Aspects of Algebra

Abhijnan Rej

Lectures at the Institute of Mathematics & Applications

Bhubaneswar 2012

Preface

In the Fall of 2010 and 2011, I taught an introductory course on Lie groups and representation theory at the Institute of Mathematics and Applications, Bhubaneswar. The course was cataloged as "Algebra IV", an equivalent of a senior year topics course in a North American university. The students, having exposed to basic algebra in their previous semesters, were to be shown an interplay of algebra, geometry and analysis. Having been tasked with such an ambitious project, I presented a course in two parts: The first part was on all the algebra needed to state and prove fundamental yet accessible theorems in representation theory of finite groups (such as Frobenius reciprocity and Artin's theorem). The second part was a standard introduction to Lie groups. The bridge between these two parts, in my mind, was the Schur–Weyl duality relating representations of the symmetric and general linear groups.

What follows are lectures from the first part; the second part comprised of lectures from straight out of Brian Hall's Lie groups book and was therefore not written up. I have tried to cover

1. Some linear algebra,
2. Group actions on sets,
3. Basics of modules,
4. An introduction to the functorial language,
5. Tensor products and related notions, and finally
6. Some basic representation theory of finite groups.

I have freely borrowed from the existing literature, citing sources in the beginning of each "chapter". I learnt this material as an undergraduate and MS student at the University of Connecticut through lectures of K. Conrad, Kaufmann and Spiegel. As a mathematician working in adjacent areas I have also been greatly influenced by Atiyah–McDonald's *Commutative algebra*, S. Lang's *Algebra* and Serre's wonderful little book on linear representations of finite groups. All of these sources are very much present in my notes and, consequently, any claim to originality would be pointless vanity or worse.

I thank Professors Sudarshan Padhy and Swadheen Pattanayak of IMA Bhubaneswar for their interest in the courses and encouragement towards writing the lectures up.

Bhubaneswar
July 21 2012

Introduction and linear algebra review

Introduction to the course

Two objects:

- Lie group G: group + manifold with some “extra structure".
- Lie algebra $\mathfrak{g}$ associated to G: (sub)algebra of left-invariant vector fields on the manifold G.

Historically, they were (as the name gives away!) introduced by the Norwegian mathematician Sophus Lie in the 19th century as an infinitesimal description of group action!

Slogan: Smoothly varying family of symmetries!

Main idea: Galois studied symmetries of algebraic equations through groups. Lie studied symmetries of partial differential equations through groups!

Unifies almost all of mathematics and is the basis of contemporary particle physics!

I will focus on matrix Lie groups, specifically subgroups of $\mathrm{GL}(n,k)$ where the field k will be $\mathbb{R}$ or $\mathbb{C}$ and locally compact and compact groups.

Linear algebra: basic concepts

To begin with, we will study the following linear algebraic notions: For X an arbitrary matrix

1. the exponential map e^X, ($e^X e^Y \neq e^{X+Y}$),
2. the commutator $[X, Y] := XY - YX$ and the *tcb* $\mathrm{ad}_Y X = [X, Y]$,
3. $\mathrm{Ad}_A X := AXA^{-1}$,
4. and representations $\rho : G \to \mathrm{GL}(n, \mathbb{C})$, $\rho(g_1 g_2) = \rho(g_1)\rho(g_2)$ for $g_1, g_2 \in G$ some group.

Let $A \in M_n(\mathbb{C})$.
Definition 1. The characteristic polynomial is defined as

$$p(\lambda) := \det(A - \lambda I), \lambda \in \mathbb{C}.$$

Definition 2. We say that $A, B \in M_n(\mathbb{C})$ are similar if there exists an invertible matrix C such that

$$A = CBC^{-1}.$$

The map $B \mapsto CBC^{-1}$ is called conjugation.

A is diagonizable if A is similar to

$$\begin{pmatrix} a_1 & \cdots & 0 \\ \vdots & \ddots & \vdots \\ 0 & \cdots & a_n \end{pmatrix}$$

Definition 3. For $A \in M_n(\mathbb{C})$, the adjoint of A is

$$A^*_{kl} = \overline{A_{lk}}.$$

A self-adjoint if

$$A^* = A.$$

A is unitary if

$$A^* = A^{-1}.$$

A is normal if

$$AA^* = A^*A.$$

Definition 4. A is nilpotent if there exists $k \in \mathbb{N}$ such that

$$A^k = 0.$$

Let $A \in M_n(\mathbb{C})$. The trace of A is defined as

$$\operatorname{trace}(A) := \sum_{k=1}^{n} A_{kk}.$$

It is easy to show that $\operatorname{trace}(AB) = \operatorname{trace}(BA)$ and $\operatorname{trace}(CAC^{-1}) = \operatorname{trace}(C^{-1}CA) = \operatorname{trace}(A)$. Let $V_{\mathbb{C}}$ be a complex vector space. An inner product on $V_{\mathbb{C}}$ is a map

$$\boxed{\langle \cdot, \cdot \rangle : V_{\mathbb{C}} \to \mathbb{C}}$$

such that

1. $\langle v, u \rangle = \overline{\langle u, v \rangle}$ for all $u, v \in V_{\mathbb{C}}$,
2. $\langle u, v_1 + av_2 \rangle = \langle u, v_1 \rangle + a\langle u, v_2 \rangle$ for all $u, v_1, v_2 \in V_{\mathbb{C}}$ and $a \in \mathbb{C}$,
3. For all $v \in V_{\mathbb{C}}$, $\langle v, v \rangle \in \mathbb{R}$ and
$$\langle v, v \rangle \geq 0$$
with
$$\langle v, v \rangle = 0 \iff v = 0.$$

Example 5. Let $V_{\mathbb{C}} = M_n(\mathbb{C})$. Then define

$$\langle A, B \rangle := \mathrm{trace}(A^* B).$$

This is indeed an inner product (check!)

Let V be some vector space over a field k.

Definition 6. A linear functional V is some linear map $V \longrightarrow k$. If $v_1, \ldots, v_n$ is a basis of V then for each set of constants $a_1, \ldots, a_n$ there exists unique linear functional ϕ such that

$$\phi(v_k) = a_k.$$

The dual space of V is defined as

$$V^* := \mathrm{Hom}_k(V, k).$$

Caveat: $\dim V = \dim V^*$ and all finite dimensional vector spaces are isomorphic so may be tempted to think of V and V^* as the same. Be careful with this!

Definition 7. If $W \subset V$, then the annihilator subspace of W is defined as

$$W^\bullet := \{\phi \in V^* : \phi(w) = 0 \text{ for all } w \in W\}.$$

Check that

1. $W^\bullet \subset V^*$ is indeed a subspace,

2. $\dim W + \dim W^\bullet = \dim V$,

3. $\{\text{subspaces of } V\} \overset{1-1}{\leftrightarrow} \{\text{subspaces of } V^*\}$.

Definition 8 (Simultaneous eigenvectors and eigenvalues)**.** V some vector space and and $\mathcal{A}$ a set of linear operators on V. Then a simultaneous eigenvector for $\mathcal{A}$ is a nonzero $v \in V$ such that for all $A \in \mathcal{A}$, there exists a constant λ_A with

$$Av = \lambda_A v.$$

These constants λ_A are called simultaneous eigenvalues.

Definition 9. A weight for $A \in \mathcal{A}$ is a linear functional μ on $\mathcal{A}$ such that there exists $v \in V$ with

$$Av = \mu(A)v$$

for all $A \in \mathcal{A}$. For a given weight μ the set of all $v \in V$ satisfying $Av = \mu(A)v$ (for all $A \in \mathcal{A}$) is called the weight space associated to μ.

Definition 10. Elements of $\mathcal{A}$ are said to be simultaneously diagonalizable (s.d.) if there exists a basis $v_1, \ldots, v_n$ for V such that each v_k is a simultaneous eigenvector.

A very important consequence– elements of $\mathcal{A}$ are s.d. iff V can be decomposed as a direct sum of weight spaces.

Group actions on sets

The theory of Lie groups is concerned about the action of a Lie group on a manifold. We start with a much simpler and purely algebraic problem-

The action of a group on a *set*!

Main source/reference: Keith Conrad's "Group actions" (available from his UConn homepage)

Let S_n be the symmetric group in n elements. Concretely

$$S_n \text{ is the group of permutations of } \{1, 2, 3, \ldots, n\}.$$

Abstract definition:

$$\boxed{\mathrm{Sym}(X) \text{ is the set of all permutations of the elements of a set } X}$$

Clearly if $X = \{x_1, \ldots, x_n\}$, then can think of $\mathrm{Sym}(X)$ as S_n.

Theorem 11 (Cayley)**.** *Every finite group G can be embedded in a symmetric group.*

Proof. For all $g \in G$ define

$$\begin{array}{rcl} l_g : G & \to & G, \\ x & \mapsto & gx, \end{array}$$

for all $x \in G$. Since G is finite, l_g is a permutation with inverse $l_{g^{-1}}$. So $l_g \in \mathrm{Sym}(G)$. Now

$$\begin{array}{rcl} g_1(g_2 x) & = & (g_1 g_2)x, \\ \Longrightarrow l_{g_1} \circ l_{g_2} & = & l_{g_1 g_2}, \end{array}$$

so the map $g \mapsto l_g$ is a group homomorphism $G \to \mathrm{Sym}(G)$. This is 1-1 since g determines l_g ($l_g(e) = g$ where $e \in G$ identity.) So $g \mapsto l_g$ is an embedding

$$G \hookrightarrow \mathrm{Sym}(G)$$

as subgroups. □

Group actions basics

Definition 12. An **action** of a group G on a set X is a permutation $\pi_g : X \to X$ for each $g \in G$ such that

1. π_e is the identity: $\pi_e(x) = x$ for all $x \in X$.
2. For all $g_1, g_2 \in G$, $\pi_{g_1} \circ \pi_{g_2} = \pi_{g_1 g_2}$.

Example 13. S_n acts on $X = \{1, 2, \ldots, n\}$ by permutations: $\pi_\sigma(i) = \sigma(i)$, $\sigma : S_n \to S_n$.

Notational shift– write $\pi_g(x)$ simply as $g \cdot x$ or gx. This is the notation for the "effect of g on X and **not** multiplication of two different sets G and X.

Proposition 14. *Let G act on X. Then*

1. *If $x \in X$, $g \in G$ and $y = gx$ then $x = g^{-1}y$.*
2. *If $x \neq x'$ then $gx \neq gx'$.*

Proof. Homework! $\square$

Proposition 15. *Actions of the group G on the set X same as group homomorphism $G \to Sym(X)$.*

Proof. For all $g \in G$ we have a function

$$\begin{aligned} \pi_g : X &\to X, \\ x &\mapsto gx. \end{aligned}$$

(This follows from viewing gx as a function of x with **fixed** $g \in G$.)

$$\begin{aligned} ex = x &\implies \pi_e \text{ identity}, \\ g_1(g_2)x = (g_1 g_2)x &\implies \pi_{g_1} \circ \pi_{g_2} = \pi_{g_1 g_2}. \end{aligned}$$

Also π_g has an inverse– $\pi_{g^{-1}} \circ \pi_g = \pi_e$. Therefore $\pi_g \in \mathrm{Sym}(X)$ and $g \mapsto \pi_g$ is a homomorphism $G \to \mathrm{Sym}(X)$. Converse– let $f : G \to \mathrm{Sym}(X)$ be a group homomorphism. For all $g \in G$ we have a permutation $f(g)$ on X and $f(g_1 g_2) = f(g_1) \circ f(g_2)$. $\square$

Remark 16. View $f(g)$ acting on $x \in X$ as

$$g \cdot x = f(g)x.$$

This gives us a group action (following the fact that f is a group homomorphism.)

Important– Let $G \xrightarrow{f} \mathrm{Sym}(X)$ be a homomorphism

$$\ker f := \{g \in G : g \cdot x = x \forall x \in X\}.$$

This is the set of all trivial actions of G on X.
Example 17. Action of S_n on n-variables polynomials–

$$\sigma f(T_1, \ldots, T_n) = f(T_{\sigma(1)}, \ldots, T_{\sigma(n)}).$$

Example 18. Action of $\mathbb{R}^n$ by translations– for all $v \in \mathbb{R}^n$, let $T_v : \mathbb{R}^n \to \mathbb{R}^n$ be given by $w \mapsto w + v$. Then

$$\begin{aligned} T_0(w) &= w, \\ T_{v_1}(T_{v_2}(w)) &= T_{v_1+v_2}(w). \end{aligned}$$

These follow from the laws of vector addition.

