Lecture 6
Algebraic Structures II
Analysis of Home Exercises

1. Consider a following mathematical structure and find out if it is
an algebraic structure?
   a semigroup?
   a monoid?
   a group?
   an Abelian group?

   a) Carrier set: set of rational numbers
      Operation: multiplication

   b) Carrier set: set of continuous functions defined over [0, 1]
      Operation: adding
Classification of Algebras

Algebraic structure: Carrier set + operation; closed with respect to the operation
Semigroup: Algebraic structure with associative binary operation
Monoid: Semigroup with an identity element
Group: Monoid with a unary inversion operator
Abelian group: Group with commutative binary operation
Lattice: Abelian group with two binary operations and distributivity property for both operations.

a) Carrier set: set of rational numbers
   Operation: multiplication

b) Carrier set: set of continuous functions defined over [0, 1]
   Operation: adding

Solution:
Are these mathematical structures algebras?

\[
\frac{p}{q} \cdot \frac{r}{s} = \frac{pr}{qs} = \frac{m}{n} \quad f(x) + g(x) = h(x) \quad \text{OK}
\]
Solution, Continued

Are these algebras semigroups?

\[
\frac{p}{q} \cdot \left( \frac{r}{s} \cdot \frac{m}{n} \right) = \left( \frac{p}{q} \cdot \frac{r}{s} \right) \cdot \frac{m}{n}
\]

\[
f(x) + (g(x) + h(x)) = (f(x) + g(x)) + h(x)
\]

OK

Are these semigroups monoids?

\[
\frac{p}{q} \cdot 1 = 1 \cdot \frac{p}{q} = \frac{p}{q}
\]

\[
f(x) + 0 = 0 + f(x) = f(x)
\]

OK

Are these monoids groups?

\[
\left( \frac{p}{q} \right) = \frac{q}{p} \quad \text{However,} \quad \left( \frac{0}{1} \right)^{-1} = ?
\]

\[
f(x) = -f(x)
\]

OK for the set of continuous functions

Set of rational numbers with operation of multiplication would be a group only if the element 0 is excluded from the set.

Are these groups Abelian?

\[
\frac{p}{q} \cdot \frac{r}{s} = \frac{r}{s} \cdot \frac{p}{q}
\]

\[
f(x) + g(x) = g(x) + f(x)
\]

OK
Solution, Continued

Are these Abelian groups lattices?

No, the second binary operation is not defined.

Try addition as the second binary operation for the set of rational numbers excluding zero:

one of the distributivity properties fails

$$\frac{p}{q} + \left( \frac{r \cdot m}{s \cdot n} \right) \neq \left( \frac{p}{q} + \frac{r}{s} \right) \cdot \left( \frac{p}{q} + \frac{m}{n} \right)$$

Try multiplication as the second binary operation for the set of continuous functions:

one of the distributivity properties fails

$$f(x) + (g(x) \cdot h(x)) \neq (f(x) + g(x)) \cdot (f(x) + g(x))$$
Analysis of home exercises

2. A geometrical figure on a plane is an infinite honeycomb structure. Give examples of the elements of the symmetry group for this figure.

1) Translations (two basic vectors)
2) Reflections (line symmetry, 6 lines)
3) Rotations by $60^\circ$, $120^\circ$, $180^\circ$ etc. with respect to the center of the cell
4) Rotations by $120^\circ$, $240^\circ$ with respect to the corner of the cell
Algebra of complex numbers

Carrier set is a cross-product \( C = \mathbb{R} \times \mathbb{R} = \mathbb{R}^2 \)

Elements are 2-tuples (ordered pairs) \( z = (x, y) \)

The first component of the pair is called the real part of \( z \), \( x = \text{Re}(z) \)

The second component of the pair is called the imaginary part of \( z \): \( y = \text{Im}(z) \)

Operation “+”, addition: \( z_1 = (x_1, y_1), \ z_2 = (x_2, y_2) \), then \( z_1 + z_2 = (x_1 + x_2, y_1 + y_2) \)

Corresponding unary inverse operation: \(-z = (-x, -y)\)

Related constant (identity element) \( O = (0, 0) \)

