Math 325 - Algebra 1

Lectures by Victor Ginzburg
Notes by Zev Chonoles

The University of Chicago, Fall 2012

Introduction

Math 325 is one of the nine courses offered for first-year mathematics graduate students at the University of Chicago. It is the first of three courses in the year-long algebra sequence.

These notes were live-TeXed, though I edited for typos and added diagrams requiring the Ti*k*Z package separately. I used the editor TeXstudio.

I am responsible for all faults in this document, mathematical or otherwise; any merits of the material here should be credited to the lecturer, not to me.

Please email any corrections or suggestions to chonoles@math.uchicago.edu.

Acknowledgments

Thank you to all of my fellow students who sent me suggestions and corrections, and who lent me their own notes from days I was absent. My notes are much improved due to your help.

I would like to especially thank Jonathan Wang for supplementing my notes from class with his own observations and explanations in numerous places, as well as for catching many of my typos and misunderstandings.

Lecture 1 (2012-10-01)

Today we'll be talking about the Chinese Remainder Theorem and some of its consequences.

Lagrange Interpolation Formula. Let k be a field. Then for any $c_1, \ldots, c_n \in k$, and any distinct $x_1, \ldots, x_n \in k$, there exists a $p \in k[t]$ such that $p(x_i) = c_i$ for all i.

Proof. The proof comes in three steps.

Step 1: For each $i = 1, \ldots, n$, define

$$p_{ij}(t) = \frac{t - x_j}{x_i - x_j}.$$

Note that

$$p_{ij}(t) = \begin{cases} 1 & \text{if } t = x_i, \\ 0 & \text{if } t = x_j. \end{cases}$$

Step 2: For each $i = 1, \ldots, n$, define

$$p_i(t) = \prod_{j \neq i} p_{ij}(t).$$

Note that

$$p_i(t) = \begin{cases} 1 & \text{if } t = x_i, \\ 0 & \text{if } t = x_j \text{ for any } j \neq i. \end{cases}$$

Step 3: Define

$$p(t) = \sum_{i=1}^{n} c_i p_i(t).$$

It is easy to verify that this p satisfies the claimed property. $\square$

In this course, rings will always be unital, though they will not necessarily be commutative.

Given a ring A and two-sided ideals $I_1, \ldots, I_n \subset A$, there are some important ways we can create new two-sided ideals.

The sum of the I_i is defined by

$$I_1 + \cdots + I_n = \{x_1 + \cdots + x_n \mid x_i \in I_i\}.$$

The product of the I_i is defined by

$$I_1 \cdots I_n = \{\sum x_1 \cdots x_n \mid x_i \in I_i\}.$$

The intersection of the I_i is just their intersection as subsets of A.

Note that we always have $I_1 \cdots I_n \subseteq I_1 \cap \cdots \cap I_n$.

We can re-express the Lagrange Interpolation Formula as follows:

Lagrange Interpolation Formula. Let k be a field, and let $A = k[t]$. For any $c_1, \ldots, c_n \in k$, and any distinct $x_1, \ldots, x_n \in k$, let $I_i = (t - x_i)$. There exists a $p \in A$ such that $p - c_i \in I_i$ for all i.

Note that

$$\begin{aligned} \text{the } x_i \text{ are distinct} &\iff \text{for any } i \neq j,\ -(t - x_i) + (t - x_j) = x_i - x_j \neq 0 \\ &\iff \text{for any } i \neq j,\ I_i + I_j = A. \end{aligned}$$

Chinese Remainder Theorem. Let A be a not-necessarily-commutative ring, and $I_1, \ldots, I_n$ two-sided ideals of A such that $I_i + I_j = A$ for all $i \neq j$. Then

1. For any $c_1, \ldots, c_n \in A$, there exists $p \in A$ such that $p - c_i \in I_i$ for all i.
2. If A is commutative, then $I_1 \cdots I_n = I_1 \cap \cdots \cap I_n$.

Proof of Part 1. The proof comes in three steps.

