Today's lecture reviews the main results we have seen in this course.

1 Algebras and representations

Let $\mathbb{K}$ be an algebraically closed field.

Definition. An *(associative, unital) algebra* is a nonzero $\mathbb{K}$-vector space A with a bilinear *product* map $A \times A \to A$ and a *unit* element $1 \in A$ that satisfy $a(bc) = (ab)c$ and $1a = a1 = a$ for all $a, b, c \in A$.

A *morphism* $f : A \to B$ of algebras is a $\mathbb{K}$-linear map with $f(1) = 1$ and $f(ab) = f(a)f(b)$ for all $a, b \in A$.

A morphism that is a bijection is called an *isomorphism*.

Example. If V is a nonzero $\mathbb{K}$-vector space, then the vector space $\mathsf{End}(V)$ of all linear maps $V \to V$ is an algebra, where the product is composition $\rho_1\rho_2 = \rho_1 \circ \rho_2$ and the unit is the identity map $\mathrm{id}_V : V \to V$.

Definition. A *representation* of an algebra A is a pair (ρ, V) where

- V is a $\mathbb{K}$-vector space, and
- ρ is a linear map $A \to \mathsf{End}(V)$ satisfying $\rho(1) = \mathrm{id}_V$ and $\rho(ab) = \rho(a)\rho(b)$ for all $a, b \in A$.

A *morphism* $\phi : (\rho_1, V_1) \to (\rho_2, V_2)$ of representations of A is a linear map $\phi : V_1 \to V_2$ with

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

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

We say that (ρ, V) is *irreducible* if $V \neq 0$ and there are no other subrepresentations except V and 0.

A representation is *indecomposable* if it is not a direct sum of two nonzero representations.

Every irreducible representation is indecomposable.

Proposition (*Schur's Lemma*)**.** Let $\phi : (\rho_1, V_1) \to (\rho_2, V_2)$ be a morphism of representations of A.

(a) If both representations are irreducible then ϕ is an isomorphism or zero.

(b) If $(\rho, V) = (\rho_1, V_1) = (\rho_2, V_2)$ is irreducible with $\dim(V) < \infty$, then $\phi = \lambda \cdot \mathrm{id}_V$ for some $\lambda \in \mathbb{K}$.

(c) If A is *commutative* (so $ab = ba$ for all $a, b \in A$) then every irreducible repn (ρ, V) has $\dim(V) = 1$.

2 Tensor products

Let V and W be two $\mathbb{K}$-vector spaces

The *tensor product* $V \otimes W$ is the $\mathbb{K}$-vector spanned by *pure tensors* $v \otimes w$ with $v \in V$ and $w \in W$, where

$$(v_1 + v_2) \otimes w = v_1 \otimes w + v_2 \otimes w, \quad v \otimes (w_1 + w_2) = v \otimes w_1 + v \otimes w_2, \quad av \otimes w = v \otimes aw = a(v \otimes w)$$

for any $a \in \mathbb{K}, v_1, v_2, v \in V$, $w_1, w_2, w \in W$.

If V has basis $\{v_i\}_{i\in I}$ and W has basis $\{w_j\}_{j\in J}$ then $\{v_i \otimes w_j\}_{(i,j)\in I\times J}$ is a basis for $V \otimes W$.

The *tensor algebra* of a vector space V is defined as $\mathcal{T}V = \bigoplus_{n\geq 0} V^{\otimes n}$.

Any choice of basis for V determines an isomorphism from $\mathcal{T}V$ to a free algebra $\mathbb{K}\langle X_1, X_2, \dots\rangle$.

The *symmetric algebra* of V is $\mathcal{S}V \overset{\text{def}}{=} \mathcal{T}V/\langle v\otimes w - w\otimes v : v,w\in V\rangle$.

The *exterior algebra* is $\bigwedge V \overset{\text{def}}{=} \mathcal{T}V/\langle v\otimes v : v\in V\rangle$.

3 Semisimplicity

Proposition (*Density theorem*)**.** Let $(\rho_1, V_1), \dots (\rho_r, V_r)$ be irreducible finite-dimensional A-representations. If we have $(\rho_i, V_i) \not\cong (\rho_j, V_j)$ for all $i\neq j$ then $\bigoplus_{i=1}^r \rho_i : A \to \bigoplus_{i=1}^r \mathsf{End}(V_i)$ is surjective.

