Introduction to representation theory
Lecture 5

Alexei KOTOV

University of Hradec Králové
Faculty of Science

July 23, 2021, Hradec Kralove

Plan of the lecture

(1) Recollection of facts and notations.

(2) Examples of non-semisimple modules.

(3) Canonical filtration of modules.

(4) Composition series.

(5) Modules over finite groups.

(6) Group rings and algebras.

(7) Decomposition of group algebras.

Let is recollect some important definitions and statements from the previous two lectures.

Rings and algebras.

- (*) A ring (an algebra) is simple if it does not contain nontrivial ideals;
- (*) semisimple if it is a direct sum of simple subalgebras $\Longleftrightarrow$ a direct sum of simple (minimal) ideals.

General problem in representation theory.

- (*) Classify representations/modules over a group (ring, algebra) up to isomorphisms.

Modules.

(*) A module is called simple if it does not contain non-trivial submodules; such a representation is called irreducible.

(*) Schur's Lemma: any morphism between simple modules is either an isomorpism or zero. The set of endomorphisms of a simple module (the commutant of an irreducible representation) is a division ring (algebra).

(*) A module is called semisimple if any of the following three equivalent properties holds:

  (i) it is a sum of simple submodules,
  (ii) it is a direct sum of simple submodules,
  (iii) every its submodule is a direct summand.

(*) The decomposition into the direct sum of simple modules, semisimple decomposition, is unique up to isomorphisms.

(*) Any submodule of a semisimple module is semisimple.

(*) A module V over a ring $\mathcal{R}-$ is called faithful, if $\mathcal{R} \to \mathrm{End}_k(V)$ is injective.

Theorem (Wedderburn).

Let V be a simple faithful module over $\mathcal{R}$, D be the commutant. Then $\mathcal{R} = \mathrm{End}_D(V)$.

Corollary.

(i) Every simple finite-dimensional k$-$algebra $\mathcal{A}$ is isomorphic to a matrix algebra over some division k$-$algebra.

(ii) In particular, if k is algebraically closed then $\mathcal{A}$ is isomorphic to $M_n(k)$ for some n.

Not every module is semisimple.

Examples.

- Take $\mathcal{M} = \mathbb{Z}$ as a module over $\mathcal{R} = \mathbb{Z}$, $\mathcal{N} = 2\mathbb{Z}$ as a submodule. The quotient module is $\mathbb{Z}_2 = \mathbb{Z}/2\mathbb{Z}$.

  All elements of the quotient have order 2. On the other hand, every non-zero element of $\mathbb{Z}$ is of infinite order, thus the embedding $\mathbb{Z}_2 \subset \mathbb{Z}$ is not possible and $2\mathbb{Z} \subset \mathbb{Z}$ is not a direct summand.

- $\mathcal{R} = \mathrm{k}[\mathrm{x}]$ for a field k, $\mathcal{M} = \mathrm{k}[\mathrm{x}]$, $\mathcal{N} = \mathrm{x}^2\mathrm{k}[\mathrm{x}]$.

  The image of x under the projection map $\mathcal{M} \to \mathcal{M}/\mathcal{N}$ is annihilated by the action of x. $\mathcal{M}$ does not possess elements with this property, therefore the embedding of the quotient into $\mathcal{M}$ is not possible and hence $\mathcal{N}$ is not a direct summand.

- $\mathcal{R} = \mathbb{C}[\mathrm{x}]$, $\mathrm{V} = \mathbb{C}^2$, such that

$$\mathrm{x} \mapsto \mathrm{A} = \begin{pmatrix} \lambda & 1 \\ 0 & \lambda \end{pmatrix}, \quad \lambda \in \mathbb{C}$$

  $\mathrm{W} = (\mathbb{C}, \lambda)$ is a submodule (the generator x acts by multiplication on λ). The quotient module is again $(\mathbb{C}, \lambda)$.

  If W was a direct summand then A would have been conjugated to $\lambda\,\mathrm{id}$, which is not the case.

  Here we have a filtration of the module by submodules

$$0 \subset (\mathbb{C}, \lambda) \subset \mathbb{C}^2 \to (\mathbb{C}, \lambda) \to 0$$

  such that each quotient is simple.

  Notice that $(\mathbb{C}, \lambda)$ is the only simple submodule of $\mathbb{C}^2$

Proposition.

For any module V, there is a canonical ascending filtration by submodules

$$\{0\} \subset V_{(0)} \subset V_{(1)} \subset V_{(2)} \subset \ldots \subset V_{(r)} \subset \ldots \subset V$$

such that each quotient module $V_{(i)}/V_{(i-1)}$ is semisimple.

Proof.