Step 1: For any $i \neq j$, we have that $I_i + I_j = A$. Thus, for any $i \neq j$ there are some $q_{ij} \in I_i$ and $p_{ij} \in I_j$ such that $q_{ij} + p_{ij} = 1$. Note that $1 - p_{ij} = q_{ij} \in I_i$.

Step 2: For each i, let

$$p_i = \prod_{j \neq i} p_{ij} \in \prod_{j \neq i} I_j \subset I_j \text{ for all } j \neq i.$$

We claim that $1 - p_i \in I_i$. This follows from observing that

$$p_i = \prod_{j \neq i} (1 - q_{ij}) = 1 + (\text{terms involving the } q_{ij})$$

and that for all $j \neq i$, $q_{ij} \in I_i$.

Step 3: Let

$$p = \sum_{i=1}^{n} c_i p_i.$$

Checking that this p works, we see that for any i,

$$p - c_i = c_i(1 - p_i) + \sum_{j \neq i} c_j p_j,$$

and $(1 - p_i) \in I_i$ and each $p_j \in I_i$ by Step 2, so that $p - c_i \in I_i$ for all i. □

Proof of Part 2. We proceed by induction. For the case of $n = 2$, note that because $I_1 + I_2 = A$, there are some $u_1 \in I_1$, $u_2 \in I_2$ such that $u_1 + u_2 = 1$. For any $a \in I_1 \cap I_2$, we then have

$$a = au_1 + au_2.$$

Because $a \in I_2$ and $u_1 \in I_1$, we have that $au_1 \in I_2 I_1$. Because $a \in I_1$ and $u_2 \in I_2$, we have that $au_2 \in I_1 I_2$. Now using the assumption that A is commutative, we have that $I_2 I_1 = I_1 I_2$ and therefore $a \in I_1 I_2$. This proves that $I_1 \cap I_2 \subseteq I_1 I_2$, and hence $I_1 \cap I_2 = I_1 I_2$.

Now for the inductive step. By the inductive hypothesis, we know that

$$I_2 \cap \cdots \cap I_n = I_2 \cdots I_n,$$

and therefore

$$I_1 \cap (I_2 \cap \cdots \cap I_n) = I_1 \cap (I_2 \cdots I_n).$$

We would like to show that

$$I_1 \cap (I_2 \cdots I_n) = I_1 I_2 \cdots I_n.$$

This will follow from the $n = 2$ case, provided that we can show that

$$I_1 + (I_2 \cdots I_n) = A.$$

Recall that in the proof of part 1, we constructed a $p_1 \in A$ such that $1 - p_1 \in I_1$ and

$$p_1 \in \prod_{j \neq i} I_j = I_2 \cdots I_n.$$

Then the fact that

$$1 = p_1 + (1 - p_1)$$

implies that $1 \in I_1 + (I_2 \cdots I_n)$, and hence $I_1 + (I_2 \cdots I_n) = A$. □

Because the I_i are two-sided ideals, we can quotient the ring A by them. Define the homomorphisms $\pi_i : A \to A/I_i$ to be the quotient maps, so that $\ker(\pi_i) = I_i$.

Define π to be the composition

$$\pi : A \xrightarrow{\text{diag}} \bigoplus_{i=1}^{n} A \xrightarrow{\oplus \pi_i} \bigoplus_{i=1}^{n} A/I_i,$$

so that

$$\pi(a) = (a \bmod I_1, \ldots, a \bmod I_n).$$

Clearly, $\ker(\pi) = \bigcap \ker(\pi_i) = \bigcap I_i$.

We can now restate the Chinese Remainder Theorem in a more abstract form.

