Ok, these examples are exaggerated. The point is that the content of the sets is irrelevant. This is why algebra is often known as **abstract algebra** (or modern algebra).

Algebraic structures

So, what is algebra?

Nowadays, algebra is defined as the **the study of algebraic structures**, which are sets of objects and a set of certain operations over such sets.

+ mix

+ chords

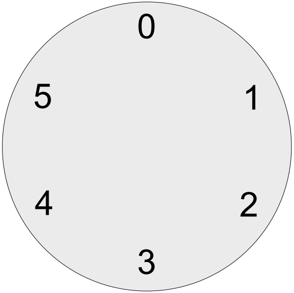
Ok, these examples are exaggerated. The point is that the content of the sets is irrelevant. This is why algebra is often known as **abstract algebra** (or modern algebra).

A list of 357 algebraic structures:
`https://math.chapman.edu/~jipsen/structures/doku.php`

Groups

Clock arithmetic

$$\langle \{0,1,2,3,4,5\}\ ,\ +\rangle$$



$1+1=$

$3+2=$

$5+2=$

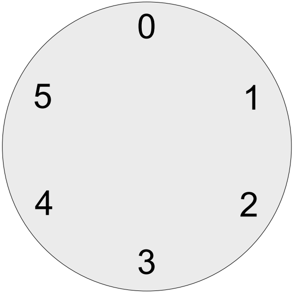
$2+4=$

$2-4=$

$2+2=$

~~Clock~~ Modular arithmetic

$$\langle \{0,1,2,3,4,5\}\ ,\ +\rangle$$



$1+1=2 \qquad 1+1 \equiv 2 (\text{mod } 6)$

$3+2=5 \qquad 3+2 \equiv 5 (\text{mod } 6)$

$5+2=1 \qquad 5+2 \equiv 1 (\text{mod } 6)$

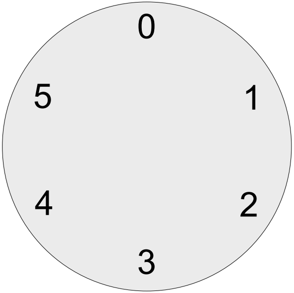
$2+4=$

$2-4=$

$2+2=$

~~Clock~~ Modular arithmetic

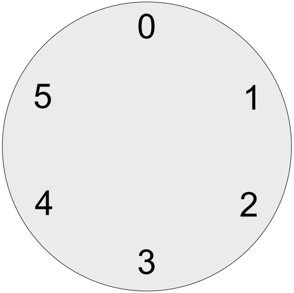
$$\langle \{0,1,2,3,4,5\}\ ,\ +\rangle$$



$$\begin{array}{ll}
1+1=2 & 1+1\equiv 2(\text{mod }6)\\
3+2=5 & 3+2\equiv 5(\text{mod }6)\\
5+2=1 & 5+2\equiv 1(\text{mod }6)\\
2+4=0 & 2+4\equiv 0(\text{mod }6)\\
2-4= & \\
2+2= &
\end{array}$$

~~Clock~~ Modular arithmetic

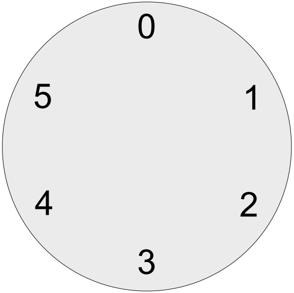
$$\langle \{0,1,2,3,4,5\}\ ,\ +\rangle$$



$$\begin{aligned}
1+1&=2 & \quad 1+1&\equiv 2 (\text{mod } 6)\\
3+2&=5 & \quad 3+2&\equiv 5 (\text{mod } 6)\\
5+2&=1 & \quad 5+2&\equiv 1 (\text{mod } 6)\\
2+4&=0 & \quad 2+4&\equiv 0 (\text{mod } 6)\\
2-4&=4 & \quad 2-4&\equiv 4 (\text{mod } 6)\\
2+2&=
\end{aligned}$$

~~Clock~~ Modular arithmetic

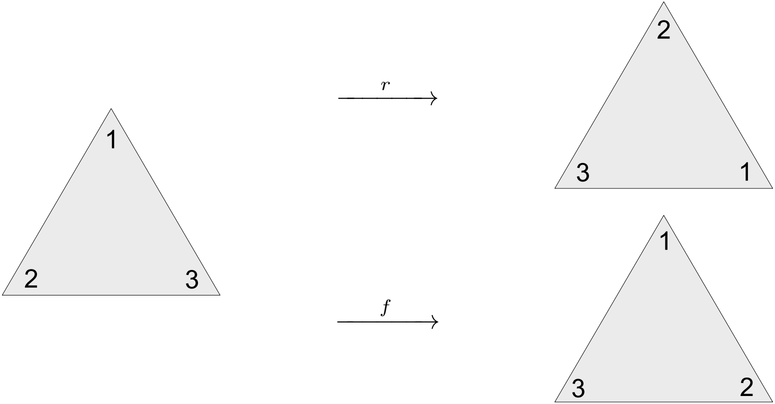
$$\langle \{0, 1, 2, 3, 4, 5\} \ , \ +\rangle$$



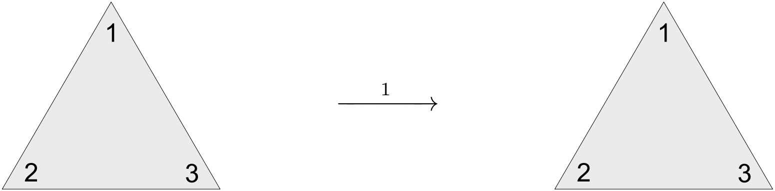
$$\begin{aligned}
1 + 1 &= 2 & 1 + 1 &\equiv 2 (\text{mod } 6)\\
3 + 2 &= 5 & 3 + 2 &\equiv 5 (\text{mod } 6)\\
5 + 2 &= 1 & 5 + 2 &\equiv 1 (\text{mod } 6)\\
2 + 4 &= 0 & 2 + 4 &\equiv 0 (\text{mod } 6)\\
2 - 4 &= 4 & 2 - 4 &\equiv 4 (\text{mod } 6)\\
2 + 2 &= 4 & 2 + 2 &\equiv 4 (\text{mod } 6)
\end{aligned}$$

Triangle symmetries

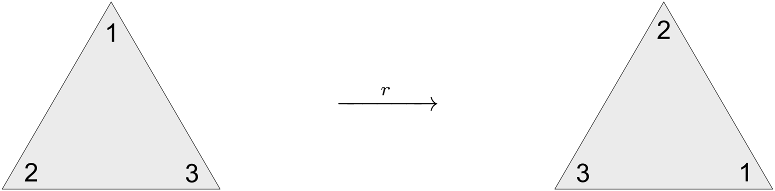
This is a symmetry problem. How many ways can you rotate or flip the triangle?