Example 19. Action of S_n on $\mathbb{R}^n$ coordinate-wise– for all $\sigma \in S_n$ and a fixed $v = (c_1, \ldots, c_n) \in \mathbb{R}^n$, set

$$\sigma \cdot v = (c_{\sigma(1)}, \ldots, c_{\sigma(n)}).$$

Let $d_i = c_{\sigma(i)}$ and compute– for $\sigma' \in S_n$,

$$\begin{aligned} \sigma'(\sigma v) &= \sigma'(d_{\sigma'(1)}, \ldots, d_{\sigma'(n)}), \\ &= (c_{\sigma(\sigma'(1))}, \ldots, c_{\sigma(\sigma'(n))}), \\ &= (c_{(\sigma\sigma')(1)}, \ldots, c_{(\sigma\sigma')(n)}), \\ &= (\sigma\sigma')v \end{aligned}$$

but then $\sigma'\sigma = \sigma\sigma'$ so **not** an action. For a “real action" redefine

$$\begin{aligned} \sigma v &= (c_{\sigma^{-1}(1)}, \ldots, c_{\sigma^{-1}(n)}), \\ \Longrightarrow \sigma(\sigma' v) &= (\sigma\sigma')V. \end{aligned}$$

Example 20. Action of G on itself by conjugation– $X = G$ and, for $g, x \in G$,

$$gx = gxg^{-1}.$$

Check!

$$ex = exe^{-1} = x.$$

$$g_1(g_2x) = (g_1g_2)x.$$

Example 21. Let $H \subset G$ be a subgroup. Consider the left coset space

$$G/H = \{aH : a \in G\}.$$

Just think of G/H as a set. G acts on G/H by left multilpications–

$$g(aH) = gaH = \{gy : y \in aH\}.$$

Definition 22. A group action of G on X is called faithful or effective if different elements of G act on X in different ways: when $g_1 \neq g_2$, there exists $x \in X$ such that $g_1x \neq g_2x$.

Proposition 23. *The action of G on itself by conjugation is faithful iff G has a trivial center.*

Proof. Homework! $\square$

Orbits, stabilizers and fixed points

Let G act on X. For all $x \in X$, make the following definitions.
Definition 24. The orbit of x is defined as

$$\mathrm{Orb}_x := \{gx : g \in G\} \subset X.$$

The stabilizer of x is defined as

$$\mathrm{Stab}_x := \{g \in G : gx = x\} \subset G.$$

Remark 25. $\mathrm{Orb}_x = \{x\} \iff \mathrm{Stab}_x = G$. x is called the fixed point of the action.
Example 26. G acting on itself by left multiplication

$$\begin{array}{rcl} l_g : G & \to & G, \\ h & \mapsto & gh. \end{array}$$

- Orbit: one orbit $g = ge \in \mathrm{Orb}_e$.
- Stabilizer: $\mathrm{Stab}_x = \{g : gx = x\} = \{e\}$ trivial.
- Fixed points: $\mathrm{Stab}_x \neq G$ if $\#G > 1$ so no fixed points.

Example 27. Let G act on itself by conjugation.

- Orbit:

$$\mathrm{Orb}_a = \underbrace{\{gag^{-1} : g \in G\}}_{\text{conjugacy class of } a}.$$

- Stabilizer:

$$\begin{aligned} \mathrm{Stab}_a &= \{g : gag^{-1} = a\} \\ &= \{g : gag^{-1}g = ag\} \\ &= \underbrace{\{g : ga = ag\}}_{\text{centralizer of } a}. \end{aligned}$$

- Fixed points:

$$\begin{aligned} a \text{ fixed point} &\implies \mathrm{Stab}_a = G \\ &\implies a \text{ commutes with all } g \\ &\implies \text{ fixed points } a \text{ form } Z(G). \end{aligned}$$

Example 28. Let G act on G/H by left multiplication.

- Orbit: one orbit $gH = H \in \mathrm{Orb}_{\{H\}}$.
- Stabilizer:

$$\begin{aligned}\mathrm{Stab}_{aH} &= \{g : gaH = aH\} \\ &= \{g : a^{-1}gaH = a^{-1}aH = H\} \\ &= \{g : a^{-1}ga \in H\} = aHa^{-1}.\end{aligned}$$

- Fixed points: None if $H \neq G$.

Theorem 29. *Let G act on X. Then the following holds–*

1. *Different orbits are disjoint (in the set-theoretic sense).*
2. *For all $x \in X$, $Stab_x$ is a subgroup of G and $Stab_{gx} = gStab_x g^{-1}$*
3. $gx = g'x \iff g, g'$ *in the same left coset of* $Stab_x$. *Also the orbit-stabilizer formula holds–*

$$\boxed{\#Orb_x = [G : Stab_x]}$$

Proof. (1) We show that different orbits are disjoint by showing that two orbits which overlap must coincide: Let Orb_x and Orb_y have a same element z. So,

$$z = g_1 x \text{ and } z = g_2 y.$$

We need to show $\mathrm{Orb}_x = \mathrm{Orb}_y$ or the two inclusions

$$\begin{aligned} \mathrm{Orb}_x &\subset \mathrm{Orb}_y, \\ \mathrm{Orb}_y &\subset \mathrm{Orb}_x. \end{aligned}$$

For any $u \in \mathrm{Orb}_x$ write $u = gx$ for some $g \in G$. Since $z = g_1 x$, $x = g_1^{-1} z$. So

$$\begin{aligned} u &= g(g_1^{-1} z), \\ &= (g g_1^{-1}) z = (g g_1^{-1})(g_2 y), \\ &= (g g_1^{-1} g_2) y, \\ \implies u &\in \mathrm{Orb}_y. \end{aligned}$$

Repeat the same argument for Orb_y to obtain the other inclusion! $\square$

Proof. (2) Clear that $e \in \mathrm{Stab}_x$. If $g_1, g_2 \in \mathrm{Stab}_x$,

$$(g_1 g_2)x = g_1(g_2)x = g_1 x = x \text{ (from the definition of stabilizer)}$$

so $g_1, g_2 \in \mathrm{Stab}_x$ so closed under multiplication. Also $gx = x \implies x = g^{-1}x$ so closed under inverses.

To show $\mathrm{Stab}_{gx} = g\mathrm{Stab}_x g^{-1}$– for all $x \in X$ and $g \in G$,

$$\begin{aligned} h \in \mathrm{Stab}_{gx} &\iff h(gx) = gx, \\ &\iff (hg)x = gx, \\ &\iff g^{-1}((hg)x) = x, \\ &\iff (g^{-1}hg)x = x, \\ &\iff g^{-1}hg \in \mathrm{Stab}_x, \\ &\iff h \in g\mathrm{Stab}_x g^{-1}. \end{aligned}$$

$\square$

Proof. (3) Orb_x consists of points gx for varying g and elements of g act in the same way if they lie in the same left coset of Stab_x so we get a function

$$\begin{array}{rcl} G & \longrightarrow & \mathrm{Orb}_x, \\ g & \mapsto & gx \end{array}$$

which is surjective. The inverse image of each point in Orb_x under this map is a left coset of Stab_x. Therefore

$$\begin{array}{rcl} \#\mathrm{Orb}_x & = & \#\text{ left cosets of } \mathrm{Stab}_x \text{ in } G, \\ & = & [G : \mathrm{Stab}_x]. \end{array}$$

□

An important application–
Theorem 30. *Let G be a finite group acting on a finite set X with r orbits. Then r is the average number of fixed points of the elements of the group:*

$$\boxed{r = \frac{1}{\#G} \sum_{g \in G} \#Fix_g(X)}$$

where $\#Fix_g(X) = \{x \in X : gx = x\}$ the set of elements fixed by a fixed g.

Remark 31. $\mathrm{Fix}_g(X) \neq \#$ of fixed points of the action! Only includes points fixed by a fixed g. The number of fixed points of the action is given, instead, by

$$\bigcap_{g \in G} \mathrm{Fix}_g(X).$$

Count $\#\{(g, x) \in G \times X : gx = x\}$ in two different ways–

- Counting over g first we add the no. of x with $gx = x$. So
$$\#\{(g, x) \in G \times X : gx = x\} = \sum_{g \in G} \#\mathrm{Fix}_g(X).$$
- Counting over x and adding up the number of g with $gx = x$ (same as saying $g \in \mathrm{Stab}_x$) we get
$$\#\{(g, x) \in G \times X : gx = x\} = \sum_{x \in X} \#\mathrm{Stab}_x.$$

Therefore $\sum_{g\in G} \#\mathrm{Fix}_g(X) = \sum_{x\in X} \#\mathrm{Stab}_x$. By the orbit-stabilizer formula

$$\#G/\#\mathrm{Stab}_x = \#\mathrm{Orb}_x$$

so

$$\sum_{g\in G} \#\mathrm{Fix}_g(X) = \sum_{x\in X} \frac{\#G}{\#\mathrm{Orb}_x}.$$

Dividing out both sides by the order of G gives us

$$\frac{1}{\#G}\sum_{g\in G} \#\mathrm{Fix}_g(X) = \sum_{x\in X} \frac{1}{\#\mathrm{Orb}_x}.$$

Now note that if orbit has m points then the sum over the points on that orbit is a sum over $1/m$ which is one. Therefore the sum on the RHS $\sum_{x\in X} \frac{1}{\#\mathrm{Orb}_x}$ is the number of orbits r.

Basics of modules

References:

- Serge Lang, *Algebra*, Springer
- Michael F. Atiyah and Ian G. Mcdonald, *Introduction to commutative algebra*, Addison-Wesley
- Igor R. Shafarevich, *Basic notions of algebra*, Encyl. Math. Sci., Springer

Basic idea: vector spaces are defined over a *field*. Modules are a generalization of vector spaces– they are more generally defined over some *ring* (not neccesarily commutative!)

Remark 32. A module M over a ring R differs from a vector space V over a field k only in that multiplication of elts. of M with elements of R is defined rather than multiplication of elts. of V with elements of k. All other axioms are the same.

Caveat: R may or may not be commutative so it can act on M on the left or right. Our convention– we would deal with actions on the left and thus with *left R-modules* which we would refer to simply as *R-modules*.

Exercise 33. Write down the definition of a module M over a ring R.

Example 34. R is an R-module. This is immediate! It is the generalization of the notion of a 1-dimensional vector space.

Example 35. A module over a field k is a vector space over k. Again this is immediate!

Example 36. Any abelian group is a $\mathbb{Z}$-module M. To see this define

$$\begin{array}{rcl} \mathbb{Z} \times M & \longrightarrow & M, \\ nx & \mapsto & \underbrace{x + \ldots + x}_{n}. \end{array}$$

Example 37. $\mathfrak{j}$ a two-sided ideal of ring R. Then $R/\mathfrak{j}$ is an R-module.

If $r \in R$, $x + \mathfrak{j}$ coset of $\mathfrak{j}$ in R then define

$$r(x + \mathfrak{j}) := rx + \mathfrak{j}$$

and verify the axioms.

Example 38. Let S be some set and M an R-module. Then $\mathrm{Maps}(S, M)$ is an R-module.

Already know $\mathrm{Maps}(S, M)$ is an abelian group ($(f+g)(s) := f(s) + g(s)$) so it is a $\mathbb{Z}$-module. $\mathrm{Maps}(S, M)$ is an R-module as well with multiplication defined by

$$(rf)(s) := rf(s) \text{ for } f \in \mathrm{Maps}(S, M) \text{ and } r \in R.$$

Example 39. V vector space over k and $A : V \to V$ a linear tranformation. Then V is a $k[t]$-module with multiplication defined by

$$f(t)x := (f(A))(x) \text{ for } f(t) \in k[t] \text{ and } x \in V.$$

Example 40 (Interesting!)**.** Linear differential operators with constant $\mathbb{C}$-coeffecients ($\mathbb{C}$-lpdo) can be written as polynomials in $\frac{\partial}{\partial x_1}, \ldots, \frac{\partial}{\partial x_n}$ giving us a ring

$$\mathbb{C}\left[\frac{\partial}{\partial x_1}, \ldots, \frac{\partial}{\partial x_n}\right].$$

The map $\frac{\partial}{\partial x_i} \mapsto t_i$ gives a ring isomorphism (check!)

$$\mathbb{C}\left[\frac{\partial}{\partial x_1}, \ldots, \frac{\partial}{\partial x_n}\right] \simeq \mathbb{C}[t_, \ldots, t_n]. \tag{1}$$

The ring of $\mathbb{C}$-lpdo acts on (fixed and specified) spaces of functions $\mathcal{F}$ (say C^∞, with compact support, ...) and makes $\mathcal{F}$ a $\mathbb{C}\left[\frac{\partial}{\partial x_1}, \ldots, \frac{\partial}{\partial x_n}\right]$-module.

View $\mathbb{C}[t, \ldots, t_n]$ as a module over itself and call it M. By (1) view $\mathcal{F}$ as a module over M– call this module N. In general M and N are **not** isomorphic. However the Fourier transform can establish an isomorphism between M and N in a lot of interesting cases.