Operation “\( \cdot \)”, multiplication: \( z_1 = (x_1, y_1), \ z_2 = (x_2, y_2) \), then \( z_1 \cdot z_2 = (x_1 \cdot x_2 - y_1 \cdot y_2, x_1 \cdot y_2 + x_2 \cdot y_1) \)

Corresponding unary inversion operation (for \( z \neq O \)) \[ \frac{1}{z} = \left( \frac{x}{x^2 + y^2}, -\frac{y}{x^2 + y^2} \right) \]

Related constant (identity element) \( 1 = (1, 0) \)

Interrelation between the operations \( z_1 \cdot (z_2 + z_3) = z_1 \cdot z_2 + z_1 \cdot z_3 \)

Both operations are commutative by definition.

Signature \((\mathbb{R}^2, +, \cdot, -, 1/z, (0,0), (1,0))\)
Algebra of complex numbers: Is it a group?

Remember, however, the element $O$ must be in the group as identity element for “$+$” operation, while inversion for “$\cdot$” operation is not defined for $O$. Strictly speaking, algebra of complex numbers with respect to multiplication is a monoid.

Try to resolve the problem: add one more element to the set: infinity, $\infty$

By definition, $(0,0)^{-1} = \infty$ and $\infty^{-1} = (0,0)$

This, however, is inconsistent with other group properties. For example, solving equation $a \cdot x = b$. On a group, there always should be a unique solution, for any choice of $a$ and $b$: $x = a^{-1} \cdot b$. However, the equations such as $O \cdot x = O$, $\infty \cdot x = \infty$, etc are difficult to interpret.

Set of complex numbers excluding $(0,0)$ forms a group with respect to operation of multiplication.
Complex numbers, continued

There is another constant, and then, another operation

The imaginary unity \( i = (0, 1) \)

Its property: \( i^2 = (0, 1) \cdot (0, 1) = (-1, 0) = -(1, 0) \)

Any complex number \( z = (x, y) = (x, 0) \cdot (1, 0) + (y, 0) \cdot (0, 1) = x + y \cdot i \)

For convenience, \( (x, 0) \equiv x \) and \( (y, 0) \equiv y \) e.t.c.

Another unary operation, complex conjugation \( z^* = x - y \cdot i \)

Interrelation with the other operations:

\[
(z_1 \cdot z_2)^* = (z_1)^* \cdot (z_2)^* \\
(z_1 + z_2)^* = (z_1)^* + (z_2)^* \\
(-z)^* = -(z^*) \\
\left( \frac{1}{z} \right)^* = \frac{1}{z^*}
\]

Signature \( \left( \mathbb{C}, +, -, \cdot, \frac{1}{z}, z^*, 1, 0, i \right) \)
Geometric representation of complex numbers

Magnitude (or amplitude) $r = |z| = \sqrt{x^2 + y^2} = \sqrt{z \cdot z^*}$

Angle $\varphi = \tan^{-1}\left(\frac{y}{x}\right) = \tan^{-1}\left(\frac{z - z^*}{i(z + z^*)}\right)$ (add $\pi$ if $x<0$)

$x = r \cdot \cos(\varphi) \quad y = r \cdot \sin(\varphi)$

$z = r \cdot (\cos(\varphi) + i \cdot \sin(\varphi))$
Geometric representation of adding complex numbers

\[ z_1 = (x_1, y_1), \quad z_2 = (x_2, y_2), \quad z = z_1 + z_2 = (x_1 + x_2, y_1 + y_2) \]

Add complex numbers ⇔
add vectors on a complex plane
Geometric representation of multiplying complex numbers

\[ z = (r, \varphi) \]
\[ z_1 = (r_1, \varphi_1) \]
\[ z_2 = (r_2, \varphi_2) \]

\[ r_1 \cdot (\cos(\varphi_1) + i \cdot \sin(\varphi_1)) \cdot r_2 \cdot (\cos(\varphi_1) + i \cdot \sin(\varphi_2)) = \]
\[ r_1 \cdot r_2 \cdot \left[ \cos(\varphi_1) \cdot \cos(\varphi_2) - \sin(\varphi_1) \cdot \sin(\varphi_2) \right] + i \cdot \left[ \cos(\varphi_1) \cdot \sin(\varphi_2) + \sin(\varphi_1) \cdot \cos(\varphi_2) \right] = \]
\[ = r \cdot (\cos(\varphi) + i \cdot \sin(\varphi)) \]

\[ r = r_1 \cdot r_2 \quad \varphi = \varphi_1 + \varphi_2 \]

Multiply complex numbers ⇔
multiply the magnitudes and add the angles
Functions of a complex variable

A possible way to define a function of a complex variable is to use a concept of analytical extension of a corresponding function defined on $\mathbb{R}$.