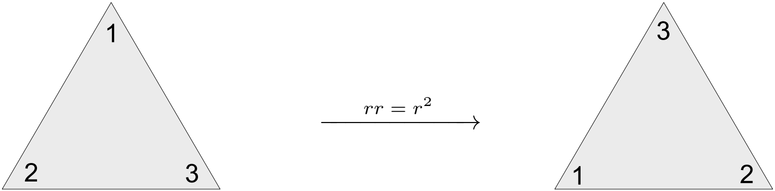
Triangle symmetries



Triangle symmetries

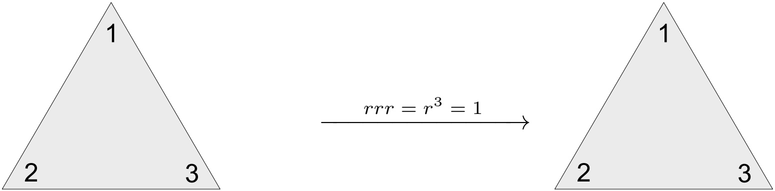


Triangle symmetries

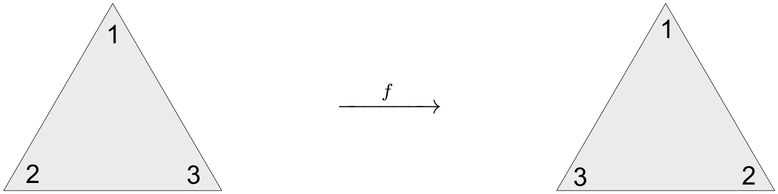


$\xrightarrow{rr = r^2}$

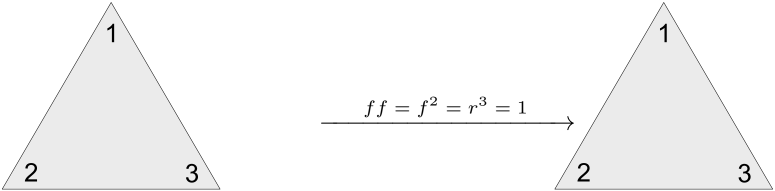
Triangle symmetries



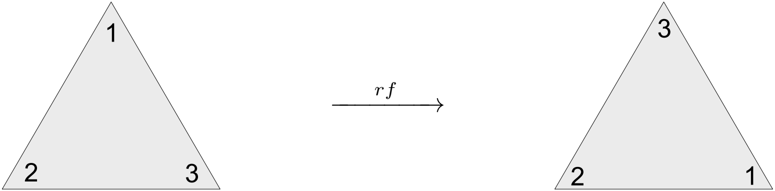
Triangle symmetries



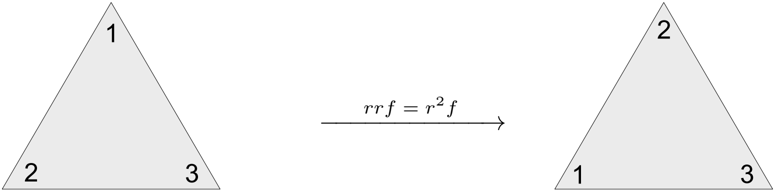
Triangle symmetries



Triangle symmetries



Triangle symmetries



~~Triangle symmetries~~ Dihedral group

In the case of a triangle, there are six symmetries.

So, the algebraic structure is

$$\langle \{1, r, r^2, f, r\cdot f, r^2\cdot f\}\ ,\ \cdot\ \rangle$$

~~Triangle symmetries~~ Dihedral group

In the case of a triangle, there are six symmetries.

So, the algebraic structure is

$$\langle \{1, r, r^2, f, r \cdot f, r^2 \cdot f\} \ , \ \cdot \ \rangle$$

Notice that,

$$\forall S \ , \ 1 \cdot S = S \ \text{ and } \ S \cdot 1 = S$$

~~Triangle symmetries~~ Dihedral group

In the case of a triangle, there are six symmetries.

So, the algebraic structure is

$$\langle \{1, r, r^2, f, r \cdot f, r^2 \cdot f\}\ ,\ \cdot\ \rangle$$

Notice that,

$$\forall S\ ,\ 1 \cdot S = S \ \text{ and } \ S \cdot 1 = S$$

and

$$\forall S\ \exists (-S)\ ,\ S \cdot (-S) = 1 \ \text{ and } \ (-S) \cdot S = 1$$

Integer sum

$$\langle \{\ldots, -3, -2, -1, 0, 1, 2, 3, \ldots\}\ ,\ +\rangle$$

This is the traditional sum operator

$$\begin{aligned} 5 + 2 &= 7 \\ 4 + (-8) &= -4 \\ 10 + (-10) &= 0 \end{aligned}$$

Integer sum

$$\langle \{\ldots,-3,-2,-1,0,1,2,3,\ldots\}\ ,\ +\rangle$$

This is the traditional sum operator

$$5+2=7$$
$$4+(-8)=-4$$
$$10+(-10)=0$$

$$5+0=5$$
$$0+(-8)=-8$$
$$x+0=0$$
$$0+x=x$$

Groups

What is common to all these examples?

🕒 $\triangle$ $\mathbb{Z}$

Groups

What is common to all these examples?

	🕒	$\triangle$	$\mathbb{Z}$
Set	$\{0,1,2,3,4,5\}$	$\{1,r,r^2,f,r\cdot f,r^2\cdot f\}$	$\mathbb{Z}$

Groups

What is common to all these examples?

	🕒	$\triangle$	$\mathbb{Z}$
Set	$\{0, 1, 2, 3, 4, 5\}$	$\{1, r, r^2, f, r \cdot f, r^2 \cdot f\}$	$\mathbb{Z}$
Operation	$+$	$\cdot$	$+$

Groups

What is common to all these examples?

	🕒	△	$\mathbb{Z}$
Set	$\{0, 1, 2, 3, 4, 5\}$	$\{1, r, r^2, f, r \cdot f, r^2 \cdot f\}$	$\mathbb{Z}$
Operation	$+$	$\cdot$	$+$
Closure	✓	✓	✓

Groups

What is common to all these examples?

	🕒	$\triangle$	$\mathbb{Z}$
Set	$\{0,1,2,3,4,5\}$	$\{1,r,r^2,f,r\cdot f,r^2\cdot f\}$	$\mathbb{Z}$
Operation	$+$	$\cdot$	$+$
Closure	$\checkmark$	$\checkmark$	$\checkmark$
Identity	0	1	0

Groups

What is common to all these examples?

	🕒	$\triangle$	$\mathbb{Z}$
Set	$\{0,1,2,3,4,5\}$	$\{1, r, r^2, f, r\cdot f, r^2\cdot f\}$	$\mathbb{Z}$
Operation	$+$	$\cdot$	$+$
Closure	$\checkmark$	$\checkmark$	$\checkmark$
Identity	0	1	0
Inverse	$x+(-x)=0$	$x\cdot(-x)=1$	$x+(-x)=0$

Groups

What is common to all these examples?

	🕒	$\triangle$	$\mathbb{Z}$
Set	$\{0,1,2,3,4,5\}$	$\{1, r, r^2, f, r\cdot f, r^2\cdot f\}$	$\mathbb{Z}$
Operation	$+$	$\cdot$	$+$
Closure	✓	✓	✓
Identity	0	1	0
Inverse	$x+(-x)=0$	$x\cdot(-x)=1$	$x+(-x)=0$
Associativity	✓	✓	✓

Groups

Definition

A **group** is an algebraic structure $\langle G, + \rangle$, such that

Groups

Definition

A **group** is an algebraic structure $\langle G, + \rangle$, such that

- G is a set of elements,

Groups

Definition

A **group** is an algebraic structure $\langle G, +\rangle$, such that

- G is a set of elements,
- $+$ is a binary operation,

Groups

Definition

A **group** is an algebraic structure $\langle G, + \rangle$, such that

- G is a set of elements,
- $+$ is a binary operation,
- $x + y = z$ (closure property),

Groups

Definition

A **group** is an algebraic structure $\langle G, +\rangle$, such that

- G is a set of elements,
- $+$ is a binary operation,
- $x + y = z$ (closure property),
- $x + (-x) = e$ (inverse),

Groups

Definition

A **group** is an algebraic structure $\langle G, +\rangle$, such that

- G is a set of elements,
- $+$ is a binary operation,
- $x + y = z$ (closure property),
- $x + (-x) = e$ (inverse),
- $y + e = e + y = y$ (identity),

Groups

Definition

A **group** is an algebraic structure $\langle G, +\rangle$, such that

- G is a set of elements,
- $+$ is a binary operation,
- $x + y = z$ (closure property),
- $x + (-x) = e$ (inverse),
- $y + e = e + y = y$ (identity),
- and $(x + y) + z = x + (y + z)$ (associativity).