Let M an R-module.
Definition 41. $N \subset M$ is a submodule if N is an additive subgroup of M and

$$RN \subset N.$$

N is an R-module induced by the operation of R on M.
Definition 42. N submodule of M. Then the factor group M/N is an R-module called the factor module– let $x + N$ be a coset of N in M and let $r \in R$. Then define

$$\begin{array}{rcl} R \times M/N & \longrightarrow & M/N, \\ r(x+N) & \mapsto & rx + N. \end{array}$$

Definition 43. M, M' R-modules. A module homomorphism $f : M \longrightarrow M'$ satisfies

$$\begin{array}{rcl} (f)(x+y) & = & f(x) + f(y) \text{ for all } x, y \in M, \\ f(rx) & = & rf(x) \text{ for } r \in R. \end{array}$$

f is called an R-homorphism or an R-linear map.

The set of R-module homomorphism is denoted as $\mathrm{Hom}_R(M, M')$. ($\mathrm{Hom}_R(\cdot, \cdot)$ is, in fact, a functor, see upcoming lecture on "categories and functors"!)
Exercise 44. If $f \in \mathrm{Hom}_R(M, M')$ then $\ker f$ (resp. $\mathrm{im} f$) is a submodule of M (resp. M').

Exactness and related notions

Definition 45. Let $f \in \mathrm{Hom}_R(M, M')$. The cokernel of f is defined as

$$\mathrm{coker} f := M'/\mathrm{im} f = M'/f(M).$$

With this we come to an extremely important notion.

Definition 46. If we have $f \in \mathrm{Hom}_R(M', M)$ and $g \in \mathrm{Hom}_R(M, M'')$, a sequence of composition

$$M' \xrightarrow{f} M \xrightarrow{g} M''$$

is exact if

$$\mathrm{im} f = \ker g.$$

More generally,

Definition 47. Consider a sequence of R-modules and R-homomorphisms

$$\cdots \longrightarrow M_{i-1} \xrightarrow{f_i} M_i \xrightarrow{f_{i+1}} M_{i+1} \longrightarrow \cdots$$

This sequence is exact at M_i if $\mathrm{im} f_i = \ker f_{i+1}$. The sequence is exact if it is exact at each M_i.

Exactness is, *inter alia*, defined through the following properties

1. $0 \longrightarrow M' \xrightarrow{f} M$ is exact iff f is injective,

2. $M \xrightarrow{g} M'' \longrightarrow 0$ is exact iff g is surjective,

3. $0 \longrightarrow M' \xrightarrow{f} M \xrightarrow{g} M'' \longrightarrow 0$ is exact if f is injective, g is surjective and
$$\mathrm{coker} f \simeq M''$$
through g.

Functorial properties of $\mathrm{Hom}_R(\cdot, \cdot)$

Suppose Y be an R-module and $f \in \mathrm{Hom}_R(X', X)$. Then define a map

$$\begin{array}{ccc} \mathrm{Hom}_R(X, Y) & \longrightarrow & \mathrm{Hom}_R(X', Y), \\ g & \mapsto & g \circ f \end{array}$$

which is an element of $\mathrm{Hom}_R(f, Y)$.

For the sequence $X' \xrightarrow{f} X \xrightarrow{g} Y$, we have

1. f is a homomorphism iff

$$(g_1 + g_2) \circ f = f \circ g_1 + f \circ g_2 \text{ for all } g_1, g_2 \in \mathrm{Hom}_R(X, Y).$$

2. If $f = \mathrm{id}$ then the composition acts as an identity mapping

$$g \circ \mathrm{id} = g.$$

If we have a sequence of R-homomorphisms $X' \longrightarrow X \longrightarrow X''$, we get an induced sequence

$$\mathrm{Hom}_R(X', Y) \longleftarrow \mathrm{Hom}_R(X, Y) \longleftarrow \mathrm{Hom}_R(X'', Y).$$

Again, this will become more clearer (?) when we get to categories and functors!

Let M be an R-module. From the compositions

$$\begin{aligned} (g_1 + g_2) \circ f &= g_1 \circ f + g_2 \circ f, \\ g \circ (f_1 + f_2) &= g \circ f_1 + g \circ f_2, \\ g \circ \mathrm{id} &= g, \end{aligned}$$

we conclude

$$\boxed{\mathrm{End}_R(M) := \mathrm{Hom}_R(M, M) \text{ is a ring}}$$

This will be called the endomorphism ring of M.

Definition 48. A some other ring than R and

$$\rho : A \longrightarrow \mathrm{End}_R(M)$$

a ring homomorphism. Then ρ is called a representation of A on M.

Remark 49. If we replace rings by fields and therefore modules by vector spaces,

$$\mathrm{End}(V) = \mathrm{GL}(V).$$

Upon a choice of basis for the vector space V (say over k) this is, concretely,$\mathrm{GL}_n(k)$ where $n = \dim V$.

Let us revisit example 40 for a purely algebraic version. Let V be a vector space over a field k (of arbitrary characteristic– so could be different from $\mathbb{R}$ or $\mathbb{C}$!)

Example 50. Let $D_i \in \mathrm{End}_k(V)$. For any polynomial

$$P(X) \in k[X]$$

(so $P(X) = \sum_i a_i X^i$) define

$$P(D) = \sum_i a_i D_i$$

as an endomorphism. The map $P(X) \mapsto P(D)$ induces a representation

$$\rho : k[X] \longrightarrow \mathrm{End}_k(V)$$

making V a $k[X]$-module.

Sums and products of modules

Definition 51. M, N R-modules. The direct sum of M and N is denoted as

$$M \oplus N$$

and is a module consisting of pairs (m, n) for $m \in M$ and $n \in N$ with addition and multiplication (by elements of R) given by

$$\begin{aligned} (m,n) + (m',n') &:= (m+m', n+n'), \\ r(m,n) &:= (rm, rn) \end{aligned}$$

for all $m' \in M$, $n' \in N$ and $r \in R$. For a family of R-modules M_i with $i \in I$ a index set (not necessarily finite!) the direct sum of M_i's is denoted as

$$\bigoplus_i M_i.$$

The elements of $\bigoplus_i M_i$ are tuples (m_i) with $m_i \in M_i$ and almost all m_i are zero. Without this condition we get the direct product

$$\prod_i M_i.$$

Let $\{M_i\}$ be a family of submodules of M. Then we have the inclusion homomorphisms

$$\lambda_i : M_i \hookrightarrow M$$

which induces homomorphisms

$$\lambda_{i*} : \bigoplus_i M_i \longrightarrow M$$

given by

$$\lambda_{i*}((x_i)) = \sum_i x_i$$

for $x_i \in M_i$ and $M_i \subset M$ a submodule. If λ_{i*} is an isomorphism for all $i \in I$ we say that $\{M_i\}$ is a direct sum decomposition.

As an exercise write down the analogous definition of direct sum for vector spaces.

Proposition 52. *The following isomorphisms hold:*

$$\begin{aligned} Hom_R(M \oplus M', N) &\tilde{\leftrightarrow} Hom_R(M, N) \times Hom_R(M', N), \\ Hom_R(N, M \oplus M') &\tilde{\leftrightarrow} Hom_R(N, M) \times Hom_R(N, M'). \end{aligned}$$

Categories, functors and commutative diagrams

References:

- Serge Lang, *Algebra*, Springer
- Charles A. Weibel, *Introduction to homological algebra*, Cambridge Univ. Press
- Michael F. Atiyah and Ian G. Mcdonald, *Introduction to commutative algebra*, Addison-Wesley

Canonical references:

- Saunders MacLane, *Categories for the working mathematician*, Springer
- Peter Freyd, *Abelian categories*, Harper and Row

Basic definitions

Definition 53. A category **C** consists of objects $\mathrm{Obj}(\mathbf{C})$ and for two objects $A, B \in \mathrm{Obj}(\mathbf{C})$ a set $\mathrm{Mor}(A, B)$ called the set of morphisms of A into B; and for three objects $A, B, C \in \mathrm{Obj}(\mathbf{C})$ a composition map

$$\mathrm{Mor}(B, C) \times \mathrm{Mor}(A, B) \longrightarrow \mathrm{Mor}(A, C)$$

satisfying

1. $\mathrm{Mor}(A, B) \cap \mathrm{Mor}(A', B') = \emptyset$ unless $A = A'$ and $B = B'$ in which case $\mathrm{Mor}(A, B) = \mathrm{Mor}(A', B')$.

2. For every $A \in \mathrm{Obj}(\mathbf{C})$ there is a morphism $\mathrm{id}_A \in \mathrm{Mor}(A, A)$ which acts as left and right identity for the elements of $\mathrm{Mor}(A, B)$ and $\mathrm{Mor}(B, A)$ respectively, for all $B \in \mathrm{Obj}(\mathbf{C})$.

3. The law of composition is associative (when defined), i.e. given $f \in \mathrm{Mor}(A, B)$, $g \in \mathrm{Mor}(B, C)$ and $h \in \mathrm{Mor}(C, D)$ when

   $$(h \circ g) \circ f = h \circ (g \circ f)$$

   for all $A, B, C, D \in \mathrm{Obj}(\mathbf{C})$.

Example 54. The category **Sets** with

- $\mathrm{Obj}(\textbf{Sets})$ are sets and
- $\mathrm{Mor}(S, S')$ are maps between sets for $S, S' \in \mathrm{Obj}(\textbf{Sets})$.

Nothing to check here, the definition is trivially satisfied.

Remark 55. $\mathrm{Obj}(\mathbf{C})$ is in general not a set but what in mathematical logic is called a *class*. This is because in case of $\mathbf{C} = \textbf{Sets}$ if $\mathrm{Obj}(\textbf{Sets})$ was a set we'd run into *Russell's paradox*. See any book on mathematical logic for more on it!

"In practice" however, we can think of $\mathrm{Obj}(\mathbf{C})$ as a set. Such categories where $\mathrm{Obj}(\mathbf{C})$ are sets are called small.

Example 56. The category **AbGp** with

- $\mathrm{Obj}(\textbf{AbGp})$ are abelian groups and
- $\mathrm{Mor}(G, G')$ are group homomorphisms for $G, G' \in \mathrm{Obj}(\textbf{AbGp})$.

Here the only thing to check is the composition law in the definition above. This follows from the composition of group homomorphisms. (Verify the details!)

Example 57. The category $\mathbf{Mod}_R$ with

- $\mathrm{Obj}(\mathbf{Mod}_R)$ are R-modules and
- $\mathrm{Mor}(M, N)$ are R-module homomorphisms (which we denoted last class as $\mathrm{Hom}_R(M, N)$) for $M, N \in \mathrm{Obj}(\mathbf{Mod}_R)$.

Again, the composition law can be verified in this case by using the facts about $\mathrm{Hom}_R(M, N)$.

Question: Does every category $\mathbf{C}$ have $\mathrm{Mor}(X, Y)$ (for all $X, Y \in \mathrm{Obj}(\mathbf{C})$) as an abelian group? Group? Can you find an example/counterexample?

Some special kinds of morphisms– f is said to be

- an epimorphism if $g \circ f = h \circ f$ then $g = h$ (analogue of surjective maps),
- a monomorphism if $f \circ g = f \circ h$ then $g = h$ (analogue of injection).

Commutative diagrams

One of the main tools of category theory is a *commutative diagram*. Let $A, B, C \in \mathrm{Obj}(\mathbf{C})$ and $f \in \mathrm{Mor}(A, B)$, $g \in \mathrm{Mor}(B, C)$ and $h \in \mathrm{Mor}(A, C)$. We say that the diagram

$$\begin{tikzcd} A \arrow[r, "f"] \arrow[dr, "h"'] & B \arrow[d, "g"] \\ & C \end{tikzcd}$$

commutes if

$$h = g \circ f.$$

Similarly the diagram

$$\begin{tikzcd} A \arrow[r, "g"] \arrow[d, "f"'] & B \arrow[d, "h"] \\ C \arrow[r, "i"'] & D \end{tikzcd}$$

commutes if

$$h \circ g = i \circ f$$

where, for some $A, B, C, D \in \mathrm{Obj}(\mathbf{C})$, $f \in \mathrm{Mor}(A, C)$, $g \in \mathrm{Mor}(A, B)$, $h \in \mathrm{Mor}(B, D)$ and $i \in \mathrm{Mor}(C, D)$.

Diagrams are a very powerful way of writing down definitions of objects without appealing to their elements (i.e. not by referring to the elements of the objects as sets). As an example– recall/know

Definition 58. Let k be a field and A a k-vector space. A is a k-algebra if in addition we have

- a k-linear associate map $\mu_A : A \otimes A \to A$ called the "multiplication" and
- a k-linear multiplicative map $\eta_A : k \to A$ with $\eta_A(1) = 1_A$ where $1 \in k$ is the unit of k and $1_A \in A$ the unit of A.