Suppose A is a finite-dimensional algebra over $\mathbb{K}$. The *radical* of A is

$$\begin{aligned}\mathsf{Rad}(A) &\overset{\text{def}}{=} \{\text{the elements in } A \text{ that act as zero in every irreducible representation of } A\}\\ &= (\text{the largest nilpotent 2-sided ideal in } A)\,.\end{aligned}$$

Theorem. A finite-dimensional algebra A has finitely many irreducible representations $V_1,\dots,V_r$ up to isomorphism, and it holds that $A/\mathsf{Rad}(A) \cong \bigoplus_{i=1}^r \mathsf{End}(V_i)$

An A-representation is *semisimple* if it is a direct sum of irreducible subrepresentations.

The algebra A is *semisimple* if any (and hence all) of the following equivalent properties hold:

(1) $\mathsf{Rad}(A) = 0$.

(2) If $V_1, V_2, \dots, V_r$ represent all distinct isomorphism classes of irreducible A-representations, then

$$\dim(A) = \textstyle\sum_{i=1}^r \dim(V_i)^2.$$

(3) A is isomorphic to a finite direct sum of matrix algebras $\mathsf{Mat}_{d_1}(\mathbb{K}) \oplus \mathsf{Mat}_{d_2}(\mathbb{K}) \oplus \cdots \oplus \mathsf{Mat}_{d_r}(\mathbb{K})$.

(4) Every A-representation of finite dimension is semisimple.

(5) The regular representation of A is semisimple.

4 Characters

Assume (ρ, V) is an A-representation with $\dim(V) < \infty$.

The *character* of (ρ, V) is the linear map $\chi_{(\rho,V)} : A \to \mathbb{K}$ with the formula

$$\chi_{(\rho,V)}(a) = \mathrm{trace}(\rho(a)) \overset{\text{def}}{=} \textstyle\sum_{i=1}^n (\text{coefficient of } b_i \text{ in } \rho(a)(b_i)) \quad \text{for any basis } b_1, b_2, \dots, b_n \text{ of } V.$$

Theorem. The characters of non-isomorphic irreducible finite-dimensional A-representations are linearly independent (and therefore distinct).

It always holds that $\mathsf{kernel}(\chi_{(\rho,V)}) \supset [A,A] \overset{\text{def}}{=} \mathbb{K}\text{-span}\{ab - ba : a,b\in A\}$.

This means we can view a character as a linear map $A/[A,A] \to \mathbb{K}$.

Theorem. If A is finite-dimensional and semisimple, then the irreducible characters of A are a basis for the dual space $(A/[A,A])^*$. If $\mathrm{char}(\mathbb{K}) = 0$, then two finite-dimensional A-representations are isomorphic if and only if they have same characters.

5 Jordan-Hölder and Krull-Schmidt theorems

Suppose V is an A-representation with $\dim(V) < \infty$.

Theorem (*Jordan-Hölder theorem*)**.** There exists a filtration of subrepresentations

$$0 = V_0 \subset V_1 \subset \cdots \subset V_n = V$$

with irreducible quotients V_i/V_{i-1}, and the length n of the filtration and the isomorphism classes of the quotients are uniquely determined up to permutation of indices.

Theorem (*Krull-Schmidt theorem*)**.** There is a direct sum decomposition of V into indecomposable subrepresentations that is unique up to isomorphism and rearrangement of factors.

6 Group representations

Assume G is a finite group.

Theorem (*Maschke's theorem*)**.** $\mathbb{K}[G]$ is semisimple if and only if $\mathrm{char}(\mathbb{K})$ does not divide $|G|$.

Assume (ρ, V) is a finite dimensional G-representation.

The *character* of (ρ, V) is a linear map $\chi_{(\rho,V)} : \mathbb{K}[G] \to \mathbb{K}$ sending $g \mapsto \mathrm{trace}(\rho(g))$ for all $g \in G$.

We say that $\chi_{(\rho,V)}$ is *irreducible* if (ρ, V) is an irreducible representation.

Let $\mathrm{Irr}(G)$ denote the set of irreducible characters of G.

When $\mathbb{K}[G]$ is semisimple, the following properties hold:

(1) $\mathrm{Irr}(G)$ is a basis for the $\mathbb{K}$-vector space of class functions $G \to \mathbb{K}$.