Chinese Remainder Theorem. Let A be a not-necessarily-commutative ring, and $I_1, \ldots, I_n$ two-sided ideals of A such that $I_i + I_j = A$ for all $i \neq j$. Then the map π is surjective, and induces an isomorphism

$$\overline{\pi} : A/(I_1 \cap \cdots \cap I_2) \to \bigoplus_{i=1}^{n} A/I_i.$$

Proof. Because we induced the map $\overline{\pi}$ by quotienting out by the kernel of π, we have that $\ker(\overline{\pi}) = 0$. Therefore, $\overline{\pi}$ is injective. Also, $\overline{\pi}$ is surjective, because for any choice of $\overline{c_i} \in A/I_i$ for each i, there is some $a \in A$ such that $a \bmod I_i = \overline{c_i}$ by the Chinese Remainder Theorem. □

Now we will review some basics about PIDs.

A ring A is a PID when

1. A is commutative,
2. A has no zero-divisors, and
3. Any ideal of A is principal.

Examples of PIDs include the ring $\mathbb{Z}$, and the polynomial ring $k[t]$ over a field k.

Let A be a PID. For any $a, b \in A \setminus \{0\}$, we say that $d \in A$ is a gcd of a and b when $d \mid a$ and $d \mid b$, and when for any $g \in A$ such that $g \mid a$ and $g \mid b$, we also have $g \mid d$.

The following is a fundamental result about PIDs.

Theorem. *Let A be a PID. For any $a, b \in A \setminus \{0\}$,*

$$Aa + Ab = A\gcd(a, b).$$

Proof. Since A is a PID, we know the ideal $Aa + Ab$ is equal to Ad for some d. Note that

$$a \in Aa \subset Aa + Ab = Ad$$

implies that $d \mid a$. By symmetry, $d \mid b$ as well. If $g \mid a$ and $g \mid b$, then $a, b \in Ag$, so that

$$Ad = Aa + Ab \subset Ag,$$

which implies that $d \in Ag$ and hence $g \mid d$. □

Corollary. *Let A be a PID. Then*

$$\gcd(a, b) = 1 \iff Aa + Ab = A \iff \text{ there exist } u, v \in A \text{ such that } au + bv = 1.$$

Corollary. *Let A be a PID, and let $a = a_1 \cdots a_n$ where $\gcd(a_i, a_j) = 1$ for all $i \neq j$. Then*

$$A/(a) \cong A/(a_1) \oplus \cdots \oplus A/(a_n).$$

Lecture 2 (2012-10-03)

Today we'll be talking about modules.

In a sentence, a module is a vector space over a ring. More precisely, let A be a ring. Then a (left) A-module is an abelian group $(M, +)$ with an action map $A \times M \to M$ satisfying

1. $1_A m = m$,
2. $(a_1 + a_2)m = a_1 m + a_2 m$,
3. $a(m_1 + m_2) = am_1 + am_2$,
4. $(ab)m = a(bm)$.

N is a submodule of M if N is an A-stable subgroup of M. For any submodule N, we can construct the quotient module M/N.

A map $f : M \to N$ is an A-module morphism if it is A-linear, i.e. $f(m_1 + m_2) = f(m_1) + f(m_2)$ and $f(am) = af(m)$.

Given an A-module morphism $f : M \to N$, then $\ker(f) = f^{-1}(0)$ is a submodule of M, and $\operatorname{im}(f)$ is a submodule of N. An isomorphism is a bijective A-module morphism.

Examples.

1. Let $A = \mathbb{Z}$. A $\mathbb{Z}$-module is just an abelian group. For any abelian group M, any $k \in \mathbb{Z}_{\geq 0}$ and $m \in M$, we set
$$km = \underbrace{m + \cdots + m}_{k \text{ times}}.$$
2. Let $A = k$ a field. Then k-modules are just k-vector spaces.
3. Let $A = k[x]$ where k is a field. Then an A-module is just a k-vector space V equipped with a k-linear map $\widehat{x} : V \to V$.
4. Let $A = k[x]/(x^4 - 1)$. Then an A-module is just a k-vector space V equipped with a k-linear map $\widehat{x} : V \to V$ satisfying $\widehat{x}^4 = \mathrm{id}_V$.
5. Let $A = k[x, y]$. Then an A-module is just a k-vector space V equipped with two **commuting** k-linear maps $\widehat{x}, \widehat{y} : V \to V$.
6. Let $A = k\langle x, y\rangle$. Then an A-module is just a k-vector space V equipped with two arbitrary k-linear maps $\widehat{x}, \widehat{y} : V \to V$.