In the language of diagrams, this definition can be rewritten in the following way
Definition 59. A triple (A, μ_A, η_A) is a k-algebra if A is a k-vector space and the following diagrams commute:

$$\begin{tikzcd} A \otimes A \otimes A \arrow[rr, "\mu_A \otimes \mathrm{id}_A"] \arrow[d, "\mathrm{id}_A \otimes \mu_A"'] & & A \otimes A \arrow[d, "\mu_A"] \\ A \otimes A \arrow[rr, "\mu_A"'] & & A \end{tikzcd}$$

and

$$\begin{tikzcd} A \otimes k \arrow[r, "\mathrm{id}_A \otimes \eta_A"] \arrow[dr, "\sim"'] & A \otimes A \arrow[d, "\mu_A"'] & k \otimes A \arrow[l, "\eta_A \otimes \mathrm{id}_A"'] \arrow[dl, "\sim"] \\ & A & \end{tikzcd}$$

Reversing arrows in this diagram gives us the notion of a k-coalgebra!

As a (hard?) exercise write down the definition of an abelian group in terms of a commutative diagram. Hint: ab groups are $\mathbb{Z}$-modules so $\otimes$ makes sense there! Its just $\otimes_{\mathbb{Z}}$ (to be explained in the next lectures).

Functors

We know functions that take elements of a given set to another set. *Functors* provide the analogy at the level of categories– it takes objects and morphisms in one category to objects and morphisms to another category. A formal definition–

Definition 60. Let **A** and **B** be two categories. A covariant functor F of **A** into **B** is a rule which associates to each $A \in \mathrm{Obj}(\mathbf{A})$ and object $F(A) \in \mathrm{Obj}(\mathbf{B})$ to each morphism $f \in \mathrm{Mor}(A, A')$ $(A, A' \in \mathrm{Obj}(A))$ a morphism $F(f) \in \mathrm{Mor}(F(A), F(A'))$ such that

1. For all $A \in \mathrm{Obj}(\mathbf{A})$ we have $F(\mathrm{id}_A) = \mathrm{id}_{F(A)}$.

2. If f and g are two morphisms of **A** then
$$F(g \circ f) = F(g) \circ F(f).$$

A contravariant functor has the same definition as above except in (2) the arrows are reversed–
$$F(g \circ f) = F(f) \circ F(g).$$

Our main examples would be the functors $-\otimes_R N$ and $\mathrm{Hom}_R(-, M)$. The first one would be discussed after we formally introduce tensor products of modules in the next lectures. However we have already seen and discussed $\mathrm{Hom}_R(-, M)$.

Recall that if M, N are (left) R-modules then $\mathrm{Hom}_R(M, N)$ is an abelian group (from last lecture's discussion.) In fact we saw that $\mathrm{Hom}_R(M, M)$ is more; it is a ring.

If we have a sequence of R-homomorphisms $X' \longrightarrow X \longrightarrow X''$, we get an induced sequence

$$\mathrm{Hom}_R(X', Y) \longleftarrow \mathrm{Hom}_R(X, Y) \longleftarrow \mathrm{Hom}_R(X'', Y).$$

of abelian groups, for another R-module Y. Abstractly, this is just the application of the functor

$$\mathrm{Hom}_R(-, Y)$$

to the sequence. Therefore one way to see this is to say

$$\mathrm{Hom}_R(-, Y) \text{ is a functor } \textbf{Mod}_R \longrightarrow \textbf{AbGp}.$$

The assignment $A \mapsto \mathrm{Hom}_R(A, -)$ is called the Yoneda embedding.
Exercise 61. Think about the last proposition from last lecture on modules

$$\begin{aligned}
\mathrm{Hom}_R(M \oplus M', N) &\quad \tilde{\leftrightarrow} \quad \mathrm{Hom}_R(M, N) \times \mathrm{Hom}_R(M', N), \\
\mathrm{Hom}_R(N, M \oplus M') &\quad \tilde{\leftrightarrow} \quad \mathrm{Hom}_R(N, M) \times \mathrm{Hom}_R(N, M').
\end{aligned}$$

in this way!

Natural transformations

Of course we can go one more step up in this ladder of abstraction and talk of the analogue of “maps" between functors! This is formalized by the notion of a *natural transformation*.

Definition 62. Suppose F and G are two functors from **C** to **D**. A natural transformation $\eta : F \implies G$ (this is the standard notation!) is a rule that assigns a morphism $\eta_C : F(C) \to F(C)$ in **D** to every object $C \in \mathrm{Obj}(C)$ in such a way that for every morphism $f : C \to C'$ in C such that the following diagram commutes

$$\begin{tikzcd}
F(C) \arrow[r, "F(f)"] \arrow[d, "\eta"'] & F(C') \arrow[d, "\eta"] \\
G(C) \arrow[r, "G(F)"'] & G(C')
\end{tikzcd}$$

Consider right R-modules M and M'. For every right module N there is a natural map $\eta_N : \mathrm{Hom}_R(M', N) \to \mathrm{Hom}_R(M, N)$ given by $\eta_N(f) = fh$ (we already saw this map last lecture). This gives rise to the natural transformation

$$\mathrm{Hom}_R(M', -) \implies \mathrm{Hom}_R(M, -).$$

The tensor product and related notions I

Definition and universal property

Let R be a *commutative* ring and M, N, L R-modules. Define a bilinear multiplication between M and N with values in L in the following way:

Definition 63. A bilinear multiplication between M and N with values in L is a map

$$\begin{array}{rcl} M \times N & \longrightarrow & L, \\ (m,n) & \mapsto & mn \text{ for all } m \in M, n \in N \text{ and } mn \in L \end{array}$$

with the following properties–

$$\begin{array}{rcl} (m_1 + m_2)n & = & m_1 n + m_2 n \text{ for } m_1, m_2 \in M \text{ and } n \in N, \\ m(n_1 + n_2) & = & mn_1 + mn_2 \text{ for } m \in M \text{ and } n_1, n_2 \in N, \\ (rm)n & = & m(rn) = r(mn) \text{ for } m \in M, n \in N \text{ and } r \in R. \end{array}$$

Let L' be another R-module and $\phi : L \to L'$ a homomorphism. Then $\phi(xy)$ defines a multiplication with values in L'. Basic (but very vague!) idea–

> There is a universal module $M \otimes_R N$ which contains all possible multiplications between M and N. This will be called *the tensor product* of M and N.

Let us make this idea precise and then show that (1) $M \otimes_R N$ exists and (2) $M \otimes_R N$ is unique. Consider the category $\mathbf{Mod}_R$ and the following diagram

$$\begin{tikzcd}
M \times N \arrow[r, "\text{bilinear}"] \arrow[dr] & L \arrow[d, "\text{linear}"] \\
& L'
\end{tikzcd}$$

The composition $M \times N \to L'$ is bilinear.

The tensor product occurs as a solution to the following *universal mapping problem*– for all R-modules M, N, P construct an R-module $M \otimes_R N$ and a bilinear map $f : M \times N \to M \otimes_R N$ such that all bilinear maps $M \times N \to P$ are composites of f and all linear maps $M \otimes_R N \to P$.

$$\begin{tikzcd}
M \times N \arrow[r, "f"] \arrow[dr, "\text{bilinear}"'] & M \otimes_R N \arrow[d, dotted, "\exists\ \text{linear?}"] \\
& P
\end{tikzcd}$$

In the language of category theory if $M \otimes_R N$ exists as a solution to the above universal mapping problem then it is called a universal object in $\mathbf{Mod}_R$.

Definition 64. The tensor product between M and N is an R-module $M \otimes_R N$ equipped with a bilinear multiplication map

$$\otimes : M \times N \longrightarrow M \otimes_R N$$

such that for any bilinear map $g : M \times N \to P$ there exists a lin map $h : M \otimes_R N \to P$ making the following diagram commute:

$$\begin{tikzcd} M \times N \arrow[r, "\otimes"] \arrow[dr, "g"'] & M \otimes_R N \arrow[d, "h"] \\ & P \end{tikzcd}$$

Of course we have to now show that the above definition is not empty, that is, there does indeed exist an R-module $M \otimes_R N$ and a bilinear map $\otimes$ that satisfies the above universal mapping problem.

Let $S \subset M$ be a subset of M an R-module. A linear combination of S is a sum

$$\sum_{x \in S} r_x x \text{ where } r_x \in R$$

with almost all of which are zero. Two facts– let N be the set of linear combinations of S. N is a submodule of M if

1. for $\sum_{x \in S} r_x x$ and $\sum_{x \in S} r'_x x$ the sum

$$\sum_{x \in X} (r_x + r'_x) x$$

   is a linear combination of S.

2. if $c \in R$ then

$$c\Big(\sum_{x \in S} r_x x\Big) = \sum_{x \in S} c r_x x$$

   is also a linear combination of S.

We say that N is a submodule generated by S and S is the set of generators of N. N is finitely generated if $\#S < \infty$.

An R-module is free if it is isomorphic to an R-module of the form $\bigoplus_i M_i$ where $M_i \simeq R$ in the category $\mathbf{Mod}_R$.

Theorem 65. *For any two given R-modules M and N, the R-module $M \otimes_R N$ exists.*

In Atiyah–Mcdonald, p. 24. this theorem is proved in the following way:
We will construct the R-module $M \otimes_R N$ in the following way. Let C be the free module $R^{(M \times N)}$ with elements formal linear combinations of elements of $M \times N$ with coefficients in R. That is, elements of C are of the form

$$\sum_{i=1}^{n} r_i(m_i, n_i) \text{ where } m_i \in M, n_i \in N \text{ and } r_i \in R.$$

Let D be a submodule of C generated by elements of C of the following form:

$$\begin{array}{rcl} (m+m', n) & - & (m,n) - (m',n), \\ (m, n+n') & - & (m,n) - (m,n'), \\ (rm, n) & - & r(m,n), \\ (m, rn) & - & r(m,n). \end{array}$$

Let $M \otimes_R N := C/D$. Then for each basis element $(m,n) \in C$ let $m \otimes n$ denote the image of (m,n) in $M \otimes_R N$. Therefore $M \otimes_R N$ is generated by elements of the form $m \otimes n$ and from our definitions of C and D

$$\begin{array}{rcl} (m+m') \otimes n & = & m \otimes n + m' \otimes n, \\ m \otimes (n+n') & = & m \otimes n + m \otimes n', \\ (rm) \otimes n & = & m \otimes (rn) = r(m \otimes n). \end{array}$$

Equivalently the bilin map $\otimes(m,n) := m \otimes n$ is bilinear.

Any map $f : M \times N \to P$ extends by linearity to an R-module hom $\tilde{f} : C \to P$. Let f be bilinear. Then from our definition of D, $\tilde{f}$ vanishes on all generators of D hence (extending by linearity) on all of D.

$\implies$ a well-defined hom $f' : M \otimes_R N \to P$ such that $f'(x \otimes y) = f(x,y)$. The mapping is uniquely defined by this.

$\implies$ the pair $(M \otimes_R N, \otimes)$ satisfies the above condition. This concludes the proof of the existence of the tensor product. The (easy) proof that the tensor product is unique upto unique isomorphism is omitted.

Remark 66. Very important! Take the following example $R = \mathbb{Z}$, $M = \mathbb{Z}$ and $N = \mathbb{Z}/2\mathbb{Z}$. Let M' be the submodule $2\mathbb{Z}$ of $\mathbb{Z}$ and $N' = N$. Let x be a nonzero element of N and consider $2 \otimes x$. Now

$$2 \otimes x = 1 \otimes 2x = 1 \otimes 0 = 0$$

as an element of $M \otimes N$. However as an element of $M' \otimes N'$ it is nonzero– look at the exact sequence

$$0 \longrightarrow \mathbb{Z} \xrightarrow{f} \mathbb{Z}$$

where $f(x) = 2x$ for all $x \in \mathbb{Z}$. Tensor this exact sequence with $N = \mathbb{Z}/2\mathbb{Z}$ to get

$$0 \longrightarrow \mathbb{Z} \otimes N \xrightarrow{f \otimes 1} \mathbb{Z} \otimes N$$

a nonexact sequence since for all $x, y \in \mathbb{Z} \otimes N$ we have

$$(f \otimes 1)(x \otimes y) = 2x \otimes y = x \otimes 2y = x \otimes 0 = 0$$

so $f \otimes 1$ is the zero mapping whereas $\mathbb{Z} \otimes N \neq 0$. Moral: Let M', N' be submodules of M, N respectively and $x \in M'$, $y \in N'$. $x \otimes y$ as an element of $M \otimes N$ may be zero while as an element of $M' \otimes N'$ it may be nonzero!

Exercise 67. Show $(\mathbb{Z}/m\mathbb{Z}) \otimes (\mathbb{Z}/n\mathbb{Z}) = 0$ if (m, n) are coprime.