(1) Let $V_{(0)}$ be the sum of all simple submodules, i.e. each vector in $V_{(0)}$ is a finite sum of elements, belonging to one of the simple submodules. It is semisimple.

(2) Repeat the same procedure for the quotient module $V/V_{(0)}$: take the sum of all its simple submodules; $V_{(1)}$ is the preimage of the latter under the projection map $V \to V/V_{(0)}$.

(3) Continue by induction.

Remark.

The quotients of the canonical filtration does not determine the representation uniquely: there might exist modules V and V', such that $V_{(i)}/V_{(i-1)} \simeq V'_{(i)}/V'_{(i-1)}$ for for all i, but V and V' are not isomorphic.

Example (two non-isomorphic representations with isomorphic quotients).

Any representation of the ring of polynomials of two variables $\mathcal{R} = k[x, y]$ on a $k-$vector space V is uniquely determined by the image of generators B and C, such that $x \mapsto B$, $y \mapsto C$ and

$$k[x, y] \ni p(x, y) \mapsto p(B, C) \in End(V)$$

The only requirement: B and C must commute.

Consider $\mathcal{R}-$modules $(\mathrm{k}^2, \mathrm{B}_\alpha, \mathrm{C}_\alpha)$, $\alpha = 1, 2$, with

$$\mathrm{B}_1 = \begin{pmatrix} \lambda_1 & 0 \\ 0 & \lambda_1 \end{pmatrix}, \quad \mathrm{B}_2 = \begin{pmatrix} \lambda_1 & 1 \\ 0 & \lambda_1 \end{pmatrix}$$

$$\mathrm{C}_1 = \begin{pmatrix} \lambda_2 & 1 \\ 0 & \lambda_2 \end{pmatrix}, \quad \mathrm{C}_2 = \begin{pmatrix} \lambda_2 & 0 \\ 0 & \lambda_2 \end{pmatrix}$$

for distinct $\lambda_1, \lambda_2 \in \mathrm{k}$.

All quotient modules associated to the canonical filtration in both cases are isomorphic to $(\mathrm{k}, \lambda_1, \lambda_2)$, where

$$\mathrm{k}[\mathrm{x}, \mathrm{y}] \ni \mathrm{p}(\mathrm{x}, \mathrm{y}) \mapsto \mathrm{p}(\lambda_1, \lambda_2) \in \mathrm{M}_1(\mathrm{k}) \simeq \mathrm{k}$$

However, the two representations of $\mathcal{R}$ are not isomorphic: B_1 is a scalar multiplier of the identity, while B_2 is not, so these operators can not be conjugated by any module isomorphism.

Irreducible representations of the algebra of polynomials over an algebraically closed field.

Any irreducible finite-dimensional representation of $k[x_1, \ldots, x_n]$ is of the above form.

Indeed, let A_i be the generators, such that $x_i \mapsto A_i$, $i = 1, \ldots, n$. We require that all A_i are commuting.

Take the space V_{λ_1} of eigenvectors for A_1 corresponding to an eigenvalue λ_1; since A_1 and A_j, $j = 2, \ldots, n$ are commuting, every A_j preserves V_{λ_1}.

Take the subspace $V_{\lambda_1 \lambda_2} \subset V_{\lambda_1}$ of eigenvectors for A_2 in V_{λ_2} corresponding to some eigenvalue λ_2 of A_2 and then proceed by induction.

At the end of day we obtain the joint eigenspace $V_{\lambda_1 \ldots \lambda_n}$, which is the direct sum of simple modules $(\mathbb{C}^1, \lambda_1, \ldots, \lambda_n)$, on which every x_i acts by multiplication on λ_i.

Definition.

A series for a module $\mathcal{M}$ is a strictly decreasing sequence of submodules

$$\mathcal{M} = \mathcal{M}_0 \supset \mathcal{M}_1 \supset \ldots \supset \mathcal{M}_{\mathrm{n}} = \{0\}$$

beginning with $\mathcal{M}$ and finishing with $\{0\}$.

The length of this series is n. In general, the length is allowed to be infinite.

A composition series is a series in which no further submodule can be inserted. This is equivalent to saying each composition factor (the quotient module) $\mathcal{M}_{\mathrm{i}}/\mathcal{M}_{\mathrm{i+1}}$ is simple.

Given a composition series F for a module $\mathcal{M}$, denote by $\mathrm{S}(\mathrm{M}, \mathrm{F})$ the set of all (not necessarily distinct) simple factors. Then the length of the series is the cardinal number of $\mathrm{S}(\mathcal{M}, \mathrm{F})$:

$$\mathrm{l}(\mathcal{M}, \mathrm{F}) = |\,\mathrm{S}(\mathcal{M}, \mathrm{F})\,|$$

Let $\mathcal{N} \subset \mathcal{M}$ be a submodule, $\mathcal{L} = \mathcal{M}/\mathcal{N}$ be the quotient module.