Where $x, y, z, e \in G$ and e is unique.

Groups

In the dihedral group, $r \cdot f$ is different from $f \cdot r$. So, commutativity is not always a necessary property of groups.

Groups

In the dihedral group, $r \cdot f$ is different from $f \cdot r$. So, commutativity is not always a necessary property of groups.

Definition

A group with the commutative property is called a **commutative group** or an **abelian group**.

Groups

In the dihedral group, $r \cdot f$ is different from $f \cdot r$. So, commutativity is not always a necessary property of groups.

Definition

A group with the commutative property is called a **commutative group** or an **abelian group**.

Definition

$|G|$ is the **order** of the group.

Groups

Theorem

*(**Cancellation law**) If $\langle G, \, + \, \rangle$ is a group and a, b, c are elements of G, then*

$$a + b = a + c \;\; \textit{implies} \;\; b = c \;\; \textit{and}$$
$$b + a = c + a \;\; \textit{implies} \;\; b = c$$

Groups

Theorem

*(**Cancellation law**) If $\langle G, + \rangle$ is a group and a, b, c are elements of G, then*

$$a + b = a + c \ \textit{implies} \ b = c \ \textit{and}$$
$$b + a = c + a \ \textit{implies} \ b = c$$

Proof.

$$a + b = a + c$$

□

Groups

Theorem

*(**Cancellation law**) If $\langle G, + \rangle$ is a group and a, b, c are elements of G, then*

$$a + b = a + c \;\; \textit{implies} \;\; b = c \;\; \textit{and}$$
$$b + a = c + a \;\; \textit{implies} \;\; b = c$$

Proof.

$$a + b = a + c$$
$$-a + (a + b) = -a + (a + c)$$

□

Groups

Theorem

*(**Cancellation law**) If $\langle G, + \rangle$ is a group and a, b, c are elements of G, then*

$$\begin{aligned} a+b=a+c \quad &\textit{implies} \quad b=c \quad \textit{and} \\ b+a=c+a \quad &\textit{implies} \quad b=c \end{aligned}$$

Proof.

$$\begin{aligned} a+b&=a+c \\ -a+(a+b)&=-a+(a+c) \\ (-a+a)+b&=(-a+a)+c \end{aligned}$$

□

Groups

Theorem

*(**Cancellation law**) If $\langle G, + \rangle$ is a group and a, b, c are elements of G, then*

$$\begin{aligned} a+b=a+c \ \ &\textit{implies} \ \ b=c \ \ \textit{and} \\ b+a=c+a \ \ &\textit{implies} \ \ b=c \end{aligned}$$

Proof.

$$\begin{aligned} a+b&=a+c \\ -a+(a+b)&=-a+(a+c) \\ (-a+a)+b&=(-a+a)+c \\ e+b&=e+c \end{aligned}$$

□

Groups

Theorem

*(**Cancellation law**) If $\langle G, + \rangle$ is a group and a, b, c are elements of G, then*

$$a + b = a + c \quad \textit{implies} \quad b = c \quad \textit{and}$$
$$b + a = c + a \quad \textit{implies} \quad b = c$$

Proof.

$$\begin{aligned} a + b &= a + c \\ -a + (a + b) &= -a + (a + c) \\ (-a + a) + b &= (-a + a) + c \\ e + b &= e + c \\ b &= c \end{aligned}$$

□

Groups

Theorem

*(**Cancellation law**) If $\langle G, + \rangle$ is a group and a, b, c are elements of G, then*

$$a + b = a + c \text{ implies } b = c \text{ and}$$
$$b + a = c + a \text{ implies } b = c$$

Proof.

$$\begin{aligned} a + b &= a + c \\ -a + (a + b) &= -a + (a + c) \\ (-a + a) + b &= (-a + a) + c \\ e + b &= e + c \\ b &= c \end{aligned}$$

The second part is proved analogously. □

Groups

Theorem

If $\langle G, \, + \, \rangle$ *is a group and* a, b *are elements of* G, *then*

$$a + b = e \ \ \textit{implies} \ \ a = -b \ \ \textit{and} \ \ b = -a$$

Groups

Theorem

If $\langle G, \ + \ \rangle$ is a group and a, b are elements of G, then

$$a + b = e \ \ \textit{implies} \ \ a = -b \ \ \textit{and} \ \ b = -a$$

Proof.

By definition,

$$a + (-a) = e$$

□

Groups

Theorem

If $\langle G, + \rangle$ is a group and a, b are elements of G, then

$$a + b = e \quad \textit{implies} \quad a = -b \quad \textit{and} \quad b = -a$$

Proof.

By definition,

$$a + (-a) = e$$

Thus,

$$a + b = a + (-a)$$

□

Groups

Theorem

If $\langle G, + \rangle$ is a group and a, b are elements of G, then

$$a + b = e \text{ implies } a = -b \text{ and } b = -a$$

Proof.

By definition,

$$a + (-a) = e$$

Thus,

$$a + b = a + (-a)$$

By the cancellation law

$$b = -a$$

□

Groups

Theorem

If $\langle G, \ + \ \rangle$ is a group and a, b are elements of G, then

$$a + b = e \ \textit{ implies } \ a = -b \ \textit{ and } \ b = -a$$

Proof.

By definition,

$$a + (-a) = e$$

Thus,

$$a + b = a + (-a)$$

By the cancellation law

$$b = -a$$

Analogously, $a = -b$ □

Groups

Theorem

If $\langle G,\ +\ \rangle$ *is a group and* a, b *are elements of* G, *then*

$$-(a+b)=(-b)+(-a)$$

Groups

Theorem

If $\langle G, + \rangle$ *is a group and* a, b *are elements of* G, *then*

$$-(a+b) = (-b) + (-a)$$

Proof.

$$(a+b) + ((-b) + (-a)) = a + ((b + (-b)) + (-a))$$

□

Groups

Theorem

If $\langle G, \ + \ \rangle$ is a group and a, b are elements of G, then

$$-(a+b) = (-b) + (-a)$$

Proof.

$$\begin{aligned}(a+b) + ((-b) + (-a)) &= a + ((b + (-b)) + (-a)) \\ &= a + (e + (-a))\end{aligned}$$

□

Groups

Theorem

If $\langle G, + \rangle$ is a group and a, b are elements of G, then

$$-(a+b) = (-b) + (-a)$$

Proof.

$$\begin{aligned}(a+b)+((-b)+(-a)) &= a+((b+(-b))+(-a))\\ &= a+(e+(-a))\\ &= a+(-a)\end{aligned}$$

□

Groups

Theorem

If $\langle G, + \rangle$ is a group and a, b are elements of G, then

$$-(a+b) = (-b) + (-a)$$

Proof.

$$\begin{aligned}(a+b)+((-b)+(-a)) &= a+((b+(-b))+(-a)) \\ &= a+(e+(-a)) \\ &= a+(-a) \\ &= e\end{aligned}$$

□

Groups

Theorem

If $\langle G, + \rangle$ *is a group and* a, b *are elements of* G, *then*

$$-(a+b) = (-b) + (-a)$$

Proof.

$$\begin{aligned}(a+b)+((-b)+(-a)) &= a+((b+(-b))+(-a)) \\ &= a+(e+(-a)) \\ &= a+(-a) \\ &= e\end{aligned}$$

Therefore, $a+b$ is the inverse of $(-b)+(-a)$ and, by the previous theorem

$$(-b)+(-a) = -(a+b)$$

□

Groups

Theorem

If $\langle G, \ + \ \rangle$ *is a group and* a, b *are elements of* G, *then*

$$-(-a) = a$$

Groups

Theorem

If $\langle G, + \rangle$ is a group and a, b are elements of G, then

$$-(-a) = a$$

Proof.

$$a + (-a) = e$$

□

Groups

Theorem

If $\langle G, \ + \ \rangle$ is a group and a, b are elements of G, then

$$-(-a) = a$$

Proof.

$$a + (-a) = e$$

By one of the previous theorems,

$$a = -(-a)$$

□

Cayley tables

$$\langle \{1, -1, i, -i\}, \ \times \ \rangle$$

$\times$	1	-1	i	$-i$
1	1	-1	i	$-i$
-1	-1	1	$-i$	i
i	i	$-i$	-1	1
$-i$	$-i$	i	1	-1

Cayley tables

$$\langle \{1, -1, i, -i\}, \ \times \ \rangle$$

$\times$	1	-1	i	$-i$
1	1	-1	i	$-i$
-1	-1	1	$-i$	i
i	i	$-i$	-1	1
$-i$	$-i$	i	1	-1

Observation

The first row and column are identical to the headers (assuming the first listed element is the identity element).