Consider a real function of a real variable that is infinitely differentiable ("absolutely smooth").

$$f(x) = f(x_0) + f'(x_0) \cdot (x - x_0) + \frac{1}{2} f''(x_0) \cdot (x - x_0)^2 + ...$$

Notice: $x \in \mathbb{R}, f(x_0) \in \mathbb{R}, f'(x_0) \in \mathbb{R}, f''(x_0) \in \mathbb{R}, ...$

Now form $f(z) = f(x_0) + f'(x_0) \cdot (z - x_0) + \frac{1}{2} f''(x_0) \cdot (z - x_0)^2 + ...$

That is, replace $x$ with a complex variable $z$.
$f(z)$ becomes a complex valued function of a complex variable.

This procedure is known as analytical extension of a real function on complex plane.

The Euler formula $e^{ix} = \cos(x) + i \cdot \sin(x)$

Obtained by the analytical extension of $e^x = 1 + x + \frac{1}{2} x^2 + ...$
Linear Space

Linear space (real linear space) is a mathematical structure that combines an Abelian group and the algebra of complex (real) numbers.

Linear space includes: an Abelian group \((V, +, -, \theta)\), the algebra of complex numbers \((\mathbb{C}, +, \cdot, -, 1/z, z^*, O, 1, i)\), and operation “\(\cdot\)” that defines a mapping \(\mathbb{C} \times V \rightarrow V \) \((v' = \alpha \cdot v, v \in V, v' \in V, \alpha \in \mathbb{C})\) with properties

1) **Associativity** \[ \alpha_1 \cdot (\alpha_2 \cdot v) = (\alpha_1 \cdot \alpha_2) \cdot v \]

2) **First distributivity** \[ \alpha \cdot (v_1 + v_2) = (\alpha \cdot v_1) + (\alpha \cdot v_2) \]

3) **Second distributivity** \[ (\alpha_1 + \alpha_2) \cdot v = (\alpha_1 \cdot v) + (\alpha_2 \cdot v) \]

4) **Identity** \[ 0 \cdot v = \theta \quad \text{and} \quad 1 \cdot v = v \]
Examples of Linear Spaces

A trivial example: Algebra of complex numbers itself (take \( V = \mathbb{C} \)). Then the operation that defines \((\mathbb{C} \times V \rightarrow V) \iff (\mathbb{C}^2 \rightarrow \mathbb{C})\) is a conventional multiplication of complex numbers as it was defined previously.

Another example: vectors in \( \mathbb{R}^3 \) (and in any \( \mathbb{R}^n \)) \( (x, y, z) \in \mathbb{R}^3 \) = \( \begin{pmatrix} x \\ y \\ z \end{pmatrix} \)

Operations in the Abelian group \((\mathbb{R}^3, +, -, \theta)\)

\[
\begin{pmatrix} x_1 \\ y_1 \\ z_1 \end{pmatrix} + \begin{pmatrix} x_2 \\ y_2 \\ z_2 \end{pmatrix} = \begin{pmatrix} x_1 + x_2 \\ y_1 + y_2 \\ z_1 + z_2 \end{pmatrix} \quad - \begin{pmatrix} x \\ y \\ z \end{pmatrix} = \begin{pmatrix} -x \\ -y \\ -z \end{pmatrix}
\]

Operation in the linear space

\[
\alpha \cdot \begin{pmatrix} x \\ y \\ z \end{pmatrix} = \begin{pmatrix} \alpha \cdot x \\ \alpha \cdot y \\ \alpha \cdot z \end{pmatrix}
\]

One more example:

\( V = \) set of all complex-valued functions \( f(x) \) of the real variable \( x \in [0, 1] \)

\( f_1(x) + f_2(x) \) is a conventional sum of the values \( f_1(x) \) and \( f_2(x) \)

Elements of linear space are often called “vectors”. Functions \( f_1(x) \) and \( f_2(x) \) in the previous example are also referred to as vectors.
Linear combination and span.
Linear mapping

\{v_i, i = 1, 2, \ldots, n\} = \{v_1, v_2, \ldots, v_n\} = V' \subset V

Linear combination: \( L.c.({v_i}) = \sum_{i=1}^{n} \alpha_i v_i \)

(If \( n = \infty \), the linear combination contains infinite number of terms)

A trivial linear combination is the combination that produces the zero element

\[ \sum_{i=1}^{n} \alpha_i v_i = \theta \]

Span of the set \( \{v_i\} \) (denoted \( [\{v_i\}] \)) is a set of all possible \( L.c.({v_i}) \) generated using all possible scalar coefficients \( \alpha_i \). Obviously, \( L.c.({v_i}) \subset V \), but not necessarily every element in \( V \) can be presented as a linear combination of \( \{v_i\} \).

Consider a mapping from a linear space \( V \) to a linear space \( W \). \((V \rightarrow W, w=b(v), v \in V, w \in W. \) The codomain \( W \) is another linear space). The mapping is called linear if for any set of scalar coefficients \( \alpha_i \)

\[ b\left( \sum_{i=1}^{n} \alpha_i \cdot v_i \right) = \sum_{i=1}^{n} \alpha_i \cdot b(v_i) \]
Linear and nonlinear mapping

\[ v_3 = \alpha_1 v_1 + \alpha_2 v_2 \]

\[ w_3 = \alpha_1 w_1 + \alpha_2 w_2 \]

\[ w_1 = b(v_1) \]

\[ w_2 = b(v_2) \]

\[ w_3' = b(v_3) \]
Linear subspaces

Linear subspace $V'$ of a space $V$ ($V' \subseteq V$) has a carrier set that coincides with its own span $V' = [V']$

"Any linear combination of elements from $V'$ belong to $V'$"

$(v_1, v_2 \in V') \land (\alpha_1, \alpha_2 \in \mathbb{C}) \rightarrow (\alpha_1 \cdot v_1 + \alpha_2 \cdot v_2 \in V')$

Example of a subspace: take $v \neq \theta$ in $\mathbb{R}^3$ and construct $\mathbb{R}_v = [v]$

Example of a subset in $\mathbb{R}^3$ that is not a subspace: $\{(x, y, z) = \begin{pmatrix} x \\ y \\ z \end{pmatrix} \mid x^2 + y^2 + z^2 < 1\}$

Another example: a set of polynomials defined on $[0, 1]$ is a subspace of the linear space of all functions on $[0,1]$

Important property: If $V_1$ and $V_2$ are linear subspaces of $V$, then $V_1 \cap V_2$ and $V_1 \cup V_2$ are also linear subspaces.
Linear independence

A set \( \{v_i\} \) is called linearly independent if the only trivial linear combination is that with all coefficients equal to zero.

\[
\sum_{i=1}^{n} \alpha_i \cdot v_i = \theta \Rightarrow \forall \alpha_i = 0
\]

Example of linearly independent set: \( \{1, i\} \subset \mathbb{C} \)

Another example: vectors \( \{e_x, e_y, e_z\} \) in \( \mathbb{R}^3 \)

\[
e_x = \begin{pmatrix} 1 \\ 0 \\ 0 \end{pmatrix}, \quad e_y = \begin{pmatrix} 0 \\ 1 \\ 0 \end{pmatrix}, \quad e_z = \begin{pmatrix} 0 \\ 0 \\ 1 \end{pmatrix}
\]

Examples of linearly dependent sets:

Any set that contains the zero element.

Any set, in which one element can be obtained by multiplying another element by a scalar coefficient.