Consider the following decreasing filtrations, induced by F:

$$\mathcal{N}_\mathrm{i} = \mathcal{N} \cap \mathcal{M}_\mathrm{i}, \quad \mathcal{L}_\mathrm{i} = \mathrm{im}\,(\mathcal{M}_\mathrm{i} \to \mathcal{L} = \mathcal{M}/\mathcal{N})$$

It is possible that $\mathcal{N}_\mathrm{i} = \mathcal{N}_\mathrm{i+1}$ or $\mathcal{L}_\mathrm{i} = \mathcal{L}_\mathrm{i+1}$ for some i.

By getting rid of repeated submodules, we obtain two series F_N and F_L for $\mathcal{N}$ and $\mathcal{L}$, respectively.

Proposition.

(i) F_N and F_L are composition series.

(ii) $S(F, \mathcal{M}) = S(F_N, \mathcal{N}) \cup S(F_L, \mathcal{L})$

Proof.

There is a short exact sequence of modules for each admissible i

$$0 \to \mathcal{N}_i/\mathcal{N}_{i+1} \to \mathcal{M}_i/\mathcal{M}_{i+1} \to \mathcal{L}_i/\mathcal{L}_{i+1} \to 0$$

Each factor $\mathcal{M}_i/\mathcal{M}_{i+1}$ is simple, thus by Schur's Lemma either

$$\mathcal{N}_i/\mathcal{N}_{i+1} = 0, \quad \mathcal{M}_i/\mathcal{M}_{i+1} \simeq \mathcal{L}_i/\mathcal{L}_{i+1}$$

or

$$\mathcal{N}_i/\mathcal{N}_{i+1} \simeq \mathcal{M}_i/\mathcal{M}_{i+1}, \quad \mathcal{L}_i/\mathcal{L}_{i+1} = 0$$

Therefore all factors in F_N and F_L are simple and (ii) holds true.

Lemma.

Assume that $\mathcal{M}$ is a semisimple module with a finite semisimple decomposition. Then:

- There is a finite composition series of $\mathcal{M}$.
- Every composition series is of such a form for some semisimple decomposition.

Proof.

- Assume that $\mathcal{M}$ is a direct sum of simple submodules $\{S_0, \ldots, S_{n-1}\}$. Take the following decreasing filtration

$$\mathcal{M}_0 = \bigoplus_{j=0}^{n-1} S_i \supset \mathcal{M}_1 = \bigoplus_{j=1}^{n-1} S_i \supset \ldots \supset \mathcal{M}_{n-1} = S_{n-1} \supset \mathcal{M}_n = 0$$

By construction, every factor is simple, $\mathcal{M}_i/\mathcal{M}_{i+1} = S_i$ for $i = 0, \ldots, n-1$, hence it is a composition series.

- If $\mathcal{M}$ is semisimple, any submodule is a direct summand, thus every composition series splits: denote $S_i = \mathcal{M}_i/\mathcal{M}_{i+1}$ for $i = 0, \ldots, n-1$, then

$$\mathcal{M}_i = \mathcal{M}_{i+1} \oplus S_i$$

  Therefore we obtain a decomposition of $\mathcal{M}$ into the direct sum of simple submodules $\{S_0, \ldots, S_{n-1}\}$, such that the composition series is of the above form.

Definition.

We will say the canonical increasing filtration of a module is finite if the number of all simple direct summands, which appear in semisimple decomposition of factors, is finite. We call them associated simple factors.

Proposition.

(i) The canonical increasing filtration of a module is finite if and only if the module admits a composition series of finite length.

(ii) Then there is a one-to-one correspondence between simple factors of the composition series and associated simple factors of the canonical filtration.

Proof.

Assume that the canonical decomposition is finite. Then one can built up a finite composition series out of the canonical filtration with the required property (ii).

We start with a composition series for a semisimple submodule $\mathcal{M}_{(0)}$ as in the above lemma.

The next step - we enrich the obtained decreasing filtration by adding of modules from the "next levels".

Eg. assume that S is a direct summand of a semisimple decomposition for the quotient $\mathcal{M}_{(1)}/\mathcal{M}_{(0)}$. Then we add its preimage under the projection map $\pi_{(1)}$ of $\mathcal{M}_{(1)}$ onto the quotient $\mathcal{M}_{(1)}/\mathcal{M}_{(0)}$

$$\pi^{-1}(\mathrm{S}) \supset \mathcal{M}_{(0)}$$

and then continue by induction until we get a decreasing filtration of $\mathcal{M}$ with all simple factors.