The tensor product as a functor

In our discussion of categories and functors, we saw an example of a contravariant functor $\mathrm{Hom}_R(-, N)$

$$\begin{array}{rcl} \textbf{Mod}_R & \longrightarrow & \textbf{AbGp}, \\ M & \mapsto & \mathrm{Hom}_R(M, N). \end{array}$$

The tensor product can also be viewed as a functor and there is an interesting relationship between these two. (They are said to be adjoints.)

To establish that $M \otimes_R -$ is indeed a functor we note (for the time being with out proof) the following unique isomorphisms:

$$\begin{array}{rcl} M \otimes_R N & \simeq & N \otimes_R M, \\ (M \otimes_R N) \otimes P & \simeq & M \otimes_R (N \otimes_R P) \simeq M \otimes_R N \otimes_R P, \\ (M \oplus N) \otimes_R P & \simeq & (M \otimes_R P) \oplus (N \otimes_R P), \\ (R \otimes_R M) & \simeq & M. \end{array}$$

Clearly if these hold, $M \otimes_R -$ is a covariant functor

$$\begin{array}{rcl} \textbf{Mod}_R & \longrightarrow & \textbf{AbGp}, \\ N & \mapsto & M \otimes_R N. \end{array}$$

Theorem 68 (Hom-tensor adjointness). *In the category* ***AbGp****,*

$$Hom_R(M \otimes N, P) \simeq Hom_R(M, Hom_R(N, P)).$$

Proof. (Atiyah–Mcdonald, p. 28.) In one direction: $f : M \times N \to P$ a bilinear map. For all $x \in M$ the map

$$\begin{array}{ccc} N & \longrightarrow & P, \\ y & \mapsto & f(x,y) \end{array}$$

gives rise to a map

$$M \longrightarrow \mathrm{Hom}_R(N, P)$$

that is linear since f is linear in x. In the other direction: any linear $\phi : M \to \mathrm{Hom}_R(N, P)$ defines a bilinear map $(x, y) \mapsto \phi(x)y \implies$ the set S of bilinear mappings $M \times N \to P$ is in natural (in the sense of natural transformations!) 1-1 with

$$\mathrm{Hom}_R(M, \mathrm{Hom}_R(N, P)).$$

At the same time, S is in 1-1 correspondence with

$$\mathrm{Hom}_R(M \otimes_R N, P)$$

by the universal mapping property of the tensor product. □

The tensor product and related notions II

Leftovers: Proofs of some useful isomorphisms

At the end of the lecture on modules I had stated
Proposition 69. *In* ***AbGp****, the following isomorphism holds:*

$$\begin{aligned} Hom_R(M \oplus M', N) &\simeq Hom_R(M, N) \times Hom_R(M', N), \\ Hom_R(N, M \oplus M') &\simeq Hom_R(N, M) \times Hom_R(N, M'). \end{aligned}$$

Let us prove this for the first isomorphism. Consider the sequences

$$M \longrightarrow M \oplus \{0\} \subset M \oplus M' \xrightarrow{f} N$$

and

$$M' \longrightarrow \{0\} \oplus M' \subset M \oplus M' \xrightarrow{f} N$$

Now look at the maps

$$M \xrightarrow{h_1} M \oplus \{0\}, \quad m \mapsto m \oplus 0,$$

and

$$M' \xrightarrow{h_2} \{0\} \oplus M', \quad m' \mapsto 0 \oplus m'.$$

Now if $f : M \oplus M'$ is a homomorphism then f induces a homomorphism $f_1 : M \to N$ by composing f with h_1, that is, $f_1 = f \circ h_1$.

Similarly, f induces a homomorphism $f_2 : M' \to N$ by $f_2 = f \circ h_2$.

(h_1 and h_2 are homomorphisms ($x \mapsto x \oplus 0$ gives $xy \mapsto (x \oplus 0)(y \oplus 0) = xy \oplus 0$) so f_1 and f_2 are homomorphisms) For the inverse, define the "projections"

$$M \oplus M' \longrightarrow M, x \oplus y \mapsto x,$$

and

$$M' \oplus M \longrightarrow M', y \oplus x \mapsto y.$$

It is trivial to check that doing exactly what was done above and composing the maps gives us identity and there the first isomorphism is established.

The second isomorphism is established the same way.

Last lecture I had also discussed some isomorphisms related to $\otimes$ and $\oplus$ without proof. Let's now see how these propositions are proved. I shall do a typical one and the rest are left as exercises (same technique as below will suffice.)

Proposition 70. *M, N, P R-modules. Then*

$$(M \otimes N) \otimes P \simeq M \otimes (N \otimes P).$$

In order to prove these statements, we have to construct homomorphisms

$$(M \otimes N) \otimes P \xrightarrow{f} M \otimes N \otimes P \xrightarrow{g} M \otimes (N \otimes P)$$

such that

$$\begin{aligned} f((x \otimes y) \otimes z) &= x \otimes y \otimes z, \\ g(x \otimes y \otimes z) &= (x \otimes y) \otimes z, \end{aligned}$$

for all $x \in M$, $y \in N$, $z \in P$.

Construction of f: Fix $z \in P$. The map $(x, y) \mapsto x \otimes y \otimes z$ is bilinear in x and y and therefore induces a homomorphism

$$\begin{aligned} M \otimes N &\xrightarrow{f_z} M \otimes N \otimes P, \\ x \otimes y &\mapsto f_z(x \otimes y) = x \otimes y \otimes z. \end{aligned}$$

Consider

$$\begin{array}{rcl} (M \otimes N) \otimes P & \longrightarrow & M \otimes N \otimes P, \\ (t, z) & \mapsto & f_z(t). \end{array}$$

This is bilinear in t and z so it induces a homomorphism

$$\begin{array}{rcl} (M \otimes N) \otimes P & \xrightarrow{f} & M \otimes N \otimes P, \\ (x \otimes y) \otimes z & \mapsto & x \otimes y \otimes z. \end{array}$$

Construction of g: Consider

$$\begin{array}{rcl} M \times N \times P & \longrightarrow & (M \otimes N) \otimes P, \\ (x, y, z) & \mapsto & (x \otimes y) \otimes z. \end{array}$$

This map is linear in each var so it induces a homomorphism

$$\begin{array}{rcl} M \otimes N \otimes P & \xrightarrow{g} & (M \otimes N) \otimes P, \\ (x \otimes y \otimes z) & \mapsto & g(x \otimes y \otimes z) = (x \otimes y) \otimes z. \end{array}$$

We see

$$f \circ g = g \circ f = \mathrm{id}.$$

Symmetric and exterior powers of modules

All through we fix a commutative ring R and write $\otimes$ to mean $\otimes_R$. Let M be an R-module. Define the tensor algebra of M to be

$$T^r(M) := \underbrace{M \otimes \cdots \otimes M}_{r-\text{times}}.$$

Elements of $T^r(M)$ are called contravariant tensors.
Definition 71. The symmetric square of M is defined as the quotient

$$\mathrm{Sym}^2 M := M \otimes M / (x \otimes y - y \otimes x).$$

(View the two-sided ideal $(x \otimes y - y \otimes x)$ as a submodule of $M \otimes M$.)

A generalization of the above is
Definition 72. The r-th symmetric power of M which is defined as the quotient

$$\mathrm{Sym}^r M = T^r(M)/I$$

where the submodule I is generated by elements of the form

$$x_1 \otimes \cdots \otimes x_i \otimes x_{i+1} \otimes \cdots \otimes x_r - x_1 \otimes \cdots \otimes x_{i+1} \otimes x_i \otimes \cdots \otimes x_r,$$

where $x_i \in M$ and for $i = 1, \ldots, r-1$.

Definition 73. The r-th exterior power of M is defined as the quotient

$$\bigwedge^r M := T^r(M)/(x_1 \otimes \cdots \otimes x_r)$$

where in the submodule two factors coincide, say $x_i = x_j$.

The exterior product of M is defined as a map

$$\begin{array}{rcl} \underbrace{M \times \cdots \times M}_{r-\text{times}} & \longrightarrow & \bigwedge^r M, \\ (x_1, \ldots, x_r) & \mapsto & x_1 \wedge \cdots \wedge x_r. \end{array}$$

The following properties are very useful for computations:

$$\begin{array}{rcl} x_1 \wedge \cdots \wedge x_r & = & 0 \text{ if } x_i = x_j \text{ where } 1 \leq i, j \leq r, \\ x_1 \wedge \cdots \wedge x_i \wedge x_{i+1} \wedge \cdots \wedge x_r & = & -x_1 \wedge \cdots \wedge x_{i+1} \wedge x_i \wedge \cdots \wedge x_r. \end{array}$$

Definition 74. M an R-module. Then $M^* := \mathrm{Hom}_R(M, R)$ is an R-module defined by

$$\begin{array}{rcl} (f+g)(m) & = & f(m) + g(m) \text{ for } f, g \in M^* \text{ and } m \in M, \\ (rf)(m) & = & rf(m) \text{ for } f \in M^*, r \in R \text{ and } m \in M. \end{array}$$

M^* is called the dual module.

The elements of $T^r(M^*)$ are called covariant tensors. The elements of

$$T^p(M) \otimes T^q(M^*)$$

are called tensors of type (p, q).

Remark 75. The terminology “covariant tensors" and “contravariant tensors" follow from the fact that $\mathrm{Hom}_R(-, N)$ is a contravariant functor and $M \otimes -$ is a covariant functor. (Notice the arrow-reversals!)

Specialization to vector spaces

We will now specialize all of the constructions discussed in the previous lectures to the case of vectors spaces (i.e. replacing rings by fields). We will also develop some tools for concrete calculations. Reference I'll follow–

- Appendix B of William Fulton and Joe Harris, "Representation theory: a first course", Springer.

The tensor product of two vector spaces V and W over a field is a vector space $V \otimes W$ equipped with a bilinear map

$$V \times W \to V \otimes W$$

which is universal in the sense discussed for modules.
Exercise 76. Trivial! Write down the definition of $V \otimes W$ by replacing R by a field k and carefully describe the universal mapping property in this case.

Let $\{e_i\}$ and $\{f_j\}$ be the basis of V and W respectively. Then

$$\{e_i \otimes f_j\}$$

form a basis for $V \otimes W$. This gives the explicit construction of $V \otimes W$ as in the case of modules.

Bilinearity can be extended to multilinearity– in case of modules, the best way to think of this would be categorically cf. Lang (3rd edition), chapter XVI. In case of vector spaces this boils down to:

Definition 77. The map

$$V \times \cdots \times V \longrightarrow U$$

is multilinear if when all but one factors V is fixed, the resulting map is linear.

The following isomorphisms hold for vector spaces–

$$\begin{aligned} V \otimes W &\simeq W \otimes V, \\ (V_1 \oplus V_2) \otimes W &\simeq (V_1 \otimes W) \oplus (V_2 \otimes W), \\ (U \otimes V) \otimes W &\simeq U \otimes (V \otimes W) \simeq U \otimes V \otimes W. \end{aligned}$$

The exterior powers $\bigwedge^n V$ comes with a universal alternating multilinear map

$$\begin{array}{ccc} V \times \cdots \times V & \longrightarrow & \bigwedge\limits^n V, \\ (v_1, \ldots, v_n) & \mapsto & v_1 \wedge \cdots \wedge v_n. \end{array}$$

An alternating multilinear map is a multilinear map β such that

$$\beta(v_1, \ldots, v_n) = 0 \text{ whenever } v_i = v_j.$$

From standard fact about polarization linear algebra, β changes sign whenever two vectors are exchanged:

$$\beta(v + w, v + w) - \beta(w, w) = \beta(v, w) + \beta(w, v).$$

In compact notation, let $\sigma \in S_n$. Then

$$\beta(v_{\sigma(1)}, \ldots, v_{\sigma(n)}) = \operatorname{sgn}(\sigma)\beta(v_1, \ldots, v_n).$$

Convention:

$$\bigwedge^0 V = k \text{ the ground field.}$$

Proposition 78. *As vector spaces, we have an isomorphism*

$$\bigwedge^n (V \oplus W) \simeq \bigoplus_{a=0}^{n} \left(\bigwedge^a V \otimes \bigwedge^{n-a} W\right).$$

Proof. Define a linear map

$$\begin{array}{ccc} \bigwedge^a V \otimes \bigwedge^b W & \longrightarrow & \bigwedge^{a+b} (V \bigoplus W), \\ (v_1 \wedge \cdots \wedge v_a) \otimes (w_1 \wedge \cdots \wedge w_b) & \mapsto & v_1 \wedge \cdots \wedge v_a \wedge w_1 \wedge \cdots \wedge w_b. \end{array}$$

Now use the definition of $\wedge$ and bilinearity of $\otimes$ to complete the proof. $\square$

