1 Course details

The first half of this course will be cover representation theory.

The second half will cover Galois theory.

Some relevant notes and textbooks are listed on the public course website:

`https://www.math.hkust.edu.hk/~emarberg/teaching/2026/Math5112/`

Grades will be based on (approximately) weekly homework assignments.

All homework assignments must be submitted **in-person, in hand-written form.**

But there will be no exams.

All lectures will be posted on the public course webpage in pdf format (without annotations).

The annotated slides presented in class, which contain the same content, will not be posted.

2 Associative algebras

Let $\mathbb{K}$ be a field. Assume that $\mathbb{K}$ is algebraically closed unless noted otherwise.

Then when V is a finite-dimensional $\mathbb{K}$-vector space, every linear map $V \to V$ has an eigenvalue in $\mathbb{K}$.

The most common example of an algebraically closed field is the complex numbers $\mathbb{C}$.

Definition. An *associative algebra* (over $\mathbb{K}$) is a $\mathbb{K}$-vector space A with a bilinear map $A \times A \to A$, written $(a, b) \mapsto ab$, that is associative in the sense that $a(bc) = (ab)c$ for all $a, b, c \in A$.

The bilinear map corresponding to an associative algebra is called its *product* or *multiplication map*.

Here *bilinear* means that for all $a, b, c \in A$ and $\lambda \in \mathbb{K}$ we have

$$(a+b)c = ac + bc \qquad \text{and} \qquad a(b+c) = ab + ac \qquad \text{and} \qquad (\lambda a)b = a(\lambda b) = \lambda(ab).$$

Because the product of an algebra A is associative, any way of parenthesizing an iterated product

$$a_1 a_2 a_3 \dots a_n$$

with each $a_i \in A$ gives the same result, so we can just omit the parentheses in such expressions.

Definition. A *unit* for an associative algebra A is an element $1 \in A$ with $1a = a1 = a$ for all $a \in A$.

Proposition. If an associative algebra A has a unit then it is unique.

Proof. If 1 and $1'$ are both units for A, then $1 = 11' = 1'$ since $a = a1'$ and $1a = a$ for all $a \in A$. □

From now on, an *algebra* (over $\mathbb{K}$) means a **nonzero**, **associative** algebra that **has a unit**.

A *subalgebra* of an algebra is a subspace containing the unit that is closed under multiplication.

Example. Here are some common examples of algebras:

- *Trivial algebras*: the field $\mathbb{K}$ is itself an algebra.

  This is the algebra of smallest possible dimension, since the zero vector space is not an algebra.

- *Polynomial algebras*: for each positive integer n the set

$$\mathbb{K}[x_1, x_2, \ldots, x_n]$$

of polynomials in commuting variables x_i with coefficients in $\mathbb{K}$ is an algebra with unit 1.

This algebra is *commutative*, meaning $fg = gf$ for all elements f and g.

- *Endomorphism algebras*: if V is a nonzero $\mathbb{K}$-vector space then the vector space

$$\mathsf{End}(V) = \{\text{all } \mathbb{K}\text{-linear maps } V \to V\}$$

is an algebra. Its product is composition of maps and its unit is the identity map $\mathrm{id}_V : V \to V$.

The vector space of *all* maps $V \to V$ is also algebra with the same product and unit, but this is an unreasonably high-dimensional object that is not of much interest.

- *Free algebras*: for each positive integer n the set

$$\mathbb{K}\langle X_1, X_2, \ldots, X_n\rangle$$

of polynomials in non-commuting variables X_i is also an algebra.

- *Group algebras*: if G is a group then the $\mathbb{K}$-vector space $\mathbb{K}[G]$ with basis $\{a_g : g \in G\}$ is an algebra.

This product for this algebra is the bilinear multiplication that has $a_g a_h = a_{gh}$ for $g, h \in G$.

The unit for $\mathbb{K}[G]$ is the basis element a_1 indexed by the group's unit $1 \in G$.

In other words, $\mathbb{K}[G]$ consists of all $\mathbb{K}$-linear combinations of elements of G, which we add and multiply as we would polynomials, just using the group law for product of individual terms.

We will sometimes use the term *$\mathbb{K}$-algebra* (rather than *algebra*) to emphasize the field.

If A and B are two $\mathbb{K}$-algebras then we typically denote the units in both by the same symbol 1.