If there exists a composition series F of $\mathcal{M}$ of finite length n, we shall prove by induction that the canonical filtration is finite and (ii) is satisfied. The canonical filtration of $\mathcal{M}$ induces the canonical filtration of the quotient by $\mathcal{M}/\mathcal{M}_{(0)}$.
Now it is sufficient to consider the associated composition series for $\mathcal{M}_{(0)}$ and $\mathcal{M}/\mathcal{M}_{(0)}$ and use the induction hypothesis, as the length of the induced composition series of submodules is strictly less than the length of the composition series of the whole module.

Corollary.

If the composition series F is finite, then

(i) $\mathrm{S}(\mathcal{M}, \mathrm{F})$ and $\mathrm{l}(\mathcal{M}, \mathrm{F})$ are independent on the choice of composition series. This allows us to omit the letter F in the corresponding notations.

(ii) For any submodule $\mathcal{N} \subset \mathcal{M}$ one has

$$\mathrm{S}(\mathcal{M}) = \mathrm{S}(\mathcal{N}) \cup \mathrm{S}(\mathcal{L}), \quad \mathrm{l}(\mathcal{M}) = \mathrm{l}(\mathcal{N}) + \mathrm{l}(\mathcal{L})$$

Modules over finite groups

There are special classes of groups for which every linear representation decomposes into a direct sum of irreducible representations; in other words, any module is semisimple

$$\mathrm{V} = \bigoplus_{\rho \in \mathrm{Irrep(G)}} \mathrm{r}_\rho \mathrm{V}_\rho, \quad \mathrm{r}_\rho \in \mathbb{Z}_{\geq 0}$$

Finite groups (compact groups, in general) are of this type.

Orthogonal and unitary representations

Let V be a real orthogonal (a unitary) G−module, i.e. V is a Euclidean (Hermitian) vector space, such that G acts by orthogonal (unitary) linear transformations. Then the orthogonal complement to each submodule is again a submodule, which implies that the module is semisimple.

Theorem.

Let $G = \{g_1, \dots, g_n\}$ be a finite group and V be a real (complex) linear $G-$module of finite dimension. Then there exists a $G-$invariant Euclidean (Hermitian) scalar product on V, i.e. a positive definite symmetric bilinear (sesquilinear) form

$$(\,,\,)\colon V \times V \to V$$

such that $(gv_1, gv_2) = (v_1, v_2)$, for all $g \in G$, $v_1, v_2 \in V$.

Proof.

Step 1. Take any Euclidean (Hermitian) scalar product on V. It is not $G-$invariant, in general.

Step 2. Replace $(\,,\,)$ with a new scalar product $(\,,\,)_G$

$$(v_1, v_2)_G = \frac{1}{n} \sum_{g \in G} (gv_1, gv_2), \quad \forall v_1, v_2 \in V$$

The obtained scalar product is:

(a) Positive definite. Indeed, for each non-zero v, $(v, v) > 0$. The sum of positive numbers is again greater than 0, therefore $(v, v)_G > 0$.

(b) G−invariant: for any $g' \in G$, $v_1, v_2 \in V$, one has

$$(g'v_1, g'v_2)_G = \frac{1}{n}\sum_{g \in G}(gg'v_1, gg'v_2) = \frac{1}{n}\sum_{g \in G}(gv_1, gv_2)$$

since the sets $\{gg' \mid g \in G\}$ and $\{g \mid g \in G\}$ coincide. Hence

$$(g'v_1, g'v_2)_G = (v_1, v_2)_G$$

Corollary.

Every real (complex) linear representation of a finite group is orthogonal (unitary) with respect to some metric.

Definition.

For any module V over a finite group G, there is an operator

$$V \ni v \mapsto \mathrm{Tr}_G(v) = \frac{1}{|G|} \sum_{g \in G} gv$$

called the averaging over elements of G.

Lemma.

Tr_G is a projector onto the submodule of G−invariant vectors.

Proof.

We use the trick as above to show that $\mathrm{Tr}_G(v)$ is G−invariant for any $v \in V$.
If v is already an invariant vector, then

$$\mathrm{Tr}_G(v) = \frac{1}{|G|} \sum_{g \in G} gv = \frac{1}{|G|} \sum_{g \in G} v = v$$

thus Tr_G is a projector onto $V^G = \{v \in V \mid gv = v, \forall g \in G\}$

Example.

V is a module over a group G.

G acts on k−linear maps V → V by conjugation:

$$g\psi = g \circ \psi \circ g^{-1} \quad g \in G, \psi \in \mathrm{End}_k(V)$$

This action obviously respects the composition of maps, i.e.

$$g(\psi_1 \circ \psi_2) = g(\psi_1) \circ g(\psi_2), \quad \psi_1, \psi_2 \in \mathrm{End}_k(V)$$

By construction, a linear map ψ is G−invariant, $\psi \in \mathrm{End}_k(V)^G$, if and only if it commutes with all elements of G:

$$g\psi = \psi \iff g \circ \psi \circ g^{-1} = \psi \iff g \circ \psi = \psi \circ g$$

Theorem (Maschke).