(2) If $\mathrm{char}(\mathbb{K}) = 0$, then $\chi_{(\rho,V)} = \chi_{(\rho',V')}$ if and only if $(\rho, V) \cong (\rho', V')$.

(3) $\sum_{\chi \in \mathrm{Irr}(G)} \chi(1)^2 = |G|$.

Given functions $f_1, f_2 : G \to \mathbb{C}$ let $(f_1, f_2) \overset{\text{def}}{=} \frac{1}{|G|} \sum_{g \in G} f_1(g)\overline{f_2(g)}$.

Theorem. $\mathrm{Irr}(G)$ is an orthonormal basis for the space of class functions $G \to \mathbb{C}$ relative to $(\cdot, \cdot)$.

Theorem. Let $g, h \in G$ and define $Z_g = \{x \in G : xgx^{-1}\}$ and $\mathcal{K}_g = \{xgx^{-1} : x \in g\}$. Then

$$\sum_{\psi \in \mathrm{Irr}(G)} \psi(g)\overline{\psi(h)} = \begin{cases} |Z_g| & \mathcal{K}_g = \mathcal{K}_h \\ 0 & \mathcal{K}_g \neq \mathcal{K}_h. \end{cases}$$

7 Restriction and induction

Let H be a subgroup of a finite group G.

If V is a G-representation, then we write $\mathrm{Res}^G_H(V)$ to denote V as an H-representation.

Now suppose W is a representation of H with corresponding map $\rho_W : H \to \mathrm{GL}(W)$.

Let $\mathrm{Ind}_H^G(W) = \Big\{ f : G \to W : f(hx) = \rho_W(h) f(x) \text{ for all } h \in H \text{ and } x \in G \Big\} \cong \mathbb{K}[G] \otimes_{\mathbb{K}[H]} W$.

Then $\mathrm{Ind}_H^G(W)$ is a G-representation (called the *induced representation*) for the action

$$g \cdot f : x \mapsto f(xg) \quad \text{for } g \in G \text{ and } f \in \mathrm{Ind}_H^G(W).$$

The induced representation has dimension $\frac{|G|}{|H|} \dim(W)$.

Theorem. If $\mathbb{K} = \mathbb{C}$ and V and W are finite-dimensional with characters χ_V and χ_W then

$$\Big(\chi_V, \mathrm{Ind}_H^G(\chi_W)\Big)_G = \Big(\mathrm{Res}_H^G(\chi_V), \chi_W\Big)_H$$

where $(f,g)_X = \frac{1}{|X|} \sum_{x \in X} f(x)\overline{g(x)}$ for $X = G$ or $X = H$.

8 Symmetric group representations

Let n be a positive integer. Define S_n to be the group of permutations of $[n] = \{1, 2, \cdots, n\}$.

For each partition $\lambda = (\lambda_1, \cdots, \lambda_\ell) \vdash n$, there is an associated *Specht module* constructed as follows:

$$V_\lambda = \mathbb{C}[S_n] a_\lambda b_\lambda$$

where

$$a_\lambda = \sum_{g \in \text{row stabilizer of } T_\lambda} g \qquad \text{and} \qquad b_\lambda = \sum_{g \in \text{column stabilizer of } T_\lambda} \mathrm{sgn}(g) g.$$

with T_λ any standard tableau of shape λ.

Theorem. Each V_λ for $\lambda \vdash n$ is an irreducible complex representation of S_n.

In addition, each irreducible complex representation of S_n is isomorphic to V_λ for a unique $\lambda \vdash n$.

The *Frobenius character formula* gives an explicit way to compute the character of V_λ.

9 Schur-Weyl duality

Fix positive integers n and N. Let $V = \mathbb{C}^N$ and set $\mathrm{GL}_N = \mathrm{GL}(V)$.

Then $V^{\otimes n} = V \otimes \cdots \otimes V$ is an S_n- and GL_N-representation in which $\sigma \in S_n$ and $g \in \mathrm{GL}_N$ act as

$$\sigma(v_1 \otimes v_2 \otimes \cdots \otimes v_n) = v_{\sigma^{-1}(1)} \otimes v_{\sigma^{-1}(2)} \otimes \cdots \otimes v_{\sigma^{-1}(n)} \quad \text{and} \quad g(v_1 \otimes v_2 \otimes \cdots \otimes v_n) = gv_1 \otimes gv_2 \otimes \cdots \otimes gv_n.$$

Let A and B be the images of $\mathbb{C}[S_n]$ and $\mathbb{C}[\mathrm{GL}_N]$ in $\mathsf{End}(V^{\otimes n})$ defined by these representations.