The definition of $\mathrm{Sym}^n V$ is also exactly analogous (write it down for yourself if you must!) We set as a convention

$$\mathrm{Sym}^0 V = k \text{ the ground field.}$$

Using the same technique as in the proof of the proposition above show as an exercise

Proposition 79. *As vector spaces, we have an isomorphism*

$$Sym^n (V \oplus W) \simeq \bigoplus_{a=0}^{n} \left(Sym^a V \otimes Sym^{n-a} W\right).$$

Some notation–

- The tensor algebra

$$T^\bullet V = \bigoplus_{n\geq 0} V^{\otimes n},$$

- The exterior algebra

$$\bigwedge^\bullet V = \bigoplus_{n\geq 0} \bigwedge^n V = T^\bullet V/(v\otimes w),$$

- The symmetric algebra

$$\mathrm{Sym}^\bullet V = \bigoplus_{n\geq 0} \mathrm{Sym}^n V = T^\bullet V/(v\otimes w - w\otimes v).$$

Interlude: Family of vector spaces over a topological space

Let X be a topological space. A family of vector spaces over X is a topological space $\mathcal{E}$ with a C^0-map

$$f : \mathcal{E} \longrightarrow X$$

in which every fiber $f^{-1}(x)$ is a vector space (over $\mathbb{R}$ or $\mathbb{C}$). A homomorphism between $f : \mathcal{E} \longrightarrow X$ and $g : \mathcal{F} \longrightarrow X$ is a C^0-map

$$\phi : \mathcal{E} \longrightarrow \mathcal{F}$$

taking $f^{-1}(x)$ to $g^{-1}(x)$. A family of vector spaces $\mathcal{E}$ defines a module $M_{\mathcal{E}}$ over the ring $A(X)$ of C^0-functions. Elements of $\mathcal{E}$ are called sections and are C^0-maps

$$s : X \longrightarrow \mathcal{E}$$

with $fs(x) = x$. The $A(X)$-module structure on $M_{\mathcal{E}}$ comes from

$$\begin{aligned} (s_1 + s_2)(x) &= s_1(x) + s_2(x) \text{ for } s_1, s_2 \in M_{\mathcal{E}} \text{ and } x \in X, \\ (\phi s)(x) &= \phi(x)s(x) \text{ for } \phi \in A(X), x \in X \text{ and } s \in M_{\mathcal{E}}. \end{aligned}$$

Representations of Finite Groups I

References I follow/suggest for these lectures–

1. William Fulton and Joe Harris, “Representation theory: a first course", Springer

2. Jean-Pierre Serre, “Linear representations of finite groups", Springer

3. Serge Lang, “Algebra", Springer

4. V. Lakshmibai and Justin Brown, “Flag varieties", Hindustan Book Agency

Some preliminary definitions

Let G be a finite group with $\#G = n$ and K a field of characteristic zero or characteristic p where p doesn't divide n.

Definition 80. A finite dimensional vector space V over K is called a G-module if there is a group homomorphism

$$\boxed{\rho : G \longrightarrow \mathrm{Aut}_K(V)}$$

where $\mathrm{Aut}_K(V) = \{f : V \longrightarrow V | f \text{ linear and invertible}\}$. We then say that V is a representation of G.

We will interchangeably write $\mathrm{GL}(V)$ to mean $\mathrm{Aut}_K(V)$ and vice-versa.

Definition 81. The group algebra $K[G]$ is the K-vector space with elts of G as a basis. Explicitly

$$K[G] = \{ \sum_{g \in G} a_g g, a_g \in K \text{ where } a_g = 0 \text{ for all but finite } g\}.$$

Example 82. Let G be finite cyclic, $G = \{1, x, \ldots, x^{n-1}\}$. Then

$$K[G] = K[x]/\langle x^n - 1\rangle.$$

Recall the definition of a K-algebra. $K[G]$ is a commutative K-algebra where the multiplicative structure is given by

$$(a_g g)(b_{g'} g') = \sum (a_g b_{g'}) g \cdot g'.$$

We have a 1-1 correspondence

$$\boxed{\{\text{representations of } G\} \longrightarrow \{\text{representations of } K[G]\}}$$

given by a map

$$\begin{aligned} \rho : K[G] &\longrightarrow \mathrm{End}_K(V), \\ \rho\Big(\sum_{g\in G} a_g g\Big)(v) &= \sum_{g\in G} a_g (g \cdot v). \end{aligned}$$

In general we have the bijection

$$\boxed{\mathrm{Hom}_{K-\textsf{alg}}(K[G], \mathrm{End}_K V) \leftrightarrow \mathrm{Hom}_{\textsf{Gp}}(G, \mathrm{Aut}_K(V))}$$

Recall basic notions about group actions on sets. In all cases, check the examples through the definition as **exercises**.

Example 83. The trivial representation– $\rho(g) = \mathrm{id}_V$ for all $g \in G$. Let $y = \sum_{g \in G}$. Then $K \cdot y$ is trivial $K[G]$-module since $gy = y$.

Example 84. The left regular representation– action of $K[G]$ on itself by left multiplication

Example 85. The permutation representations– Let G act on the set X through bijections $g : X \to X$. Let V be the K-vector space with $\{e_x, x \in X\}$ as basis. G acts on V by permuting the basis elements

$$e_x \mapsto e_{\sigma(x)}.$$

Here $\sigma \in S_n$ where $n = \#X$.

Semisimplicity and simplicity

Definition 86. An R-module M is semisimple if every submodule of M is a direct summand. In other words if N is a submodule then there exists another submodule P such that

$$M = N \oplus P.$$

This is same as saying that there exists a map $p : M \to N$ such that the composition

$$N \xrightarrow{i} M \xrightarrow{p} N$$

is identity.
Example 87. K field. Every K-module V (= K-vector space) is semisimple. Why? Because I can always find a subvector space W' for every given distinct subvector space W such that

$$V = W \oplus W'.$$

Definition 88. M is simple if M does not have a nonzero proper submodules $\iff$ (0) and (M) are the only submodules of M.

Recall the bijection between $K[G]$-modules and G-modules and note that $K[G]$ is semisimple so for V a repn of G we have $V = \bigoplus_i V_i$ for all i.

Definition 89. V is G-irreducible if V is simple as a G-module.

We come to an important result–
Proposition 90 (Schur's Lemma)**.** *Let K be algebraically closed, i.e., $K = \bar{K}$. Let V be G-irreducible. Then*

$$End_G V = K.$$

Proof. Let $f \in \mathrm{End}_G V$. Since $K = \bar{K}$ f has an eigenvalue, say λ. Therefore there is a $v \neq 0$ such that

$$\begin{aligned} f(v) &= \lambda v, \\ \implies \ker(f - \lambda \mathrm{id}_V) &\neq 0. \end{aligned}$$

Let $\phi = f - \lambda \mathrm{id}_V$ so that $\phi : V \to V$ is a G-linear map. $\ker \phi$ is a nonzero submodule of the simple G-module V. Therefore from the definition of simplicity $\ker \phi = V \iff \phi = 0 \iff f = \lambda \mathrm{id}_V$. So $\mathrm{End}_G V = K$. $\square$

Definition 91. Let V be a G-module. The space of invariants

$$V^G := \{v \in V | gv = v \text{ for all } g \in G\}.$$

This is a G-submodule of V and acts trivially on V^G.

A very important definition–
Definition 92. Define

$$\begin{aligned} \chi_V : G &\longrightarrow K, \\ g &\mapsto \operatorname{trace}(\rho(g)). \end{aligned}$$

χ_V is called the character of (V, ρ).
Example 93. Let (V, ρ) be the trivial representation. Then $\chi_V : G \to K$ is the constant function

$$\chi_V(g) = d$$

for all $g \in G$ and $d = \dim V$.
Example 94. Let $V = K[G]$ be the left regular representation, Then

$$\chi_V(g) = 0 \text{ if } g \neq e.$$

This is because– $G = \{g_1, \ldots, g_n\}$ as a K-basis implies $g \cdot g \neq g_i$. Therefore in this basis all diag entries are 0 for $g \neq e$.

Schur's lemma has the following implication– for $x \in Z(K[G])$ and a given simple G-module V,

$$\rho(x) : V \longrightarrow V$$

given by $v \mapsto x \cdot v$ is K-linear and and a G-map since $x \in Z$. So

$$\rho_x = \lambda \cdot \mathrm{id}_V.$$

For a conjugacy class C the element $y_C := \sum_{x \in C} x$ acts on V by scalars. From this the following result follows

Lemma 95. *χ_V is constant on conjugacy classes and therefore χ_V is a class function. (A class function of G (with values in K) is function $f : G \to k$ such that $f(\sigma\tau\sigma^{-1}) = f(\tau)$ for all $\sigma, \tau \in G$.)*

Irreducible representations

To step back a bit- recall the notion of stability. Let $\rho : G \to \mathrm{GL}(V)$ and $W \subset V$. W is stable under G if $\rho_s x \in W$ for all $w \in W$ and $s \in G$. Restricting ρ_s to a stable W gives an isom of W to itself. We say this restriction

$$\boxed{\rho^W : G \longrightarrow \mathrm{GL}(W)}$$

is a subrepresentation of V.

Definition 96. An irreducible representation is a representation (V, ρ) that has no subrepresentations $\iff V \neq V_1 \oplus V_2$.

Irred rep $\leftrightarrow$ simple modules!

Theorem 97. *Every representation is a direct sum of irreducible representations. (Such a property is called semisimplicity.)*

We will prove this by first proving the following:
Lemma 98. *Let W be stable under G. Then there exists a compliment W^0 of W which is stable under G.*

Let us first prove the lemma. Let W' be compliment of W in V and $p : V \to W$ projection onto the subspace W. Define the average

$$p^0 := \frac{1}{g} \sum_{t \in G} \rho_t p \rho_t^{-1}$$

where g is the order of G. Now p^0 maps V to W since p maps V to W and ρ_t preserves W (from the assumption of stability). This gives $\rho_t^{-1} x \in W$ for $x \in W$ and therefore

$$\begin{aligned} p\rho_t^{-1} x &= \rho_t^{-1} x, \\ \rho_t p \rho_t^{-1} x &= x, \\ p^0 x &= x. \end{aligned}$$

From this conclude that $p^0 : V \to W$ is a projection corresponding some compliment W^0 of W in V. We have

$$\rho_s p^0 = p^0 \rho_s \text{ for all } s \in G$$

through the following direct computation:

$$\begin{aligned}
\rho_s p^0 \rho_s^{-1} &= \frac{1}{g} \sum_{t \in G} \rho_s \rho_t p \rho_t^{-1} \rho_s^{-1}, \\
&= \frac{1}{g} \sum_{t \in G} \rho_{st} p \rho_{st}^{-1}, \\
&= p^0.
\end{aligned}$$

If $x \in W^0$ and $s \in G$ we have $p^0 \rho_s x = \rho_s p^0 x = 0 \implies \rho_s x \in W^0 \implies W^0$ stable under G.

Proof of the theorem. Induct on $\dim V$. For $\dim V = 0$ statement trivially true, so assume $\dim V \geq 1$. If V irreducible, then done. If not then by lemma, $V = V' \oplus V''$ with $\dim V' < \dim V''$ and $\dim V'' < \dim V$. By induction hypo V' and V'' are direct sum of irreducible representation so the same holds for V. $\square$

Proposition 99. *Let V, W be representations of G and $K = \mathbb{C}$. Then (exercise!)*

$$\begin{aligned}
\chi_{V \oplus W} &= \chi_V + \chi_W, \\
\chi_{V \otimes W} &= \chi_V \chi_W, \\
\chi_{V^*} &= \overline{\chi_V}.
\end{aligned}$$

We instead prove a more interesting assertion:

Proposition 100. *Let ρ be a representation of G on a vector space V and χ its character. Let χ_σ^2 be the character of $Sym^2(V)$ and χ_α^2 be a character of $\bigwedge^2(V)$. Then for all $s \in G$,*

$$\begin{aligned}
\chi_\sigma^2 &= \frac{1}{2}(\chi(s)^2 + \chi(s^2)), \\
\chi_\alpha^2 &= \frac{1}{2}(\chi(s)^2 - \chi(s^2)),
\end{aligned}$$

where $\chi_\sigma^2 + \chi_\alpha^2 = \chi^2$.