Every finite-dimensional representation of a finite group G over a field k with characteristic not dividing the order of G is semisimple

Proof.

Let V be a G−module, W be a submodule. Denote by σ the inclusion map $W \hookrightarrow V$. It is a morphism of G−modules.

Take any complementary vector subspace $W' \subset V$ and denote by π the corresponding projection onto W. One has $\pi \circ \sigma = \mathrm{Id}_W$.

In general, W' is not a submodule. Replace π with $\phi = \mathrm{Tr}_G(\pi)$; now ϕ is G−invariant, thus it is a morphism of G−modules.

ϕ is not necessarily a projector, but $\mathrm{Ker}\phi$ is a submodule of V and, moreover, it is a complement to W, since $\mathrm{Tr}_G(\sigma) = \sigma$ and

$$\phi \circ \sigma = \mathrm{Tr}_G(\pi) \circ \sigma = \mathrm{Tr}_G(\pi \circ \sigma) = \mathrm{Id}_W$$

Example.

$G = \mathbb{Z}_2$. A module over G is in one-two-one correspondence with a vector space together with a linear operator J subject to the relation $J^2 = \mathrm{Id}$ (it is called a product structure on V).

For any $v \in V$ (V is over a field, the characteristic of which must not divide 2),

$$\mathrm{Tr}_G(v) = \frac{1}{2}(v + Jv)$$

Now $V = V_+ \oplus V_-$ such that $J_{|V_\pm} = \pm \mathrm{Id}$.

The corresponding decomposition of any vector $v \in V$ is

$$v = v_+ + v_- , \quad \text{where} \quad v_\pm = \frac{1}{2}(v \pm Jv)$$

Here $V_+ = V^G$ and V_- is its complement.

Let G be a group, $\mathcal{R}$ be a ring. The group ring $\mathcal{R}[G]$ is the direct sum

$$\mathcal{R}[G] = \bigoplus_{g \in G} \mathcal{R}g = \{\sum_{g \in G} a_g g \,|\, a_g \in \mathcal{R}, \forall g \in G\}$$

such that only a finite number of a_g are not equal to zero, together with an $\mathcal{R}-$bilinear operation $\mathcal{R}[G] \times \mathcal{R}[G] \to \mathcal{R}[G]$, extending the multiplication in G, i.e.

$$\left(\sum_{g \in G} a_g g\right)\left(\sum_{g' \in G} b_{g'} g'\right) = \sum_{g \in G} \sum_{g' \in G} a_g b_{g'} g g'$$

for all $a_g, b_g \in \mathcal{R}$ or, equivalently,

$$\left(\sum_{g \in G} a_g g\right)\left(\sum_{g' \in G} b_{g'} g'\right) = \sum_{g \in G} \left(\sum_{h \in G} a_h b_{h^{-1}g}\right) g$$

Theorem.

$\mathcal{R}[G]$ is a ring over $\mathcal{R}$. If $\mathcal{R}$ is unital, then so is $\mathcal{R}[G]$.

Proof.

The associativity of $\mathcal{R}[G]$ follows from the associativity of G and $\mathcal{R}$. The unit (identity) in $\mathcal{R}[G]$ is 1e, whenever $1 \in \mathcal{R}$.

Example.

$G = \mathbb{Z}_2$ with elements $\{e, \sigma\}$, such that $\sigma^2 = e$. Now $\mathcal{R}[G] = \{ae + b\sigma \,|\, a, b \in \mathcal{R}\}$ with multiplication

$$(ae + b\sigma)\,(a'e + b'\sigma) = (aa' + bb')e + (ab' + ba')\sigma$$

for all $a, b, a', b' \in \mathcal{R}$. The algebra is commutative (unital) if and only if so is $\mathcal{R}$.