Cayley tables

$$\langle \{1, -1, i, -i\},\ \times\ \rangle$$

$\times$	1	-1	i	$-i$
1	1	-1	i	$-i$
-1	-1	1	$-i$	i
i	i	$-i$	-1	1
$-i$	$-i$	i	1	-1

Theorem

Each row and column has the identity element.

Cayley tables

$$\langle \{1, -1, i, -i\}, \ \times \ \rangle$$

$\times$	1	-1	i	$-i$
1	1	-1	i	$-i$
-1	-1	1	$-i$	i
i	i	$-i$	-1	1
$-i$	$-i$	i	1	-1

Theorem

Each row and column has the identity element.

Proof.

Because each element has an inverse. □

Cayley tables

$$\langle \{1, -1, i, -i\},\ \times\ \rangle$$

$\times$	1	-1	i	$-i$
1	1	-1	i	$-i$
-1	-1	1	$-i$	i
i	i	$-i$	-1	1
$-i$	$-i$	i	1	-1

Observation

This table is symmetric about diagonal.

Cayley tables

$$\langle \{1, -1, i, -i\}, \ \times \ \rangle$$

$\times$	1	-1	i	$-i$
1	1	-1	i	$-i$
-1	-1	1	$-i$	i
i	i	$-i$	-1	1
$-i$	$-i$	i	1	-1

Observation

This table is symmetric about diagonal.

Observation

Since the operation is commutative, the group is abelian.

Cayley tables

$$\langle \{1, -1, i, -i\}, \ \times \ \rangle$$

$\times$	1	-1	i	$-i$
1	1	-1	i	$-i$
-1	-1	1	$-i$	i
i	i	$-i$	-1	1
$-i$	$-i$	i	1	-1

Observation

Notice that each element appears once in each row and column.

Cayley tables

Theorem

Each element appears once in each row and column.

Cayley tables

Theorem

Each element appears once in each row and column.

$\times$	g_1	g_2	x	g_4	y	g_6	$\cdots$
g_1	-	-	-	-	-	-	-
g_2	-	-	-	-	-	-	-
a	-	-	z	-	z	-	-
g_4	-	-	-	-	-	-	-
g_5	-	-	-	-	-	-	-
g_6	-	-	-	-	-	-	-
$\vdots$	-	-	-	-	-	-	-

Proof.

Assume that

$$a \times x = a \times y$$

□

Cayley tables

Theorem

Each element appears once in each row and column.

$\times$	g_1	g_2	x	g_4	y	g_6	$\cdots$
g_1	-	-	-	-	-	-	-
g_2	-	-	-	-	-	-	-
a	-	-	z	-	z	-	-
g_4	-	-	-	-	-	-	-
g_5	-	-	-	-	-	-	-
g_6	-	-	-	-	-	-	-
$\vdots$	-	-	-	-	-	-	-

Proof.

Assume that

$$a \times x = a \times y$$
$$(-a) \times (a \times x) = (-a) \times (a \times y)$$

□

Cayley tables

Theorem

Each element appears once in each row and column.

$\times$	g_1	g_2	x	g_4	y	g_6	$\cdots$
g_1	-	-	-	-	-	-	-
g_2	-	-	-	-	-	-	-
a	-	-	z	-	z	-	-
g_4	-	-	-	-	-	-	-
g_5	-	-	-	-	-	-	-
g_6	-	-	-	-	-	-	-
$\vdots$	-	-	-	-	-	-	-

Proof.

Assume that

$$a \times x = a \times y$$
$$(-a) \times (a \times x) = (-a) \times (a \times y)$$
$$(-a \times a) \times x = (-a \times a) \times y$$

□

Cayley tables

Theorem

Each element appears once in each row and column.

$\times$	g_1	g_2	x	g_4	y	g_6	$\cdots$
g_1	-	-	-	-	-	-	-
g_2	-	-	-	-	-	-	-
a	-	-	z	-	z	-	-
g_4	-	-	-	-	-	-	-
g_5	-	-	-	-	-	-	-
g_6	-	-	-	-	-	-	-
$\vdots$	-	-	-	-	-	-	-

Proof.

Assume that

$$a \times x = a \times y$$

$$(-a) \times (a \times x) = (-a) \times (a \times y)$$

$$(-a \times a) \times x = (-a \times a) \times y$$

$$e \times x = e \times y$$

□

Cayley tables

Theorem

Each element appears once in each row and column.

$\times$	g_1	g_2	x	g_4	y	g_6	$\cdots$
g_1	-	-	-	-	-	-	-
g_2	-	-	-	-	-	-	-
a	-	-	z	-	z	-	-
g_4	-	-	-	-	-	-	-
g_5	-	-	-	-	-	-	-
g_6	-	-	-	-	-	-	-
$\vdots$	-	-	-	-	-	-	-

Proof.

Assume that

$$\begin{aligned} a \times x &= a \times y \\ (-a) \times (a \times x) &= (-a) \times (a \times y) \\ (-a \times a) \times x &= (-a \times a) \times y \\ e \times x &= e \times y \\ x &= y \end{aligned}$$

□

Cayley tables

Theorem

Each element appears once in each row and column.

$\times$	g_1	g_2	x	g_4	y	g_6	$\cdots$
g_1	-	-	-	-	-	-	-
g_2	-	-	-	-	-	-	-
a	-	-	z	-	z	-	-
g_4	-	-	-	-	-	-	-
g_5	-	-	-	-	-	-	-
g_6	-	-	-	-	-	-	-
$\vdots$	-	-	-	-	-	-	-

Proof.

Assume that

$$
\begin{aligned}
a \times x &= a \times y \\
(-a) \times (a \times x) &= (-a) \times (a \times y) \\
(-a \times a) \times x &= (-a \times a) \times y \\
e \times x &= e \times y \\
x &= y
\end{aligned}
$$

This contradicts our initial assumption. Thus, there is only one z at each row and column. □

Groups of order 1

+	

Groups of order 1

$+$	e
e	e

Trivial group

$$\langle \{e\},\ +\ \rangle$$

$$|G| = 1$$

Groups of order 2

+		

Groups of order 2

$+$	e	a
e	e	a
a	a	e

$$\langle \{e, a\},\ +\ \rangle$$

$$|G| = 2$$

Groups of order 3

+			

Groups of order 3

$+$	e	a	b
e	e	a	b
a	a	b	e
b	b	e	a

$$\langle \{e, a, b\},\ +\ \rangle$$

$$|G| = 3$$

Groups of order 4

$+$	e	a	b	c
e	e	a	b	c
a	a			
b	b			
c	c			

$+$	e	a	b	c
e	e	a	b	c
a	a			
b	b			
c	c			

Groups of order 4

$+$	e	a	b	c
e	e	a	b	c
a	a			
b	b			
c	c			

$+$	e	a	b	c
e	e	a	b	c
a	a			
b	b			
c	c			

Can you think of more groups of order 4?