Schur-Weyl duality refers to the following properties:

(a) A and B are commuting algebras of each other.

(b) A and B are both semisimple, and $V^{\otimes n}$ is a semisimple $\mathbb{C}[S_n] \otimes \mathbb{C}[\mathrm{GL}_N]$-representation.

(c) As a $\mathbb{C}[S_n] \otimes \mathbb{C}[\mathrm{GL}_N]$-representation, $V^{\otimes n}$ decomposes as

$$V^{\otimes n} \cong \bigoplus_{\lambda \vdash n} V_\lambda \otimes L_\lambda,$$

where V_λ is the usual *Specht module* of S_n and

$$L_\lambda = \mathrm{Hom}_A(V_\lambda, V^{\otimes n})$$

is zero or an irreducible GL_N-representation. Also, $L_\lambda \not\cong L_\mu$ if $L_\lambda \neq 0$ and $L_\mu \neq 0$ and $\lambda \neq \mu$.

We have $L_\lambda \neq 0$ if and only if λ has at most N nonzero parts.

10 Field extensions

A *homomorphism* of fields is a ring homomorphism from one field to another.

Every field homomorphism is injective.

A *field extension* of a field K, or *K-extension*, is an (injective) field homomorphism $K \hookrightarrow M$.

This injection makes M into a K-vector space. We write $M \mid K$ for the extension $K \hookrightarrow M$.

The extension is *finite* if $[M : K] = \dim_K(M)$ is finite.

A homomorphism from one field extension $M \mid K$ to another field extension $M' \mid K$ is a field homomorphism $M \to M'$ (which is necessarily injective), which makes this diagram commute:

$$\begin{tikzcd} K \arrow[r] \arrow[dr] & M \arrow[d] \\ & M' \end{tikzcd}$$

Let $\mathrm{Aut}_K(M)$ be the group of isomorphisms of field extensions $M \mid K \to M \mid K$.

11 Algebraic extensions and separable extensions

Let $M \mid K$ be a field extension and let $a \in M$. The *annihilator* of a is

$$\mathrm{Ann}(a) = \{P(x) \in K[x] : P(a) = 0\}$$

The element a is *transcendental* over K if $\mathrm{Ann}(a) = 0$.

We say that a is *algebraic* over K if $\mathrm{Ann}(a) \neq 0$.

A field extension $M \mid K$ is *algebraic* if for all $a \in M$ the element a is algebraic over K.

If a is algebraic over K, then there is a unique monic polynomial which generates $\mathrm{Ann}(a)$.

We denote this by m_a and call it the *minimal polynomial* of a.

A polynomial $P(x) \in K[x]$ *has no multiple roots* if $(P(x), P'(x)) = K[x]$.

A polynomial in $K[x] \setminus \{0\}$ is *separable* if all of its irreducible factors have no multiple roots.

An algebraic field extension $L \mid K$ is *separable* if the min. pol. over K of any element of L is separable.

12 Simple extensions and splitting extensions

Let $\iota : K \to M$ be a field extension and let $S \subseteq M$ be a subset.

The *field generated by S over K* is the subfield $K(S) \subseteq M$ defined as the intersection of all subfields of M containing both S and $\iota(K)$.

The elements of S are called *generators* of $K(S)$ over K.

$M \mid K$ is a *simple extension* if there is an element $m \in M$ such that $M = K(m)$.

Let K be a field and let $P(x) \in K[x]$ be a polynomial.

The polynomial $P(x)$ *splits* in K if for some elements $c, a_1, a_2, \ldots, a_n \in K$ we have

$$P(x) = c \cdot (x - a_1) \cdot (x - a_2) \cdots (x - a_n).$$

A field extension $M \mid K$ is a *splitting extension* (or *splitting field*) for $P(x) \in K[x]$ if

(1) $P(x)$ splits in M, and

(2) M is generated over K by the roots of $P(x)$ in M.

Theorem. There exists a field extension $M \mid K$ that is a splitting extension for any $P(x) \in K[x]$. This is unique up to isomorphism.