Assume, $\mathcal{R}$ is unital and it contains $\frac{1}{2}$. Introduce another basis

$$\mathrm{t}_\pm = \frac{1}{2}\left(\mathrm{e} \pm \sigma\right)$$

Every element $\mathrm{a} \in \mathcal{R}[\mathrm{G}]$ decomposes as $\mathrm{a} = \mathrm{a}_+\mathrm{t}_+ + \mathrm{a}_-\mathrm{t}_-$ for some $\mathrm{a}_\pm \in \mathcal{R}$.
Taking into account that

$$(\mathrm{t}_\pm)^2 = \mathrm{t}_\pm, \quad \mathrm{t}_+\mathrm{t}_- = \mathrm{t}_-\mathrm{t}_+ = 0$$

and thus

$$\left(\mathrm{a}_+\mathrm{t}_+ + \mathrm{a}_-\mathrm{t}_-\right)\left(\mathrm{a}'_+\mathrm{t}_+ + \mathrm{a}'_-\mathrm{t}_-\right) = \left(\mathrm{a}_+\mathrm{a}'_+\right)\mathrm{t}_+ + \left(\mathrm{a}_-\mathrm{a}'_-\right)\mathrm{t}_-$$

for all $\mathrm{a}_\pm, \mathrm{a}'_\pm \in \mathcal{R}$, we obtain an isomorphism of associative commutative algebras

$$\mathcal{R}[\mathrm{G}] \simeq \mathcal{R} \oplus \mathcal{R}$$

Theorem.

There is a one-to-one correspondence between k−linear representations of k[G] and G for any field k.

Proof.

We take into account that G is a multiplicative subset of the group algebra k[G] and k[G] is generated by G over k.

Examples.

(*) If $G = \mathbb{Z}^m$, then for each $\mathcal{R}$, $\mathcal{R}[G]$ is isomorphic to $\mathcal{R}[x_1, x_1^{-1}, \ldots, x_m, x_m^{-1}]$, the ring of Laurent polynomials with coefficients in $\mathcal{R}$. For $\mathcal{R} = k$, k−linear representations are uniquely determined by the image of the generators, i.e. by the set of commuting k−linear invertible maps $\{A_i\}_{i=1}^{m}$, such that $x_i \mapsto A_i$, $x_i^{-1} \mapsto A_i^{-1}$ for all $i = 1, \ldots, m$.

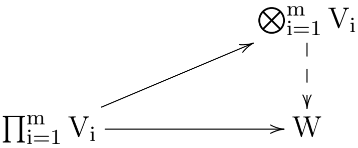
(*) Recall that the latter is true for k−linear representations of $k[x_1, \ldots, x_k]$, except A_i are not required to be invertible.

Tensor products

Let $V_1, \ldots, V_m$ be $k-$linear vector spaces. The tensor product

$$\bigotimes_{i=1}^{m} V_i = V_1 \otimes \ldots \otimes V_m$$

is a vector space together with a universal multilinear map $\prod_{i=1}^m V_i \to \bigotimes_{i=1}^m V_i$, which satisfies the following property: for any other vector space W and a multilinear map $\prod_{i=1}^m V_i \to W$, there exists a unique linear map $\bigotimes_{i=1}^m V_i \to W$, such that the following diagram is commutative



If V_i are finite-dimensional, then

- $$\mathsf{dim} \bigotimes_{i=1}^{m} V_i = \prod_{i=1}^{m} \mathsf{dim}\, V_i$$
- In particular, if $\left(e^i_j\right)_{j=1}^{\mathsf{dim}\, V_i}$ is a basis of V_i for $i = 1, \ldots, m$, then $\left(e^1_{j_1} \otimes \ldots \otimes e^m_{j_m}\right)$ is a basis for $\bigotimes_{i=1}^m V_i$.
- The space of multilinear maps $\prod_{i=1}^m V_i \to W$ is isomorphic to $W \otimes \left(\bigotimes_{i=1}^m V_i^*\right)$, where V_i^* is the space of linear functions on V_i (the dual vector space).
- In particular,

$$\mathrm{Hom}_k(V, W) \simeq W \otimes V^*, \quad \mathrm{End}_k(V) \simeq V \otimes V^*$$

- If $\mathcal{A}_i$, $i = 1, \ldots, m$ are k−algebras, then $\bigotimes_{i=1}^m \mathcal{A}_i$ is also a k−algebra with the multiplication generated by

$$(a_1 \otimes \ldots a_m)(a'_1 \otimes \ldots a'_m) = (a_1 a'_1 \otimes \ldots a_m a'_m)$$

- If V_i are $\mathcal{A}_i$ modules, $\bigotimes_{i=1}^m V_i$ is a module over $\bigotimes_{i=1}^m \mathcal{A}_i$:

$$(a_1 \otimes \ldots a_m)(v_1 \otimes \ldots v_m) = (a_1 v_1 \otimes \ldots a_m v_m)$$

- The tensor product of G_i−modules is a $\prod_i G_i$−module

$$(g_1, \ldots g_m)(v_1 \otimes \ldots v_m) = (g_1 v_1 \otimes \ldots g_m v_m)$$

- If $G_i = G$ then $\bigotimes_{i=1}^m V_i$ is G−module thanks to the diagonal embedding $\Delta_m \colon G \hookrightarrow G \times \ldots \times G$.