Operations on modules

1. The direct sum of modules M_1, M_2 is defined to be
$$M_1 \oplus M_2 = \{(m_1, m_2) \mid m_1 \in M_1, m_2 \in M_2\}.$$
The action of A is given by $a(m_1, m_2) = (am_1, am_2)$. For any collection of A-modules $\{M_i\}_{i \in I}$, we can form
$$\bigoplus_{i \in I} M_i = \{(m_i \in M_i)_{i \in I} \mid m_i = 0 \in M_i \text{ for almost all } i\}.$$

We define

$$M^n = \underbrace{M \oplus \cdots \oplus M}_{n \text{ times}}.$$

2. The sum of submodules $M_i \subseteq M$ is defined to be

$$\sum_{i \in I} M_i = \{m_{i_1} + \cdots + m_{i_j} \mid m_{i_j} \in M_{i_j}\}.$$

3. The submodule generated by $m \in M$ is defined to be

$$Am = \{am \mid a \in A\}.$$

More generally, if $\{m_i\}_{i \in I} \subset M$, then

$$\sum_{i \in I} Am_i \subset M$$

is the submodule generated by the m_i. We say that M is finitely generated if there exist $m_1, \ldots, m_k \in M$ such that $M = Am_1 + \cdots + Am_k$.

Free modules

Note that A is an A-module via left multiplication. Modules of the form

$$\bigoplus_{i \in I} A$$

are called free modules. We say that A^n is a free module of rank n.

An important observation to make is that there are modules which are not free. For example, we can choose $A = k[t]$ and then let V be any finite-dimensional k-vector space, with $\widehat{x}$ being an arbitrary linear map $V \to V$.

Definition. We say that $\{m_i \in M\}_{i \in I}$ is a basis of M if every element of M can written **uniquely** in the form $m = \sum a_i m_i$ (this is a finite sum), where the $a_i \in A$. For example, if $M = \bigoplus_{i \in I} A$, then the standard basis for M is $\{1_i \in A \mid i \in I\}$.

However, this is not a very general definition, because in fact an A-module has a basis $\{m_i\}_{i \in I}$ if and only if M is free; we can make an isomorphism

$$\bigoplus_{i \in I} A \xrightarrow{\cong} M$$

defined by sending $(a_i)_{i \in I}$ to $\sum a_i m_i$.

Note that M is finitely generated if and only if there is a surjection $A^n \to M$ for some free module of finite rank A^n.

Let $\{m_1, \ldots, m_n\}$ be a basis of M. Let $|a_{ij}| \in M_n(A)$, and put

$$m_i' = \sum_{j=1}^{n} a_{ij} m_j.$$

Then $\{m_i'\}$ is a basis for M if and only if $|a_{ij}|$ is invertible.

Morphisms of modules

Let A be a ring. We define

$$\mathrm{Hom}_A(M, N) = \{\text{morphisms } M \to N\}.$$

Note that $\mathrm{Hom}_A(M, N)$ is an abelian group (under pointwise addition of functions). If A is commutative, then $\mathrm{Hom}_A(M, N)$ has a natural A-module structure: for $a \in A$ and $f \in \mathrm{Hom}_A(M, N)$, we define $af \in \mathrm{Hom}_A(M, N)$ by $(af)(m) = a \cdot f(m)$. When A is not commutative, then the requirement that module morphisms satisfy $g(bm) = b \cdot g(m)$ will fail for af when a is not in the center of A.

For any module M, we have that $\mathrm{Hom}_A(A, M) \longleftrightarrow M$, via $f \mapsto f(1_A)$ and $[f_m : x \mapsto xm] \leftarrow\!\shortmid m$. This is not an isomorphism of modules unless A is commutative, because otherwise $\mathrm{Hom}_A(A, M)$ doesn't have the structure of a left A-module.