Groups of order 4

$+$	e	a	b	c
e	e	a	b	c
a	a	c	e	b
b	b	e	c	a
c	c	b	a	e

$+$	e	a	b	c
e	e	a	b	c
a	a	b	c	e
b	b	c	e	a
c	c	e	a	b

Groups of order 4

$+$	e	a	b	c
e	e	a	b	c
a	a	c	e	b
b	b	e	c	a
c	c	b	a	e

$+$	e	a	b	c
e	e	a	b	c
a	a	b	c	e
b	b	c	e	a
c	c	e	a	b

Are these two groups different?

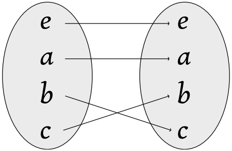
Groups of order 4

$+$	e	a	b	c
e	e	a	b	c
a	a	c	e	b
b	b	e	c	a
c	c	b	a	e

$+$	e	a	b	c
e	e	a	b	c
a	a	b	c	e
b	b	c	e	a
c	c	e	a	b

Are these two groups different?

Check this mapping:



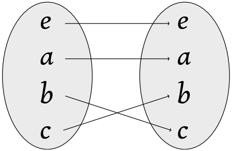
Groups of order 4

$+$	e	a	b	c
e	e	a	b	c
a	a	c	e	b
b	b	e	c	a
c	c	b	a	e

$+$	e	a	c	b
e	e	a	c	b
a	a	b	e	c
c	c	e	b	a
b	b	c	a	e

Are these two groups different?

Check this mapping:



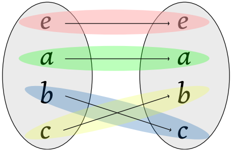
Groups of order 4

$+$	e	a	b	c
e	e	a	b	c
a	a	c	e	b
b	b	e	c	a
c	c	b	a	e

$+$	e	a	c	b
e	e	a	c	b
a	a	b	e	c
c	c	e	b	a
b	b	c	a	e

Are these two groups different?

Check this mapping:



Subgroups

Definition

Assume $\langle G, * \rangle$ is a group. $\langle H, * \rangle$ is a **subgroup** of $\langle G, * \rangle$ if

- $\langle H, * \rangle$ is a group and
- $H \subseteq G$.

This relationship is denoted by $\langle H, * \rangle \leq \langle G, * \rangle$ or just $H \leq G$. Notice that $G \leq G$

Homomorphism

Definition

A function from one algebraic structure to another that preserves the structure is called a **homomorphism** (*of the same form*).

In terms of groups, a function $\phi : G \to H$ is a homomorphism if

$$\phi(x * y) = \phi(x) \circ \phi(y)$$

where $\langle G,\ *\rangle$ and $\langle H,\ \circ\rangle$ are groups and $x, y \in G$.

Homomorphism

$$\langle \{\ldots, -3, -2, -1, 0, 1, 2, 3, \ldots\}\ ,\ +\rangle$$

$$\mathbb{Z} = \{even\} \cup \{odd\}$$

$$\begin{aligned} even + even &= even \\ even + odd &= odd \\ odd + even &= odd \\ odd + odd &= even \end{aligned}$$

$$\langle \{0, 1\}\ ,\ +\rangle$$

$$\begin{aligned} 0 + 0 &\equiv 0 (\text{mod } 2) \\ 0 + 1 &\equiv 1 (\text{mod } 2) \\ 1 + 0 &\equiv 1 (\text{mod } 2) \\ 1 + 1 &\equiv 0 (\text{mod } 2) \end{aligned}$$

Homomorphism

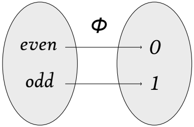
$$\langle \{\dots, -3, -2, -1, 0, 1, 2, 3, \dots\} \;,\; + \rangle$$

$$\langle \{0, 1\} \;,\; + \rangle$$

$$\mathbb{Z} = \{even\} \cup \{odd\}$$

$$\begin{aligned} even + even &= even \\ even + odd &= odd \\ odd + even &= odd \\ odd + odd &= even \end{aligned}$$

$$\begin{aligned} 0 + 0 &\equiv 0 (\text{mod } 2) \\ 0 + 1 &\equiv 1 (\text{mod } 2) \\ 1 + 0 &\equiv 1 (\text{mod } 2) \\ 1 + 1 &\equiv 0 (\text{mod } 2) \end{aligned}$$



Homomorphism

$\langle G, \ast \rangle$

$\ast$	—	—	y	—	—
—	—	—	—	—	—
—	—	—	—	—	—
—	—	—	—	—	—
x	—	—	$x \ast y$	—	—
—	—	—	—	—	—

$\langle H, \circ \rangle$

$\circ$	—	—	$\phi(y)$	—	—
—	—	—	—	—	—
—	—	—	—	—	—
—	—	—	—	—	—
$\phi(x)$	—	—	$\phi(x) \circ \phi(y)$	—	—
—	—	—	—	—	—

$$\phi : G \to H$$

$$\phi(x \ast y) = \phi(x) \circ \phi(y)$$

Homomorphism

Given the group $\langle \mathbb{Z} \ , \ + \rangle$ and $\phi : \mathbb{Z} \to \mathbb{Z}$.

Is $\phi(x) = 2x$ a homomorphism?

Homomorphism

Given the group $\langle \mathbb{Z} \ , \ + \rangle$ and $\phi : \mathbb{Z} \to \mathbb{Z}$.

Is $\phi(x) = 2x$ a homomorphism?

Is

$$\phi(x+y) = \phi(x) + \phi(y) \quad ?$$

Homomorphism

Given the group $\langle \mathbb{Z} \ , \ + \rangle$ and $\phi : \mathbb{Z} \rightarrow \mathbb{Z}$.

Is $\phi(x) = 2x$ a homomorphism?

Is

$$\phi(x+y) = \phi(x) + \phi(y) \quad ?$$

Namely, is

$$2(x+y) = 2x + 2y \quad ?$$

Isomorphism

Definition

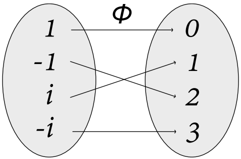
A bijective homomorphism is called a **isomorphism**.

Isomorphism

$$\langle \{1, -1, i, -i\}\ ,\ \times \rangle \qquad \langle \{0, 1, 2, 3\}\ ,\ + \rangle$$

$\times$	1	-1	i	$-i$
1	1	-1	i	$-i$
-1	-1	1	$-i$	i
i	i	$-i$	-1	1
$-i$	$-i$	i	1	-1

$+$	0	1	2	3
0	0	1	2	3
1	1	2	3	0
2	2	3	0	1
3	3	0	1	2



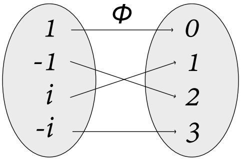
Isomorphism

$\langle \{1, -1, i, -i\}\ ,\ \times \rangle$

$\times$	1	-1	i	$-i$
1	1	-1	i	$-i$
-1	-1	1	$-i$	i
i	i	$-i$	-1	1
$-i$	$-i$	i	1	-1

$\langle \{0, 1, 2, 3\}\ ,\ + \rangle$

$+$	0	2	1	3
0	0	2	1	3
2	2	0	3	1
1	1	3	2	0
3	3	1	0	2



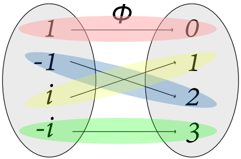
Isomorphism

$\langle \{1, -1, i, -i\} \ , \ \times \rangle$

$\times$	1	-1	i	$-i$
1	1	-1	i	$-i$
-1	-1	1	$-i$	i
i	i	$-i$	-1	1
$-i$	$-i$	i	1	-1

$\langle \{0, 1, 2, 3\} \ , \ + \rangle$

$+$	0	2	1	3
0	0	2	1	3
2	2	0	3	1
1	1	3	2	0
3	3	1	0	2



Automorphism

Definition

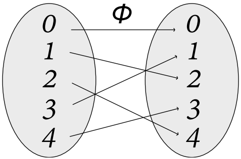
An isomorphism from one group to itself is called an **automorphism**.