Proposition.

Let V_i be simple $k-$linear finite-dimensional G_i-modules, where k is an algebraically closed field. Then $\bigotimes_{i=1}^m V_i$ is a simple $\prod_i G_i-$module.

Proof

It is sufficient to prove this statement for $m = 2$.

Choose a basis $(f_j)_{j=1}^{\dim V_2}$ for V_2. Then

$$V_1 \otimes V_2 = \bigoplus_{j=1}^{\dim V_2} V_1 \otimes f_j \simeq (\dim V_2)\, V_1$$

is a semisimple decomposition of $V_1 \otimes V_2$ as a G_1-module.

This means that any vector $v \in V_1 \otimes V_2$ decomposes as

$$v = \sum_{j=1}^{\dim V_2} v_j \otimes f_j$$

such that the correspondence $\phi_j \colon v \mapsto v_j \in V_1$ is a morphism of G_1-modules for all $j = 1, \ldots, m$.

Let $U \subset V_1 \otimes V_2$ be a simple G_1-submodule. Then it must be isomorphic to V_1 and, by Schur's Lemma, the restriction of ϕ_j to U are scalar multipliers of a fixed isomorphism. This implies that there exist constants $c_1, \ldots, c_m \in k$, such that $\forall u \in U$

$$u = \sum_{j=1}^{\dim V_2} c_j v_1 \otimes f_j = v_1 \otimes \left(\sum_{j=1}^{\dim V_2} c_j f_j \right)$$

where $v_1 \in V_1$ is uniquely associated to u.

Hence $U = V_1 \otimes L$, where L is a 1-dimensional subspace of V_2, spanned by the vector

$$v_2 = \left(\sum_{j=1}^{\dim V_2} c_j f_j \right)$$

Similarly, any G_1-submodule U' of $V_1 \times V_2$ is isomorphic to the direct sum of $r > 0$ copies of V_1, therefore there exists an $r-$dimensional vector subspace $W \subset V_2$, such that $U' = V_1 \otimes W$.

For any $g_2 \in G_2$, $v_1 \in V_1$, $w \in W$ one has

$$g_2 (v_1 \otimes w) = v_1 \otimes (g_2 w)$$

thus U' is G_2-invariant if and only if so is W, but then $W = V_2$ and U' coincides with the whole tensor product $V_1 \otimes V_2$.

Consider $k[G]$ as a module over $G \times G$, where

$$(h_1, h_2)\left(\sum_{g \in G} a_g g\right) = \sum_{g \in G} a_g \left(h_1 g h_2^{-1}\right)$$

Lemma.

I is an ideal (a simple ideal) of $k[G]$ if and only if it is a $G \times G-$submodule (a simple $G \times G-$submodule).

Proof.

It follows from the fact that $k[G]$ is generated by G.

It is worth mentioning that there is a canonical isomorphism of algebras

$$k[G \times G] \simeq k[G] \otimes k[G]$$

which associates (g_1, g_2) with $g_1 \otimes g_2$ for all $(g_1, g_2) \in G \times G$.

Given any $G-$module V, the space of $k-$linear endomorphisms of V, $End_k(V)$, is also a $G \times G-$module with the action

$$(h_1, h_2)\phi = h_1 \circ \phi \circ h_2^{-1}$$

Let us remark that this action is the same as the action of $G \times G$ on the tensor product $V \otimes V^*$.
Since V is a $k[G]-$module, there is a canonical morphism of algebras from $k[G]$ to $End_k(V)$.

Lemma.

The map $k[G] \to End_k(V)$ is a morphism of $G \times G-$modules.

Proof.

For any $v \in V$, one has

$$(h_1, h_2)\left(\sum_{g \in G} a_g g\right) v = \sum_{g \in G} a_g \left(h_1 g h_2^{-1}\right) v = h_1 \circ \left(\sum_{g \in G} a_g g\right) \circ h_2^{-1}(v)$$

Decomposition of the group algebra

Theorem.

Let G be a finite group and $\{V_\alpha\}$ be the collection of all its simple modules over k. Let $D_\alpha = \mathrm{End}_G(V_\alpha)$. Then

$$k[G] = \bigoplus_\alpha \mathrm{End}_{D_\alpha}(V_\alpha)$$

Proof.

First notice that, by the one-to-one correspondence between representations of G and k[G], a simple G−module V is also a simple k[G]−module. Since k[G] is finite-dimensional over k, k[G]v is a finite-dimensional submodule of V for any $v \in V$.

Thus every irreducible representation of a finite group must be finite-dimensional.