Proof. The main idea is this: a basis of V can be chosen consisting of eigenvectors of ρ_s- call this basis $\{e_i\}$. We have $\rho_s e_i = \lambda_i s_i$ $\lambda_i \in \mathbb{C}$ so

$$\chi(s) = \sum \lambda_i \text{ and } \chi(s^2) = \sum \lambda_i^2.$$

We also have

$$\begin{aligned}(\rho_s \otimes \rho_s)(e_i e_j + e_j e_i) &= \lambda_i \lambda_j (e_i e_j + e_j e_i),\\ (\rho_s \otimes \rho_s)(e_i e_j - e_j e_i) &= \lambda_i \lambda_j (e_i e_j - e_j e_i)\end{aligned}$$

so

$$\begin{aligned}\chi_\sigma^2(s) &= \sum_{i \leq j} \lambda_i \lambda_j = \sum \lambda_i^2 + \sum_{i<j} \lambda_i \lambda_j = \frac{1}{2}\left(\sum \lambda_i\right)^2 + \frac{1}{2}\sum \lambda_i^2,\\ \chi_\alpha^2(s) &= \sum_{i<j} \lambda_i \lambda_j = \frac{1}{2}\left(\sum \lambda_i\right)^2 - \frac{1}{2}\sum \lambda_i^2.\end{aligned}$$

□

Remark 101. The equality $\chi_\sigma^2(s) + \chi_\alpha^2(s) = \chi^2(s)$ follows from the decomposition

$$\boxed{V \bigotimes V = \mathrm{Sym}^2(V) \bigoplus \bigwedge^2(V)}$$

Definition 102. An irreducible character is a character associated to an irreducible representation.

Consider the space of all K-valued functions on G. (K either of char 0 or of $p > 0$, p not dividing n the order of G.)

$$\mathcal{F}_K(G) := \{f : G \longrightarrow K\}.$$

An irred G-module is defined exactly like a simple R-module. We want to prove

Theorem 103. *Let V, V' be two irred G-modules. Then the irred characters $\{\chi_i, 1 \le i \le g\}$ form an orthonormal basis of $\mathcal{F}_K(G)$.*

In order to prove this theorem we will need to introduce the following inner product on $\mathcal{F}_K(G)$

$$(f, g) := \frac{1}{n} \sum_{x \in G} f(x^{-1}) g(x).$$

Exercise 104. Show that this inner product is symmetric– $(f,g) = (g,f)$.

Proof. We want to show that $(\chi_V, \chi_{V'}) = 0$ if V is not isomorphic to V' and $(\chi_V, \chi_{V'}) = 1$ it is. Let $f \in \mathrm{Hom}_K(V.V')$ and $\{e_i\}$ (resp. $\{f_j\}$) basis of V (resp. V'.) Let $x \in G$ and

$$\begin{aligned}
\rho(x) &= (\rho_{ij}(x)),\ f = (f_{ij}),\\
\rho'(x) &= (\rho'_{kl}(x)),\ \tilde{f} = \frac{1}{n}\sum_{x\in G}\rho'(x)\circ f\circ\rho(x).
\end{aligned}$$

From Schur's lemma, we have $\tilde{f} = 0$ or $\tilde{f} = \lambda \mathrm{id}_V$ depending on whether or not $V \simeq V'$. Now

$$\tilde{f}_{qt} = \frac{1}{n}\sum_{x,l,i}\rho'_{ql}(x^{-1})f_{li}\rho_{it}(x).$$

Therefore

$$\begin{aligned}
(\chi',\chi) &= \frac{1}{n}\sum_{x}\chi'(x^{-1})\chi(x),\\
&= \frac{1}{n}\sum_{x}\big(\sum_{q}\rho'_{qq}(x^{-1})\big)\big(\sum_{t}\rho_{tt}(x)\big).
\end{aligned}$$

A suitable function f along with the above computation proves the existence of a orthonormal basis for $\mathcal{F}_K(G)$. □

Definition 105. If $\operatorname{char} K = 0$ representations of G are called ordinary. When $\operatorname{char} K = p > 0$ representations of G are called modular.

Next lecture we will study ordinary representations and an irreducibility criterion for them, induced representations and Mackey's criterion and begin the study of representations of the symmetric group.

Representations of Finite Groups II

Ordinary representations of finite groups

Consider the space of all K-valued functions on G. (K either of char 0 or of $p > 0$, p not dividing n the order of G.)

$$\begin{array}{rcl} \mathcal{F}_K(G) & := & \{f : G \longrightarrow K\}, \\ \mathcal{C}_K(G) & \subset & \mathcal{F}_K(G), \text{ the subset of all class functions of } G. \end{array}$$

Introduce the following inner product on $\mathcal{F}_K(G)$

$$(f, g) := \frac{1}{n} \sum_{x \in G} f(x^{-1}) g(x).$$

Last lecture we saw that $(\chi_V, \chi_{V'}) = 0$ **if** V **is not isomorphic to** V' **and** $(\chi_V, \chi_{V'}) = 1$ **if it is**. We will call this result the orthogonality formula.

I also want to mention a theorem I will not explicitly use but keep in mind.
Theorem 106 (Maschke)**.** *Let* $\#G = n$. $K[G]$ *is semisimple iff* $n \cdot 1 \neq 0$ *in* K *iff either* $\mathit{char}\ K = 0$ *or* $\mathit{char}\ K$ *doesn't divide* n*.*

A criterion for ordinary representations–

Theorem 107. *Let V and W be representation spaces of G over K a field of characteristic 0. Then*

1. $V \simeq W \iff \chi_V = \chi_W$.

2. V *irreducible* $\iff (\chi_V, \chi_V) = 1$.

3. *Let $A_K(G)$ generated by $\{\chi_V | V \text{ a } G - \text{module}\}$ be an additive subgroup of $\mathcal{C}_K(G)$. Then $A_K(G)$ is a free abelian group of rank h with irreducible chars as basis.*

Proof of (1). (Forward) If $V \simeq W$ then $\chi_V = \chi_W$. This follows directly from the definition of characters. (As an **exercise** write this out!)

(Reverse) Can assume V and W completely reducible i.e.

$$\begin{aligned} V &= \bigoplus_{i=1}^{r} d_i V_i, \\ W &= \bigoplus_{i=1}^{r} e_i W_i, \end{aligned}$$

where V_i, W_i simple. (Why? There is a bijective correspondence

$$\{\text{repn. of } G\} \leftrightarrow \{\text{representation of } K[G]\}$$

and $K[G]$ is semisimple!) $\implies \chi_V = \sum d_i \chi_{V_i} \big(= \sum d_i \chi_i \big)$.

By assumption $\chi_V = \chi_W \implies \sum (d_i - e_i)\chi_i = 0$.

Notice that since $\operatorname{char} K = 0$ there is an inclusion $\mathbb{Z} \subset K$ so $\{\chi_{V_i}\}$ is $\mathbb{Z}$-linear independent. (That it is K-linear independent followed from the orthogonality formula). So $d_i = e_i$ for all i which gives $V \simeq W$. $\square$

Proof of (2). (Forward) Already know from the orthogonality formula that if V irreducible then $(\chi_V, \chi_V) = 1$. Let $V = \oplus_i d_i V_i$ and $\chi_V = \sum_i d_i \chi_i$.

(Reverse) By assumption

$$1 = (\chi_V, \chi_V) = \sum_i d_i^2.$$

Since we are in char 0, $d_i = 1$ for precisely a single i with all $d_j = 0$ for $i \neq j$. Therefore V irreducible. $\square$

Proof of (3). This follows directly from the orthogonality formula– since $\mathrm{char}\, K = 0$ we have $\mathbb{Z} \subset K$ and then apply that theorem (from last lecture)! $\square$

A characterization of characters–

Proposition 108. *Let V be a G-module. Then $\chi_V(x)$ is an algebraic integer for all $x \in G$.*

Proof. Consider the linear automorphism

$$V \xrightarrow{x} V$$

for a fixed $x \in G$. By picking a suitable basis for V we can represent x by a diagonal matrix

$$\begin{pmatrix} a_1 & & \\ & \ddots & \\ & & a_d \end{pmatrix}.$$

Also since $x^n = e$ (e identity of G, G finite) have $\rho(x^n) = \rho(e) = \mathrm{id}$. Therefore

$$a_i^n = 1 \implies a_i \text{ is an algebraic integer for all } i.$$

(Why? any $\alpha \in \mathbb{C}$ is algebraic (by definition) if it is a root of a monic integral polynomial. Here consider the polynomial $X^n - 1 = 0$.) This implies $\chi_V(x) = \mathrm{trace}(x) = \sum a_i$ is an algebraic integer. $\square$

Induced representations

Generalities on restriction and extension of scalars–

Let $f : A \to B$ be a ring homomorphism and N a B-module. Then N has an A-module structure in the following way: if $a \in A$ and $x \in N$ then the multiplication ax is defined to be $f(a)x$. This A-module is said to be obtained from N by restriction of scalars. So f defines an A-module structure on B.

Let M be an A-module. Since B can be regarded as an A-module, we can form an A-module

$$M_B = B \otimes_A M.$$

M_B carries a B-module structure s.t. $b(b' \otimes x) = bb' \otimes x$ for all $b, b' \in B$ and $x \in M$. M_B is obtained from M by extension of scalars.

For the rest of the lecture, we assume the ground field to be $\mathbb{C}$.

Induced representations–

H subgroup of G and $\sigma \in G/H$ left coset representatives. V $\mathbb{C}[G]$-module and W sub $\mathbb{C}[H]$-module of V.

Definition 109. The representation W' is said to induced by W if

$$W' = \bigoplus_{\sigma \in G/H} \sigma H.$$

We write $W' = \mathrm{Ind}_H^G(W)$.

Let

$$W' = \mathbb{C}[G] \otimes_{\mathbb{C}[H]} W$$

be obtained through extension of scalars. Consider the diagram

$$\begin{tikzcd}
\mathbb{C}[G] \otimes_{\mathbb{C}[H]} W = W' \arrow[dr, "i"] & \\
& V \\
W \arrow[uu] \arrow[ur, hook] &
\end{tikzcd}$$

i is obtained by extending by linearity the injection $W \hookrightarrow V$. Since σ form a basis of $\mathbb{C}[G]$ considered as a $\mathbb{C}[H]$-module, $i : W' \to V$ is an isomorphism. (Existence and uniqueness is a consequence of this as well as the universal mapping property of the tensor product for modules!)

With this fact we have an equivalent way of stating definition 109.

$$W' = \mathrm{Ind}_H^G(W) = \mathbb{C}[G] \otimes_{\mathbb{C}[H]} W.$$

Proposition 110. *Let $H \subset G \subset K$ be inclusions of subgroups. Then:*

1. *Induction is transitive–*

$$Ind_G^K(Ind_H^G(W)) \simeq Ind_H^K(W).$$

2. *Let V be induced by W and E a $\mathbb{C}[G]$-module. Let $Hom_{\mathbb{C}[H]}(W, E)$ (resp. $Hom_{\mathbb{C}[G]}(V, E)$) be the vector space of $\mathbb{C}[H]$-homomorphism of W into E (resp. $\mathbb{C}[G]$-homs of V into E.) Then*

$$Hom_{\mathbb{C}[H]}(W, E) \simeq Hom_{\mathbb{C}[G]}(V, E).$$

Proof. (1) This follows from isomorphisms of the tensor product:

$$\begin{aligned}
\mathrm{Ind}_G^K(\mathrm{Ind}_H^G(W)) &= \mathbb{C}[K] \otimes_{\mathbb{C}[G]} (\mathbb{C}[G] \otimes_{\mathbb{C}[H]} W), \\
&\simeq (\mathbb{C}[K] \otimes_{\mathbb{C}[G]} \mathbb{C}[G]) \otimes_{\mathbb{C}[H]} W, \\
&\simeq \mathbb{C}[K] \otimes_{\mathbb{C}[H]} W, \\
&= \mathrm{Ind}_H^K(W).
\end{aligned}$$

(2) Again this too follows from the properties of tensor product (as an exercise write out the details!):

$$\begin{aligned}
\mathbb{C}[G] \otimes_{\mathbb{C}[H]} \mathrm{Hom}_{\mathbb{C}[H]}(W, E) &\simeq \mathrm{Hom}_{\mathbb{C}[H]}(\mathbb{C}[G] \otimes_{\mathbb{C}[H]} W, E), \\
&= \mathrm{Hom}_{\mathbb{C}[G]}(V, E).
\end{aligned}$$

□

The Frobenius Reciprocity

Let $H \subset G$ be a subgroup and $f \in \mathcal{C}_{\mathbb{C}}(H)$ ($\dim \mathcal{C}_{\mathbb{C}}(H) = \#H = h$). Define f' on G by

$$f'(s) = \frac{1}{h} \sum_{s \in G \text{ and } t^{-1}st \in H} f(t^{-1}st).$$

Definition 111. We say f' is induced by f and write

$$f' = \mathrm{Ind}_H^G(f) \text{ or } f' = \mathrm{Ind}(f).$$

Proposition 112. *Let H be a subgroup of G.*

1. *$Ind(f)$ is a class function on G.*

2. *If f is a character of a repn W on H then $Ind(f)$ is a character of the induced representation $Ind(W)$ on G.*

Proof. **Exercise!** □

Remark 113. After establishing this proposition, we can see Ind to be a functor. Question: from what category to what category?