Automorphism

$$\langle\{0,1,2,3,4\}\ ,\ +\rangle \qquad \langle\{0,1,2,3,4\}\ ,\ +\rangle$$

+	0	1	2	3	4
0	0	1	2	3	4
1	1	2	3	4	0
2	2	3	4	0	1
3	3	4	0	1	2
4	4	0	1	2	3

+	0	2	4	1	3
0	0	2	4	1	3
2	2	4	1	3	0
4	4	1	3	0	2
1	1	3	0	2	4
3	3	0	2	4	1



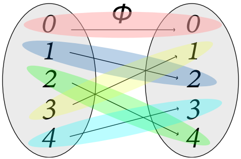
Automorphism

$\langle\{0,1,2,3,4\}\ ,\ +\rangle$

$+$	0	1	2	3	4
0	0	1	2	3	4
1	1	2	3	4	0
2	2	3	4	0	1
3	3	4	0	1	2
4	4	0	1	2	3

$\langle\{0,1,2,3,4\}\ ,\ +\rangle$

$+$	0	2	4	1	3
0	0	2	4	1	3
2	2	4	1	3	0
4	4	1	3	0	2
1	1	3	0	2	4
3	3	0	2	4	1



Rings

Rings

Definition

A **ring** is an algebraic structure $\langle G\ ,\ +\ ,\ \times\rangle$ such that

- addition $(+)$ is associative and commutative,
- multiplication $(\times)$ is associative

$$(a \times b) \times c = a \times (b \times c)$$

- multiplication is distributive over addition

$$\begin{aligned} a \times (b + c) &= (a \times b) + (a \times c) \\ (b + c) \times a &= (b \times a) + (c \times a) \end{aligned}$$

- there are inverses for addition,
- multiplication and addition have an identity.

Rings

Definition

A **ring** $\langle G \ , \ + \ , \ \times \rangle$ is an abelian group with an extra operation $\times$.

Multiplication is

- associative and
- has an identity element.

Notice that multiplication does not require

- inverses and
- commutativity.

Besides, multiplication is distributive over addition

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

Rings

The easiest examples of rings are the traditional number systems. The set $\mathbb{Z}$ of the integers, with conventional addition and multiplication, is a ring called the **ring of integers**. We designate this ring simply with the letter $\mathbb{Z}$. The context will make clear whether we are referring to the ring of the integers or the additive group of the integers.

Rings

The easiest examples of rings are the traditional number systems. The set $\mathbb{Z}$ of the integers, with conventional addition and multiplication, is a ring called the **ring of integers**. We designate this ring simply with the letter $\mathbb{Z}$. The context will make clear whether we are referring to the ring of the integers or the additive group of the integers.

Similarly, $\mathbb{Q}$ is the ring of the rational numbers, $\mathbb{R}$ is the ring of the real numbers, and $\mathbb{C}$ the ring of the complex numbers. In each case, the operations are conventional addition and multiplication.

Rings

Let $\langle A, \ + \ , \ \times \rangle$ be any ring (it can also be denoted just by A). Since A under addition is an abelian group

Rings

Let $\langle A, \ + \ , \ \times\rangle$ be any ring (it can also be denoted just by A). Since A under addition is an abelian group

$$a+b=a+c \quad \text{implies} \quad b=c$$

Rings

Let $\langle A, \ + \ , \ \times \rangle$ be any ring (it can also be denoted just by A). Since A under addition is an abelian group

$$a + b = a + c \quad \text{implies} \quad b = c$$

$$a + b = 0 \quad \text{implies} \quad a = -b \ \text{ and } \ b = -a$$

Rings

Let $\langle A, \ + \ , \ \times \rangle$ be any ring (it can also be denoted just by A). Since A under addition is an abelian group

$$a + b = a + c \quad \text{implies} \quad b = c$$

$$a + b = 0 \quad \text{implies} \quad a = -b \;\; \text{and} \;\; b = -a$$

$$-(a + b) = (-a) + (-b) = (-b) + (-a)$$

Rings

Let $\langle A, \ + \ , \ \times \rangle$ be any ring (it can also be denoted just by A). Since A under addition is an abelian group

$$a + b = a + c \quad \text{implies} \quad b = c$$

$$a + b = 0 \quad \text{implies} \quad a = -b \;\; \text{and} \;\; b = -a$$

$$-(a + b) = (-a) + (-b) = (-b) + (-a)$$

$$-(-a) = a$$

Rings

Let $\langle A, + , \times\rangle$ be any ring (it can also be denoted just by A). Since A under addition is an abelian group

$$a + b = a + c \quad \text{implies} \quad b = c$$

$$a + b = 0 \quad \text{implies} \quad a = -b \;\; \text{and} \;\; b = -a$$

$$-(a + b) = (-a) + (-b) = (-b) + (-a)$$

$$-(-a) = a$$

What happens in a ring when we multiply elements by zero or by inverses?

Rings

Theorem

Let a and b be any elements of a ring $\langle A\ ,\ +\ ,\ \times\rangle$.

$$a \times 0 = 0 \quad \textit{and} \quad 0 \times a = 0$$

Rings

Theorem

Let a and b be any elements of a ring $\langle A\ ,\ +\ ,\ \times\rangle$.

$$a \times 0 = 0 \ \ \textit{and} \ \ 0 \times a = 0$$

Proof.

$$(a \times a) + 0 = (a \times a)$$

□

Rings

Theorem

Let a and b be any elements of a ring $\langle A\ ,\ +\ ,\ \times\rangle$.

$$a \times 0 = 0 \quad \textit{and} \quad 0 \times a = 0$$

Proof.

$$\begin{aligned}(a \times a) + 0 &= (a \times a)\\ &= a \times (a + 0)\end{aligned}$$

□

Rings

Theorem

Let a and b be any elements of a ring $\langle A\ ,\ +\ ,\ \times\rangle$.

$$a \times 0 = 0 \ \ \textit{and} \ \ 0 \times a = 0$$

Proof.

$$\begin{aligned}(a \times a) + 0 &= (a \times a)\\ &= a \times (a + 0)\\ &= (a \times a) + (a \times 0)\end{aligned}$$

□

Rings

Theorem

Let a and b be any elements of a ring $\langle A\ ,\ +\ ,\ \times \rangle$.

$$a \times 0 = 0 \ \ \textit{and} \ \ 0 \times a = 0$$

Proof.

$$\begin{aligned}(a \times a) + 0 &= (a \times a)\\ &= a \times (a + 0)\\ &= (a \times a) + (a \times 0)\end{aligned}$$

By the cancellation law,

$$0 = a \times 0$$

□

Rings

Theorem

Let a and b be any elements of a ring $\langle A\ ,\ +\ ,\ \times\rangle$.

$$a \times 0 = 0 \ \ \textit{and} \ \ 0 \times a = 0$$

Proof.

$$\begin{aligned}(a \times a) + 0 &= (a \times a) \\ &= a \times (a + 0) \\ &= (a \times a) + (a \times 0)\end{aligned}$$

By the cancellation law,

$$0 = a \times 0$$

The second part is proved analogously. □

Rings

Theorem

Let a and b be any elements of a ring $\langle A\ ,\ +\ ,\ \times\rangle$.