For any A-module M, we define $\mathrm{End}_A(M) = \mathrm{Hom}_A(M, M)$. This is a ring with the multiplication being composition.

Example. $\mathrm{End}_A(A) \cong A^{op}$ as rings, with $a \in A \longleftrightarrow f_a$:

$$f_{ba} = f_a \circ f_b : x \mapsto xba,$$

and in A^{op}, we have $a * b = ba$ (we are considering A as a left A-module, so its endomorphisms are the **right**-multiplication maps $f_a(x) = xa$; left-multiplication is not an A-module homomorphism from A to itself). When A is commutative, then $A^{op} \cong A$. If $a \mapsto a^*$ is an anti-involution, then we get an isomorphism $A \to A^{op}$, but this can be non-trivial; as we've seen with the quaternions, there can be an anti-involution of a non-commutative ring A.

Let M be an A-module. Consider an $f \in \mathrm{Hom}_A(M^p, M^q)$, say mapping

$$\begin{pmatrix} m_1 \\ \vdots \\ m_p \end{pmatrix} \xrightarrow{q\times p \text{ matrices}} \begin{pmatrix} m_1' \\ \vdots \\ m_q' \end{pmatrix}$$

What kind of things are in the entries of this matrix? Elements of $\mathrm{End}_A(M)$. We have

$$\mathrm{End}_A(M^p) \cong M_p(\mathrm{End}_A(M))$$

so for example

$$\mathrm{End}_A(A^p) \cong M_p(A^{op}).$$

Note that this means there is a difference between a matrix that represents changing bases and a matrix that represents a map of modules.

Example (not from class)**.** If we have a free module A^n and three different bases for it, $\{e_i\}$, $\{v_i\}$, and $\{w_i\}$ (these need not have the same cardinality), with a_{ij}, b_{ij}, c_{ij} defined by $v_i = \sum a_{ij} e_j$, $w_i = \sum b_{ij} v_j$, and $w_i = \sum c_{ij} e_j$, then

$$(c_{ij}) = (b_{ij})(a_{ij})$$

where, when doing matrix multiplication, the elements of matrices are to be multiplied as elements of A. However, given a module homomorphism $f : A^n \to A^n$, we represent it as a matrix (f_{ij}) where

$f_{ij} \in \mathrm{End}_A(A) \cong A^{op}$ is the map obtained by restricting the domain and codomain of f to the ith and jth factors, respectively, and the matrix representing $g \circ f$ satisfies

$$((g \circ f)_{ij}) = (g_{ij})(f_{ij})$$

where now, when doing matrix multiplication, the entries of the matrices are to be multiplied as elements of A^{op}.

Some final remarks: a submodule $M \subset A$ is just a left ideal of A. We say that a submodule M is cyclic if there is an $m \in M$ such that $M = Am$. Cyclic modules are of the form $M \cong A/J$ where J is a left ideal in A. This is because $A/J = A\bar{1}$, and if $M = Am$, then we can define a surjective map $f : A \to M$ by $a \mapsto am$, so that $M \cong A/\ker(f)$.

Lecture 3 (2012-10-05)

Today we'll be talking about modules over PIDs.

Proposition. *Let M be a free module of rank m, let L be a submodule of rank L. Then there exists a basis $m_1, \ldots, m_n$ of M and $d_1, \ldots, d_k \in A$ for some $k \leq n$, such that the elements $d_1 m_1, \ldots, d_k m_k$ form a basis of L. In particular, L is free, with* $\operatorname{rank}(L) = k \leq \operatorname{rank}(M)$.

Theorem. *Any finitely generated module over a PID A is a finite direct sum of cyclic modules of the form*

$$M = \bigoplus_{i=1}^{n} A/(p_i^{d_i})$$

where each p_i is either zero, or else is a prime in A. Moreover, the collection of pairs

$$\{(p_1, d_1), \ldots, (p_k, d_k)\}$$

(counted with multiplicities) is uniquely determined by M up to permutations and replacing any p_i by $p_i u_i$ where $u_i \in A$ is a unit.