Restrict the inner product on $\mathcal{F}_{\mathbb{C}}(G)$ to class functions on G– for ϕ_1, ϕ_2 we have ($\#G = g$)

$$(\phi_1, \phi_2)_G = (\phi_1, \phi_2) = \frac{1}{g} \sum_{s \in G} \phi_1(s^{-1}) \phi_2(s).$$

Set

$$(V_1, V_2)_G := \dim \operatorname{Hom}_{\mathbb{C}[G]}(V_1, V_2).$$

Lemma 114. *If ϕ_1 and ϕ_2 are characters of V_1 and V_2 then*

$$(\phi_1, \phi_2)_G = (V_1, V_2)_G.$$

Proof. Decompose V_1 and V_2 into irreducibles and then apply the orthogonality theorem (from last lecture) which shows that irreducible characters form a basis for $\mathcal{F}_{\mathbb{C}}(G)$ and so the inner product on the left is the dimension. $\square$

Restriction of representations:

V repn of G, ϕ function on G.

$$\begin{aligned} \mathrm{Res}(V) &: \quad \text{restriction of } V \text{ to a subgroup } H, \\ \mathrm{Res}(\phi) &: \quad \text{restriction of } \phi \text{ to a subgroup } H. \end{aligned}$$

Theorem 115 (Frobenius reciprocity)**.** *Let ψ be a class function on H and ϕ be a class function on G. Then*

$$(\psi, Res(\phi))_H = (Ind(\psi), \phi)_G.$$

Proof. (Serre) Each class function is a lin comb of characters so assume ψ is a character of a $\mathbb{C}[H]$-module W and ϕ a character of $\mathbb{C}[G]$-module E. By lemma 114, it suffices to show

$$(W, \mathrm{Res}(E))_H = (\mathrm{Ind}(W), E)_G$$

which is same as showing

$$\dim \mathrm{Hom}_{\mathbb{C}[H]}(W, \mathrm{Res}(E)) = \dim \mathrm{Hom}_{\mathbb{C}[G]}(\mathrm{Ind}(W), E).$$

This follows from proposition 110 and so we have the theorem. □

A somewhat tricky exercise would be to directly prove Frobenius Reciprocity from the definition of Ind and Res and $(-,-)$. Try it if you feel enthusiatic enough!

Mackey's criterion

We continue our study of ordinary representations. Work over $\mathbb{C}$. This lecture is based on Serre's *Linear representations of finite groups*. First we will study Mackey's criterion and then state and prove Artin's theorem, both related to induced representations.

H and K subgroups of G.

$$\begin{aligned} \rho &: H \longrightarrow \mathrm{GL}(W) \text{ lin repn of } H, \\ V &= \mathrm{Ind}_H^G(W) = \mathbb{C}[G] \otimes_{\mathbb{C}[H]} W \text{ ind repn.} \end{aligned}$$

Goal: determine $\mathrm{Res}_K(W)$ of V to K.

Double cosets– S set of representatives of double cosets (H,K) of G. So

$$G = \bigsqcup_{s \in S} KsH.$$

(This is same as writing $s \in K\backslash G/H$.) Let $H_s := sHs^{-1} \cap K$ for all $s \in S$. This is a subgroup of K! (**exercise**) Let

$$\rho^s(x) := \rho(s^{-1}xs) \text{ for all } x \in H_s.$$

This gives a linear representation

$$\rho^s : H_s \longrightarrow \mathrm{GL}(W)$$

since ρ^s is a hom:

$$xy \mapsto s^{-1}xys = s^{-1}xss^{-1}ys = (s^{-1}xs)(s^{-1}ys).$$

Now $\mathrm{Ind}_{H_s}^K(W_s)$ is defined since $H_s \subset K$ is a subgroup. (W_s is the lin repn of H_s.)
Proposition 116.

$$Res_K(Ind_H^G(W)) \simeq \bigoplus_{s \in K\backslash G/H} Ind_{H_s}^K(W_s).$$

Proof. We see that

$$V = \bigoplus_{x \in G/H} xW.$$

Let $s \in S$ and $V(s)$ be the subspace of V generated by the images xW for $x \in KsH$. Then

$$V = \bigoplus_{s \in S} V(s).$$

Now need to show that $V(s)$ is K-isomorphic to $\mathrm{Ind}_{H_s}^{K}(W_s)$. But the subgroup of K consisting of elements x such that $x(sW) = s(W)$ is H_s (from the definition. of H_s.) Therefore

$$V(s) = \bigoplus_{x \in K/H_s} \mathrm{im}(x(sW))$$

and so

$$V(s) = \mathrm{Ind}_{H_s}^{K}(sW).$$

We still need

$$sW \text{ is } H_s - \text{isomorphic to } W_s.$$

This is given by $s : W_s \longrightarrow sW$. □

We are ready to state and prove a criterion due to Mackey that gives the necessary and sufficient condition for an induced representation to be irreducible. We make a preliminary definition.

Definition 117. Two representations V_1 and V_2 are disjoint if $(V_1, V_2)_K = 0$. (Recall $(-,-)_K := \dim \operatorname{Hom}_{\mathbb{C}[K]}(-,-)$.)

Let $K = H$ and $H_s = sHs^{-1} \cap H$.

Theorem 118 (Mackey)**.** *In order for the induced representation $V = Ind_H^G(W)$ to be irred, it is necessary and sufficient that*

1. *W be irred and*

2. *for all $s \in G \setminus H$, ρ^s and $Res_s(\rho)$ of H_s are disjoint.*

Proof. We know that

$$V \text{ irred} \iff (V,V)_G = 1.$$

Now by Frobenius reciprocity (thm. 10, lecture 10) we have

$$(V,V)_G = (W, \mathrm{Res}_H(V))_H$$

but by proposition 116 we have

$$\mathrm{Res}_H(V) = \bigoplus_{s \in H \backslash G / H} \mathrm{Ind}_{H_s}^H(\rho^s).$$

By applying Frobenius reciprocity again

$$(V,V)_G = \sum_{s \in H \backslash G / H} d_s \text{ where } d_s = (\mathrm{Res}_s(\rho), \rho^s)_{H_s}.$$

For $s = 1$, $d_s = (\rho, \rho) \geq 1$. For $(V,V)_G = 1$ it is necc. and suff. that $d_1 = 1$ and $d_s = 0$ for $s \neq 1$. Now these are the precise conditions (1) and (2) in thm. 118. $\square$

Artin's theorem and the representation ring

Let G be a finite group with $\chi_1, \ldots, \chi_h$ irreducible characters $\chi_i \neq \chi_j$ for $i \neq j$.

We knew from last class that $\{\chi_i\}$ forms a basis for $\mathcal{C}_{\mathbb{C}}(G)$. Let us set

$$\begin{aligned} R^+(G) &:= \text{class functions which are linear comb of } \chi_i \text{ with } \mathbb{Z}_{>0} - \text{coeffs}, \\ R(G) &:= \text{group gen. by } R^+(G). \end{aligned}$$

Note that $R(G)$ is simply the set of differences of two characters. So

$$R(G) = \mathbb{Z}\chi_1 \oplus \cdots \oplus \mathbb{Z}\chi_h.$$

Definition 119. $R(G)$ is called the representation ring of G. Each element of $R(G)$ is called a virtual character.

Note that $R(G)$ is indeed a ring from the fact that sums and products of characters are characters!

Proposition 120. *$R(G)$ is a subring of $\mathcal{F}_{\mathbb{C}}(G)$ and $\mathbb{C} \otimes R(G)$ can be identified with $\mathcal{F}_{\mathbb{C}}(G)$.*

Proof. The first assertion follows from the fact that product of characters are characters. Now χ_i form a basis of $\mathcal{F}_{\mathbb{C}}(G)$ over $\mathbb{C}$ so $\mathbb{C} \otimes R(G)$ can be identified with $\mathcal{F}_{\mathbb{C}}(G)$. $\square$

Let $H \subset G$ be a subgroup. We know

- Res gives a ring homomorphism $R(G) \longrightarrow R(H)$.
- Ind gives an abelian group homomorphism $R(H) \longrightarrow R(G)$.

By definitions of Ind and Res and their duality,

$$\mathrm{Ind}(\phi \cdot \mathrm{Res}(\psi)) = \mathrm{Ind}(\phi) \cdot \psi$$

so

$$\mathrm{im}(\mathrm{Ind} : R(H) \longrightarrow R(G)) \text{ is an ideal of } R(G).$$

Emile Artin (father of Mike Artin who wrote the *Algebra* book!) in his study of what are now called Artin L-functions in number theory proved the following theorem about characters.

For a general introduction and context of Artin's theorem in case of L-functions see the extended exercise 26, p. 727 of Lang. (Ambitious students might want to put our/Serre's approach and Lang's description together!)

Theorem 121 (E. Artin). *Let X be a family of subgroups of G and let*

$$Ind : \bigoplus_{H \in X} R(H) \longrightarrow R(G)$$

be the hom induced by Ind_H^G for all subgroups H of G. TFAE:

1. *G is the union of conjugates of the subgroups belonging to X.*

2. *$coker\big(Ind : \bigoplus_{H \subset G} R(H) \longrightarrow R(G)\big)$ is finite.*

Remark 122. Condition (2) can be rephrased in the following way: since $R(G)$ is finitely generated as a group (by definition) for each character χ of G there exists $\chi_H \in R(H)$ and $H \in X$ and an integer $d \in \mathbb{Z}_{\geq 1}$ such that

$$d \cdot \chi = \sum_{H \in X} \mathrm{Ind}_H^G(\chi_H).$$

Now the family of cyclic subgroups of G satisfy condition (1) of thm. 121 so from that we obtain the very important

Corollary 123. *Each character of G is a linear combination with $\mathbb{Q}$-coefficients of characters induced by characters of cyclic subgroups of G.*

Therefore the up-shot of Artin's theorem is that it suffices to just study characters of cyclic subgroups of G since characters of the whole group can be constructed with these through linearity and induction!

Let A be a cyclic group and $a = \#A$. Define a function on A by:

$$\theta_A(x) = a \text{ if } x \text{ generates } A \text{ else it is } 0.$$

Let $g = \#G$ and by g also denote the constant function equal to g. Then we have

Lemma 124. *$g = \sum_{A \subset G} Ind_A^G(\theta_A)$.*

Proof. Let $\theta'_A := \mathrm{Ind}_A^G(\theta_A)$. For each $x \in G$ we have

$$\begin{aligned}
\theta'_A(x) &= \frac{1}{a} \sum_{y \in G, yxy^{-1} \in A} \theta_A(yxy^{-1}), \\
&= \frac{1}{a} \sum_{y \in G, yxy^{-1} \text{ gen. } A} a, \\
&= \sum_{y \in G, yxy^{-1} \text{ gen. } A} 1.
\end{aligned}$$

Since for each $y \in G$, yxy^{-1} generates a unique cyclic subgroup of G we have

$$\sum_{A \subset G} \theta'_A(x) = \sum_{y \in G} 1 = g.$$

$\square$

Lemma 125. *If A is a cyclic subgroup then $\theta_A \in R(A)$.*

Proof. Induct on a. $a = 1$ is obviously true (why?) so by lem. 124 we have

$$\begin{aligned} a &= \sum_{B \subset A} \mathrm{Ind}_B^A(\theta_B), \\ &= \theta_A + \sum_{B \neq A} \mathrm{Ind}_B^A(\theta_B). \end{aligned}$$

By induction hypothesis, $\theta_B \in R(B)$ for $B \neq A$ so $\mathrm{Ind}_B^A(\theta_B)$ belongs to $R(A)$. But it is also clear that $a \in R(A)$ so it follows that $\theta_A \in R(B)$. $\square$

We now prove Artin's theorem.

Proof of thm. 121. ($(1) \implies (2)$). Note: if A' is in the conjugate of A then $\operatorname{im}(\operatorname{Ind}_{A'}^G) \subset \operatorname{im}(\operatorname{Ind}_A^G) \implies$ can assume X is the family of all cyclic subgroups of G. By lem. 125 have that if

$$g = \sum_{A \subset X} \operatorname{Ind}_A^G(\theta_A), \theta_A \in R(A)$$

then $g \in \operatorname{im}(\operatorname{Ind})$ but $\operatorname{im}(\operatorname{Ind})$ ideal of $R(G)$ so it contains every element of the form $g\chi$, $\chi \in R(G)$ which implies (2) by the equivalent statement of (2) of rem. 122.

($(2) \implies (1)$). Let S be the union of conjugates of subgroups H belonging to X. Each function $\sum \operatorname{Ind}_H^G(f_H)$ vanish off S for $f_H \in R(H)$. (2) satisfied $\implies$ each class function on G vanish off $S \implies S = G \implies$ (1) holds. $\square$

See proof of prop. 8.5, p.700 of Lang for a direct computation of the equation in the proof of $(1) \implies (2)$.