$$a \times (-b) = -(a \times b) \ \ \textit{and} \ \ (-a) \times b = -(a \times b)$$

Rings

Theorem

Let a and b be any elements of a ring $\langle A\ ,\ +\ ,\ \times\rangle$.

$$a \times (-b) = -(a \times b) \;\; \textit{and} \;\; (-a) \times b = -(a \times b)$$

Proof.

$$(a \times (-b)) + (a \times b) = a \times ((-b) + b)$$

□

Rings

Theorem

Let a and b be any elements of a ring $\langle A\ ,\ +\ ,\ \times\rangle$.

$$a \times (-b) = -(a \times b) \ \ \textit{and} \ \ (-a) \times b = -(a \times b)$$

Proof.

$$\begin{aligned}(a \times (-b)) + (a \times b) &= a \times ((-b) + b)\\ &= a \times 0\end{aligned}$$

□

Rings

Theorem

Let a and b be any elements of a ring $\langle A\ ,\ +\ ,\ \times\rangle$.

$$a \times (-b) = -(a \times b) \ \text{ and } \ (-a) \times b = -(a \times b)$$

Proof.

$$\begin{aligned}(a \times (-b)) + (a \times b) &= a \times ((-b) + b)\\ &= a \times 0\\ &= 0\end{aligned}$$

□

Rings

Theorem

Let a and b be any elements of a ring $\langle A\ ,\ +\ ,\ \times\rangle$.

$$a \times (-b) = -(a \times b) \ \ \textit{and} \ \ (-a) \times b = -(a \times b)$$

Proof.

$$\begin{aligned}(a \times (-b)) + (a \times b) &= a \times ((-b) + b)\\ &= a \times 0\\ &= 0\end{aligned}$$

By one of the previous theorems on groups,

$$a \times (-b) = -(a \times b)$$

□

Rings

Theorem

Let a and b be any elements of a ring $\langle A\ ,\ +\ ,\ \times\rangle$.

$$a \times (-b) = -(a \times b) \ \ \textit{and} \ \ (-a) \times b = -(a \times b)$$

Proof.

$$\begin{aligned}(a \times (-b)) + (a \times b) &= a \times ((-b) + b)\\ &= a \times 0\\ &= 0\end{aligned}$$

By one of the previous theorems on groups,

$$a \times (-b) = -(a \times b)$$

The second part is proved analogously. □

Rings

Theorem

Let a and b be any elements of a ring $\langle A\ ,\ +\ ,\ \times\rangle$.

$$(-a) \times (-b) = a \times b$$

Rings

Theorem

Let a and b be any elements of a ring $\langle A\ ,\ +\ ,\ \times\rangle$.

$$(-a)\times(-b)=a\times b$$

Proof.

We apply the previous theorem twice

$$(-a)\times(-b)=-(a\times(-b))=-(-(a\times b))=a\times b$$

□

Rings

Rings with extra features:

Rings

Rings with extra features:

- **Commutative rings**. Multiplication is commutative.

Rings

Rings with extra features:

- **Commutative rings**. Multiplication is commutative.
- **Division rings**. There are inverses under multiplication (except for 0).

Rings

Rings with extra features:

- **Commutative rings**. Multiplication is commutative.
- **Division rings**. There are inverses under multiplication (except for 0).
- **Commutative division rings**. Multiplication is commutative, and there are inverses under multiplication (except for 0).

Fields

Fields

Definition

A **field** $\langle A\ ,\ +\ ,\ \times\rangle$ is a commutative division ring.

Fields

Definition

A **field** $\langle A \ , \ + \ , \ \times \rangle$ is a commutative division ring.

Well-known fields are $\mathbb{Q}$, $\mathbb{R}$, and $\mathbb{C}$.

Fields

Loosely speaking

Group	Ring	Field
$+ \quad -$	$+ \quad - \quad \times$	$+ \quad - \quad \times \quad \div$

Vector spaces

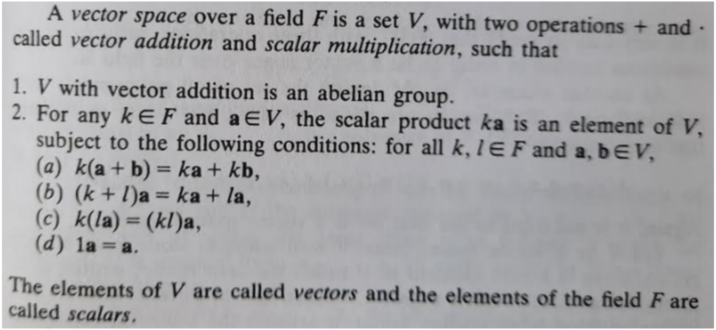
Vector spaces

Definition

$\langle V, F, \ + \ , \ \times \ \rangle$ is called a **vector space** if

- $\langle V, \ + \ \rangle$ is an abelian group. The elements of V are known as **vectors**.
- $\langle F, \ + \ , \ \times \rangle$ is a field. The elements of F are known as **scalars**.
- $f \times \mathbf{v} \in V$, for all $\mathbf{v} \in V$ and $f \in F$ (scalar multiple).
- $f \times (\mathbf{v} + \mathbf{w}) = (f \times \mathbf{v}) + (f \times \mathbf{w})$, for all $f \in F$ and $\mathbf{v}, \mathbf{w} \in V$ (distributivity).
- $(f + g) \times \mathbf{v} = (f \times \mathbf{v}) + (g \times \mathbf{v})$, for all $f \in F$ and $\mathbf{v}, \mathbf{w} \in V$ (distributivity).
- $f \times (g \times \mathbf{v}) = (f \times g) \times \mathbf{v}$, for all $f, g \in F$ and $\mathbf{v} \in V$.
- $1 \times \mathbf{v} = \mathbf{v}$ (scalar identity).

Vectors spaces



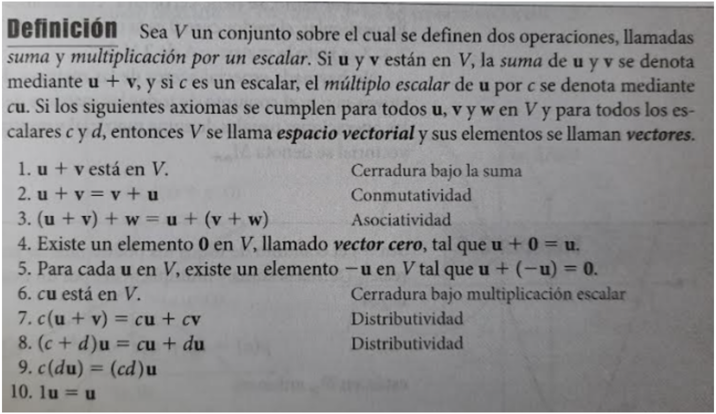
A *vector space* over a field F is a set V, with two operations $+$ and $\cdot$ called *vector addition* and *scalar multiplication*, such that

1. V with vector addition is an abelian group.
2. For any $k \in F$ and $\mathbf{a} \in V$, the scalar product $k\mathbf{a}$ is an element of V, subject to the following conditions: for all $k, l \in F$ and $\mathbf{a}, \mathbf{b} \in V$,
   (*a*) $k(\mathbf{a} + \mathbf{b}) = k\mathbf{a} + k\mathbf{b}$,
   (*b*) $(k + l)\mathbf{a} = k\mathbf{a} + l\mathbf{a}$,
   (*c*) $k(l\mathbf{a}) = (kl)\mathbf{a}$,
   (*d*) $1\mathbf{a} = \mathbf{a}$.

The elements of V are called *vectors* and the elements of the field F are called *scalars*.