Definition. A *morphism* $f : A \to B$ of $\mathbb{K}$-algebras is a $\mathbb{K}$-linear map such that

$$f(1) = 1 \qquad \text{and} \qquad f(ab) = f(a)f(b) \quad \text{for all } a, b \in A.$$

A morphism $f : A \to B$ is an *isomorphism* if there is a morphism $g : B \to A$ with

$$f \circ g = \mathrm{id}_B \qquad \text{and} \qquad g \circ f = \mathrm{id}_A\,.$$

This occurs if and only if f is a bijection.

Example. There is a unique morphism $K\langle X_1, X_2, \ldots, X_n\rangle \to K[x_1, x_2, \ldots, x_n]$ that sends each $X_i \mapsto x_i$.

In words, this morphism takes a polynomial in non-commuting variable and lets the variables commute.

More generally, if A is any algebra and $a_1, a_2, \ldots, a_n \in A$ then there is a unique morphism

$$K\langle X_1, X_2, \ldots, X_n\rangle \to A \qquad \text{sending each } X_i \mapsto a_i.$$

Example. There is a unique morphism $\mathbb{K} \to A$ for any $\mathbb{K}$-algebra A.

This means that $\mathbb{K}$ is an *initial object* in the category of $\mathbb{K}$-algebras.

3 Representations

Fix a $\mathbb{K}$-algebra A. Suppose V is a $\mathbb{K}$-vector space and $\rho : A \to \mathsf{End}(V)$ is a map.

Definition. The pair (ρ, V) is a *representation* of A if ρ is a linear map satisfying

$$\rho(1) = \mathrm{id}_V \quad \text{and} \quad \rho(ab) = \rho(a)\rho(b) \quad \text{for all } a, b \in A.$$

When $V \neq 0$ so that $\mathsf{End}(V)$ is an algebra, this just says that $\rho : A \to \mathsf{End}(V)$ is an algebra morphism. However, we allow $V = 0$ to be the zero vector space in the definition of a representation of A.

Sometimes we will call the map $\rho : A \to \mathsf{End}(V)$ a representation.
When ρ is known implicitly, we may also refer to V as a representation of A.

Definition. A *left A-module* is a $\mathbb{K}$-vector space V with a bilinear operation $A \times V \to V$ such that

$$1v = v \quad \text{for all } v \in V \qquad \text{and} \qquad a(bv) = (ab)v \quad \text{for all } a, b \in A \text{ and } v \in V.$$

Representations of A are the same thing as left A-modules in the following sense:

(1) If (ρ, V) is a representation, then we can make V into a left A-module by setting

$$av \stackrel{\text{def}}{=} \rho(a)(v) \qquad \text{for } a \in A \text{ and } v \in V$$

(2) If V is a left A-module, then we get a representation (ρ, V) by defining

$$\rho(a)(v) \stackrel{\text{def}}{=} av \qquad \text{for } a \in A \text{ and } v \in V.$$

Moreover, operations (1) and (2) are inverses of each other.

Definition. Let A^{op} be the same vector space as A but with multiplication $a *_{\mathsf{op}} b = ba$ for $a, b \in A$.
This gives another algebra with the same unit as A known as the *opposite algebra*.
It is instructive to check the associativity of $*_{\mathsf{op}}$ directly:

$$a *_{\mathsf{op}} (b *_{\mathsf{op}} c) = a *_{\mathsf{op}} (cb) = (cb)a = c(ba) = ba *_{\mathsf{op}} c = (a *_{\mathsf{op}} b) *_{\mathsf{op}} c.$$

Definition. A *right A-module* is a vector space V with a bilinear map $V \times A \to V$ such that

$$v1 = v \quad \text{for all } v \in V \qquad \text{and} \qquad (va)b = v(ab) \quad \text{for all } a, b \in A \text{ and } v \in V.$$

Representations of A^{op} are the same as right A-modules, in the same sense as above.
If A is commutative, then $A = A^{\mathsf{op}}$. In this case, left A-modules are the same thing as right A-modules.

Example. Every algebra A has a *(left) regular representation* (ρ, A) where $\rho : A \to \mathsf{End}(A)$ is the map

$$\rho(a)(b) = ab \qquad \text{for } a, b \in A.$$

If $A = \mathbb{K}$ then any $\mathbb{K}$-vector space is a left A-module and so affords a representation.

Definition. Suppose (ρ, V) is a representation of A.