Any set, in which one element can be obtained as a linear combination of other elements.
Basis and dimension of a linear space

A finite set \( \{v_1, v_2, \ldots, v_n\} \) of linearly independent elements, whose span is equal to the entire linear space \( V \) is called the basis of \( V \): \( \{v_1, v_2, \ldots, v_n\} = V \)

“the basis \( \{v_1, v_2, \ldots, v_n\} \) generates the entire space \( V \)”

A linear space that has a finite basis is called a finite-dimensional space.

Example: \( \mathbb{R}^3 \) is 3-dimensional

A set of polynomials on \([0, 1]\) is infinite-dimensional (there is no finite set that forms a basis).

Coefficients in the linear combination that generate a given element in \( V \) are called decomposition.

Decomposition is unique.

\[
\begin{align*}
v &= \sum_{i=1}^{n} \alpha_i \cdot v_i \quad (v_i \in \{v_1, v_2, \ldots, v_n\}) \\
\text{assume } v &= \sum_{i=1}^{n} \beta_i \cdot v_i \text{ then } \theta = v - v = \sum_{i=1}^{n} (\alpha_i - \beta_i) \cdot v_i \\
\text{which is only possible if } &\forall i \quad \alpha_i = \beta_i
\end{align*}
\]
Basis and dimension (continued)

Basis is not unique:

e. g. in $\mathbb{R}^3$

$\{e_1, e_2, e_3\}$ also form a basis

\[
\begin{align*}
e_1 &= \begin{pmatrix} 1 \\ 1 \\ 0 \end{pmatrix} \\
e_2 &= \begin{pmatrix} 0 \\ 0 \\ 1 \end{pmatrix} \\
e_3 &= \begin{pmatrix} 0 \\ 1 \\ 1 \end{pmatrix}
\end{align*}
\]

Different bases in a given linear space always have the same number of elements: dimensionality of the space is its fundamental property, it does not depend on the choice of the basis.

Proof: assume it’s not the case $\exists \{x_1, x_2, \ldots, x_n\} \ \exists \{y_1, y_2, \ldots, y_m\}$ $n \neq m$ (say, $m>n$)

Take a set $\{y_1, y_2, \ldots, y_n\}$. All elements in this set are linearly independent.

Form the span $[\{y_1, y_2, \ldots, y_n\}]$. Check that $[\{y_1, y_2, \ldots, y_n\}] = [\{x_1, x_2, \ldots, x_n\}]$.

Then $\{y_{n+1}, \ldots, y_m\} \subset V = [\{x_1, x_2, \ldots, x_n\}] = [\{y_1, y_2, \ldots, y_n\}]$, and each of the elements of $\{y_{n+1}, \ldots, y_m\}$ can be represented as a linear combination of $\{y_1, y_2, \ldots, y_n\}$.
Decomposition as mapping. Isomorphism of finite-dimensional linear space

\[(v \in V) \rightarrow ((\alpha_1, \alpha_2, \ldots, \alpha_n) \in \mathbb{C}^n)\]

For a given basis, there is one-to-one mapping from \(V\) to \(\mathbb{C}^n\) (or \(\mathbb{R}^n\) as a particular case)

Regardless of the nature of the elements of linear spaces, all linear spaces are equivalent to \(\mathbb{C}^n\) (or, even simpler, to \(\mathbb{R}^n\) when dealing with real numbers only).

The only difference is what you call the basis.
Exercises

1) In $\mathbb{R}^3$, consider a subset of vectors

$$v = \begin{pmatrix} x \\ y \\ z \end{pmatrix}$$

such that $x + y + z = 0$. Does this subset form a linear subspace of $\mathbb{R}^3$?

If yes, find its dimension.

2) Check if following vectors in $\mathbb{R}^3$ are linearly independent

$$v_1 = \begin{pmatrix} 1 \\ 2 \\ 3 \end{pmatrix}, \quad v_2 = \begin{pmatrix} 4 \\ 5 \\ 6 \end{pmatrix}, \quad v_3 = \begin{pmatrix} 7 \\ 8 \\ 9 \end{pmatrix}$$

3) Consider a set of real-valued functions $f(t), t \in [0,1]$ satisfying following condition

$$\frac{df}{dt} = \int_0^t f(\tau)d\tau$$

Does this set form a linear subset of all real functions defined over the interval $[0,1]$?

If yes, find its dimension.