Since $\mathrm{G} \times \mathrm{G}$ is a finite group, any module over it is semisimple, thus so is $\mathrm{k}[\mathrm{G}]$. In particular, the kernel of $\mathrm{k}[\mathrm{G}] \to \mathrm{End}_{\mathrm{k}}(\mathrm{V})$ is a direct summand, that is, there exists a $\mathrm{G} \times \mathrm{G}-$submodule $\mathcal{A}_{\mathrm{V}}$ of $\mathrm{k}[\mathrm{G}]$, such that

$$\mathrm{k}[\mathrm{G}] = \mathcal{A}_{\mathrm{V}} \oplus \mathrm{Ker}\Big(\mathrm{k}[\mathrm{G}] \to \mathrm{End}_{\mathrm{k}}(\mathrm{V})\Big)$$

Notice that $\mathcal{A}_{\mathrm{V}}$ is an ideal of the group algebra.

By Wedderburn's theorem, if V is simple, then $\mathcal{A}_{\mathrm{V}} \simeq \mathrm{End}_{\mathrm{D}_\alpha}(\mathrm{V})$.

On the other hand, for two non-isomorphic simple modules V and V', there are no non-zero morphisms between $\mathcal{A}_{\mathrm{V}}$ and $\mathrm{End}_{\mathrm{k}}(\mathrm{V}')$ as, being regarded as $\mathrm{G}-$modules,

$$\mathcal{A}_{\mathrm{V}} \subset \mathrm{End}_{\mathrm{k}}(\mathrm{V}) = \mathrm{V}^{\mathsf{dim}\,\mathrm{V}}, \;\; \mathrm{End}_{\mathrm{k}}(\mathrm{V}') = (\mathrm{V}')^{\mathsf{dim}\,\mathrm{V}'}$$

Thus $\mathcal{A}_{\mathrm{V}}$ belongs to the kernel of $\mathrm{k}[\mathrm{G}] \to \mathrm{End}_{\mathrm{k}}(\mathrm{V}')$.

We obtain the following decomposition of k[G] into the direct sum of ideals corresponding to all simple G−modules V_α:

$$\mathrm{k[G]} = \bigoplus_\alpha \mathrm{End}_{\mathrm{D}_\alpha}(\mathrm{V}_\alpha) \oplus \bigcap_\alpha \Big(\mathrm{k[G]} \to \mathrm{End}_\mathrm{k}(\mathrm{V}_\alpha)\Big)$$

But the last summand is zero as, if $\mathrm{a} \in \mathrm{k[G]}$ acts as zero on any simple k[G]−module, then it acts as zero on any k[G]−module (since any module is semisimple, i.e. it is a direct sum of simple modules); this is not true for the left action of the element a on k[G] (eg. because a does not annihilate the identity).

Therefore

$$\mathrm{k[G]} = \bigoplus_\alpha \mathrm{End}_{\mathrm{D}_\alpha}(\mathrm{V}_\alpha)$$

The next lemma provides us with the explicit construction of the summand $\mathcal{A}(\mathrm{V})$ for each simple G−module V.

Lemma.

Define a $k-$linear map ψ from $End_k(V)$ to $k[G]$

$$\psi(A) = \sum_{g \in G} Tr(Ag^{-1})\, g \in k[G] \text{ for all } A \in End_k(V)$$

Then ψ is a morphism of $G \times G-$modules.

Proof.

$$Tr\left(\left(h_1 A h_2^{-1}\right) g^{-1}\right) = Tr\left(A\left(h_2^{-1} g^{-1} h_1\right)\right) = Tr\left(A\left(h_1^{-1} g h_2\right)^{-1}\right)$$

Denote $h = h_1^{-1} g h_2$, then

$$\psi(h_1 A h_2^{-1}) = \sum_{h \in G} Tr(Ah^{-1})\, h_1 h h_2^{-1} = h_1 \psi(A) h_2^{-1}$$

Corollary

(a) Let us restrict ψ to $\mathrm{End}_D(V)$; it is not zero, as there exist $g \in G$, $A \in \mathrm{End}_D(V)$, such that $\mathrm{Tr}(Ag^{-1}) \neq 0$ (eg. when A is equal to the image of g in $\mathrm{End}_D(V)$), which implies that at least one coefficient in the decomposition of $\psi(A) \in k[G]$ is not 0 and hence $\psi(A) \neq 0$.
Therefore ψ is a monomorphism.

(b) $k[G]$ is the direct sum of simple ideals

$$k[G] = \bigoplus_{\alpha} \psi\Big(\mathrm{End}_{D_\alpha}(V_\alpha)\Big)$$

where the sum is taken over the set of all non-isomorphic simple $G-$modules.

(c)

$$|G| = \dim_k k[G] = \sum_{\alpha} (\dim_k D_\alpha)\left(\dim_{D_\alpha} V_\alpha\right)^2$$