Theorem. Suppose $L \mid K$ is a splitting extension for $P(x)$ and $J \mid K$ is any K-extension. Then the images of all the homomorphisms of K-extensions $L \hookrightarrow J$ coincide.

13 Normal extensions

An algebraic field extension $L \mid K$ is *normal* if the min. pol. over K of any element of L splits in L.

Theorem. Suppose $L \mid K$ is a finite field extension. Then the following are equivalent:

(a) The extension $L \mid K$ is normal.

(b) The extension $L \mid K$ is a splitting extension for a polynomial with coefficients in K.

Theorem. Let $L \mid K$ be the splitting field of a separable polynomial over K. Then $\#\mathrm{Aut}_K(L) = [L : K]$.

Theorem. Let $\iota : K \hookrightarrow L$ be a finite field extension.

Then $\mathrm{Aut}_K(L)$ is finite. Furthermore, the following statements are equivalent:

(i) It holds that $\iota(K) = L^{\mathrm{Aut}_K(L)}$ where $L^G = \{a \in L : g(a) = a \text{ for all } g \in G\}$.

(ii) The extension $L \mid K$ is normal and separable.

(iii) The extension $L \mid K$ is a splitting extension for a separable polynomial with coefficients in K.

A field extension with the equivalent properties in the theorem is called a *finite Galois extension*.

14 Fundamental theorem of Galois extensions

A general field extension $\iota : K \hookrightarrow L$ is a *Galois extension* if $L^{\mathrm{Aut}_K(L)} = \iota(K)$.

The *Galois group* of a Galois extension $L \mid K$ is $\mathrm{Gal}(L \mid K) := \mathrm{Aut}_K(L)$.

Theorem. Let $\iota : K \hookrightarrow L$ be a finite Galois extension.

(i) The map $M \mapsto \mathrm{Gal}(L \mid M)$ is a bijection

$$\{\text{subfields } M \text{ of } L \text{ containing } \iota(K)\} \mapsto \{\text{subgroups of } \mathrm{Gal}(L \mid K)\}.$$

Its inverse is given by the map $H \mapsto L^H$ where H is a subgroup of $\mathrm{Gal}(L \mid K)$.

(ii) Let M be a subfield of L containing $\iota(K)$. Then $[L:M] = |\operatorname{Gal}(L \mid M)|$ and $[M:K] = \frac{|\operatorname{Gal}(L|K)|}{|\operatorname{Gal}(L|M)|}$.

(iii) Let M be a subfield of L containing $\iota(K)$.

Then $M \mid K$ is a Galois extension if and only if $\operatorname{Gal}(L \mid M)$ is a normal subgroup of $\operatorname{Gal}(L \mid K)$.

15 Radical extensions

Let $L \mid K$ be a finite field extension.

The extension $L \mid K$ is *radical* if $L = K(\alpha_1, \dots, \alpha_k)$ for some elements $\alpha_i \in L$ such that

$$\alpha_1^{n_1} \in K, \qquad \alpha_2^{n_2} \in K(\alpha_1), \qquad \alpha_3^{n_3} \in K(\alpha_1, \alpha_2), \qquad \dots, \qquad \alpha_k^{n_k} \in K(\alpha_1, \dots, \alpha_{k-1})$$

for some positive integers $n_1, \dots, n_k > 0$.

Let $P(x) \in K[x]$ and suppose $L \mid K$ is a splitting extension for $P(x)$.

The polynomial $P(x)$ is *solvable by radicals* if there is an extension $M \mid L$ such that $M \mid K$ is radical.

Theorem. Assume $\operatorname{char}(K) = 0$. Then a polynomial $P(x) \in K[x]$ is solvable by radicals if and only if the group $\operatorname{Gal}(L \mid K)$ is *solvable* in the sense of having a finite filtration

$$\{1\} = G_0 \subseteq G_1 \subseteq \dots \subseteq G_n = \operatorname{Gal}(L \mid K)$$

with $G_i \lhd G_{i+1}$ and G_{i+1}/G_i abelian for all i.

Theorem. When $K = \mathbb{Q}$, every polynomial in $\mathbb{Q}[x]$ of degree ≤ 4 is solvable by radicals.

However, there exist polynomials in $\mathbb{Q}[x]$ of degree ≥ 5 that are not solvable by radicals.

Theorem. The field $\mathbb{C}$, defined as the splitting field of $x^2 + 1$ over $\mathbb{Q}$, is algebraically closed.