A book of abstract algebra, Charles C. Pinter

Vectors spaces

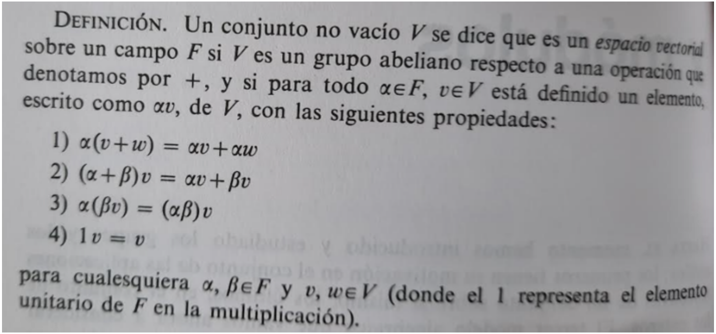


Definición Sea V un conjunto sobre el cual se definen dos operaciones, llamadas *suma* y *multiplicación por un escalar*. Si $\mathbf{u}$ y $\mathbf{v}$ están en V, la *suma* de $\mathbf{u}$ y $\mathbf{v}$ se denota mediante $\mathbf{u} + \mathbf{v}$, y si c es un escalar, el *múltiplo escalar* de $\mathbf{u}$ por c se denota mediante $c\mathbf{u}$. Si los siguientes axiomas se cumplen para todos $\mathbf{u}$, $\mathbf{v}$ y $\mathbf{w}$ en V y para todos los escalares c y d, entonces V se llama ***espacio vectorial*** y sus elementos se llaman ***vectores***.

1. $\mathbf{u} + \mathbf{v}$ está en V. Cerradura bajo la suma
2. $\mathbf{u} + \mathbf{v} = \mathbf{v} + \mathbf{u}$ Conmutatividad
3. $(\mathbf{u} + \mathbf{v}) + \mathbf{w} = \mathbf{u} + (\mathbf{v} + \mathbf{w})$ Asociatividad
4. Existe un elemento $\mathbf{0}$ en V, llamado ***vector cero***, tal que $\mathbf{u} + \mathbf{0} = \mathbf{u}$.
5. Para cada $\mathbf{u}$ en V, existe un elemento $-\mathbf{u}$ en V tal que $\mathbf{u} + (-\mathbf{u}) = \mathbf{0}$.
6. $c\mathbf{u}$ está en V. Cerradura bajo multiplicación escalar
7. $c(\mathbf{u} + \mathbf{v}) = c\mathbf{u} + c\mathbf{v}$ Distributividad
8. $(c + d)\mathbf{u} = c\mathbf{u} + d\mathbf{u}$ Distributividad
9. $c(d\mathbf{u}) = (cd)\mathbf{u}$
10. $1\mathbf{u} = \mathbf{u}$

Álgebra lineal, una introducción moderna, David Poole

Vectors spaces



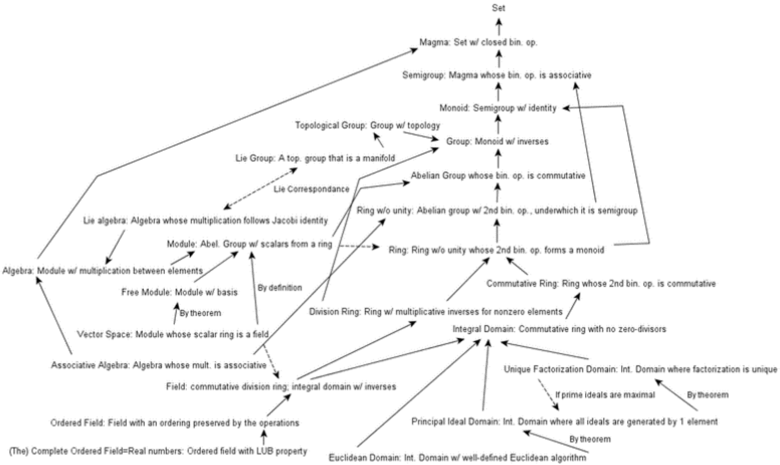
Definición. Un conjunto no vacío V se dice que es un *espacio vectorial* sobre un campo F si V es un grupo abeliano respecto a una operación que denotamos por $+$, y si para todo $\alpha \in F$, $v \in V$ está definido un elemento, escrito como αv, de V, con las siguientes propiedades:

1) $\alpha(v+w) = \alpha v + \alpha w$
2) $(\alpha+\beta)v = \alpha v + \beta v$
3) $\alpha(\beta v) = (\alpha\beta)v$
4) $1v = v$

para cualesquiera $\alpha, \beta \in F$ y $v, w \in V$ (donde el 1 representa el elemento unitario de F en la multiplicación).

Álgebra moderna, N. Herstein

Relationship between algebraic structures


Set
Magma: Set w/ closed bin. op.
Semigroup: Magma whose bin. op. is associative
Monoid: Semigroup w/ identity
Topological Group: Group w/ topology
Group: Monoid w/ inverses
Lie Group: A top. group that is a manifold
Abelian Group whose bin. op. is commutative
Lie Correspondance
Ring w/o unity: Abelian group w/ 2nd bin. op., underwhich it is semigroup
Lie algebra: Algebra whose multiplication follows Jacobi identity
Module: Abel. Group w/ scalars from a ring
Ring: Ring w/o unity whose 2nd bin. op. forms a monoid
Algebra: Module w/ multiplication between elements
Free Module: Module w/ basis
By definition
Commutative Ring: Ring whose 2nd bin. op. is commutative
By theorem
Division Ring: Ring w/ multiplicative inverses for nonzero elements
Integral Domain: Commutative ring with no zero-divisors
Vector Space: Module whose scalar ring is a field
Associative Algebra: Algebra whose mult. is associative
Unique Factorization Domain: Int. Domain where factorization is unique
Field: commutative division ring; integral domain w/ inverses
If prime ideals are maximal
By theorem
Ordered Field: Field with an ordering preserved by the operations
Principal Ideal Domain: Int. Domain where all ideals are generated by 1 element
By theorem
(The) Complete Ordered Field=Real numbers: Ordered field with LUB property
Euclidean Domain: Int. Domain w/ well-defined Euclidean algorithm

http://commons.wikimedia.org/wiki/File:Algebraic_structures.png

Ending

Summary

Homework

- What is a
  - set,
  - magma,
  - semigroup,
  - monoid,
  - group,
  - ring,
  - field,
  - vector space,
  - module,
  - algebra,
  - lattice.
- There is only one group G of order 4 where $x + x = e$ for all $x \in G$. Find its Cayley table.
- Find all the groups of order 4 (remove automorphisms). Use Cayley tables.

Homework

- Let $\mathscr{M}_2(\mathbb{R})$ designate the set of all 2×2 matrices
$$\begin{bmatrix} a & b \\ c & d \end{bmatrix}$$
whose entries are real numbers a, b, c, and d with the following addition and multiplication
$$\begin{bmatrix} a & b \\ c & d \end{bmatrix} + \begin{bmatrix} r & s \\ t & u \end{bmatrix} = \begin{bmatrix} a+r & b+s \\ c+t & d+u \end{bmatrix}$$
$$\begin{bmatrix} a & b \\ c & d \end{bmatrix} \begin{bmatrix} r & s \\ t & u \end{bmatrix} = \begin{bmatrix} ar+bt & as+bu \\ cr+dt & cs+du \end{bmatrix}$$
    - Verify that $\mathscr{M}_2(\mathbb{R})$ is a ring.
    - What are the identity elements of $\mathscr{M}_2(\mathbb{R})$.
    - Show that $\mathscr{M}_2(\mathbb{R})$ is not commutative.
    - Is $\mathscr{M}_2(\mathbb{R})$ a field?

Thank you