A *subrepresentation* of (ρ, V) is a subspace $W \subset V$ such that $\rho(a)(W) \subseteq W$ for all $a \in A$.

Both 0 and V are subrepresentations of (ρ, V).

A representation (ρ, V) of A is *irreducible* if it has exactly two subrepresentations.

This means that V must be nonzero and have no proper subrepresentations.

Definition. Suppose V is a left A-module.

A *submodule* is a subspace $W \subset V$ such that $aw \in W$ for all $a \in A$ and $w \in W$.

An A-module V is *irreducible* if it has exactly two submodules (namely, 0 and V).

Under the correspondence described above, subrepresentations $\leftrightarrow$ submodules.

In practice, we will treat subrepresentations and submodules as the same thing.

4 Morphisms of representations

The representations of a given algebra A form a category with the following notion of morphisms.

Definition. Suppose (ρ_1, V_1) and (ρ_2, V_2) are both representations of A.

A *morphism* $\phi : (\rho_1, V_1) \to (\rho_2, V_2)$ is a linear map $\phi : V_1 \to V_2$ such that

$$\phi(\rho_1(a)(v)) = \rho_2(a)(\phi(v)) \qquad \text{for all } a \in A \text{ and } v \in V_1.$$

This property holds precisely when the following diagram commutes for all $a \in A$:

$$\begin{array}{ccc} V_1 & \xrightarrow{\phi} & V_2 \\ {\scriptstyle \rho_1(a)}\downarrow & & \downarrow{\scriptstyle \rho_2(a)} \\ V_1 & \xrightarrow{\phi} & V_2 \end{array}$$

We say that ϕ is an *isomorphism* if ϕ is a bijection.

The *zero morphism* $(\rho_1, V_1) \to (\rho_2, V_2)$ is the map that sends all elements of V_1 to $0 \in V_2$.

For the following result, $\mathbb{K}$ may be any field, not necessarily algebraically closed.

Proposition (*Schur's Lemma*)**.** Let (ρ_1, V_1) and (ρ_2, V_2) be representations of A.

Suppose $\phi : (\rho_1, V_1) \to (\rho_2, V_2)$ is a nonzero morphism.

(a) If (ρ_1, V_1) is irreducible then ϕ is injective.

(b) If (ρ_2, V_2) is irreducible then ϕ is surjective.

(c) If both representations are irreducible then ϕ is an isomorphism.

Proof. The *kernel* and *image* subspaces

$$\ker(\phi) = \{v \in V_1 : \phi(v) = 0\} \subseteq V_1 \quad \text{and} \quad \text{image}(\phi) = \{\phi(v) : v \in V_1\} \subseteq V_2$$

are both subrepresentations, but $\ker(\phi) \neq V_1$ and $\text{image}(\phi) \neq 0$ since ϕ is nonzero.

Recall that ϕ is injective when $\ker(\phi) = 0$ and surjective when $\text{image}(\phi) = V_2$.

The result follows since 0 and V are the only subrepresentations of an irreducible representation (ρ, V). □

For the last two results we go back to assuming that $\mathbb{K}$ is algebraically closed.

Corollary. Suppose (ρ, V) is an irreducible representation of A with $\dim(V) < \infty$.

If $\phi : (\rho, V) \to (\rho, V)$ is any morphism then there exists $\lambda \in \mathbb{K}$ with $\phi(v) = \lambda v$ for all $v \in V$.

Proof. As $\mathbb{K}$ is algebraically closed, the linear map ϕ has an eigenvalue $\lambda \in \mathbb{K}$.

The difference $\phi - \lambda \cdot \text{id}_V$ is not invertible but it is still a morphism $(\rho, V) \to (\rho, V)$.

Therefore we must have $\phi - \lambda \cdot \text{id}_V = 0$ by Schur's Lemma. □

Corollary. Suppose A is commutative. Then every irreducible representation (ρ, V) of A has $\dim V = 1$.

Proof. Suppose (ρ, V) is a representation of A.

Fix $a \in A$. Then the map $\rho(a) : V \to V$ is a morphism $(\rho, V) \to (\rho, V)$ since A is commutative.

By the previous corollary we must have $\rho(a) = \lambda \cdot \text{id}_V$ for some $\lambda \in \mathbb{K}$.

But this applies to every $a \in A$, so every subspace of V is a subrepresentation.

Therefore V is irreducible if and only if $\dim V = 1$. □