Proof. First, note that the proposition implies the existence part of the theorem.

Let N be a finitely generated A-module. We know there exists a surjection $f : A^n \to N$, so that $N \cong A^n / \ker(f_n)$. Now let $M = A^n$ and $L = \ker(f)$.

In the basis $m_1, \ldots, m_n$, we have

$$\begin{aligned} M &= \overset{1}{A} \oplus \cdots \oplus \overset{k}{A} \oplus \cdots \oplus \overset{n}{A} . \\ L &= d_1 A \oplus \cdots \oplus d_k A \end{aligned}$$

and therefore

$$N = M/L = A/d_1 A \oplus \cdots \oplus A/d_k \oplus A \oplus \cdots \oplus A.$$

It suffices to show that any A/dA can be decomposed in a direct sum as in the theorem. We write $d = p_1^{k_1} \cdots p_r^{k_r}$, where $p_i \neq p_j$ for $i \neq j$. By the Chinese Remainder Theorem,

$$A/dA = A/(p_1^{r_1} \cdots p_r^{k_r}) \cong \bigoplus_{i=1}^{r} A/(p_i^{k_i}). \qquad \square$$

Corollary. *Any finitely generated abelian group is isomorphic to*

$$\mathbb{Z}^\ell \oplus \bigoplus_{i=1}^{n} \mathbb{Z}/(p_i^{d_i})$$

where the $p_i \in \mathbb{Z}$ are some primes.

Proof. Simply apply the theorem in the case $A = \mathbb{Z}$. $\square$

Now let $A = k[x]$, and let $f = x^n + c_{n-1} x^{n-1} + \cdots + c_0 \in k[x]$, $f \neq 0$. Let $M = k[x]/(f)$. Then we can choose $1, x, \ldots, x^{n-1}$ as a k-basis of M. Multiplication by x sends

$$1 \longrightarrow x \longrightarrow x^2 \longrightarrow \cdots \longrightarrow x^{n-1} \longrightarrow x^n = -(c_{n-1} x^{n-1} + \cdots + c_0)$$

(because $f = 0$ in M). Thus, the multiplication by x operator has matrix

$$\begin{bmatrix} 0 & 1 & & & & 0 \\ & 0 & 1 & & & 0 \\ & & \ddots & \ddots & & 0 \\ & & & & 1 & 0 \\ & & & & 0 & 0 \\ -c_0 & -c_1 & & \cdots & & -c_{n-1} \end{bmatrix}$$

(this may or may not be reversed depending on how you think about your vectors).

Corollary. *For any field k, a matrix $X \in M_n(k)$ is conjugate to a block diagonal matrix with Frobenius blocks.*

Proof. For any associative algebra A and $X \in A$, we can map $k[x] \to A$ by $f \mapsto f(X)$. In our case, we get a homomorphism $k[x] \to M_n(k)$ by sending x to X. This gives an action of $k[x]$ on k^n, so that we get a $k[x]$-module structure on k^n. Now apply the theorem. $\square$

Now suppose that our field k is algebraically closed. Then $f \in k[x]$ is a prime power if and only if it is of the form $f = (x - z)^d$ for some $z \in k$ and $d \geq 1$.

Corollary. *Any $k[x]$-module which is finite-dimensional over the algebraically closed field k is isomorphic, as a $k[x]$-module, to*

$$\bigoplus_{i=1}^{n} k[x]/(x - z_i)^{d_i}$$

for some $z_1, \dots, z_n \in k$, and $d_i > 0$.

Note that we cannot have $k[x]/(0) \cong k[x]$ because we are considering only those $k[x]$-modules that are finite-dimensional as k-vector spaces.

Now let's see how this works with matrices. The $k[x]$-module $k[x]/(x - z)^d$ has as a k-basis

$$1, (x - z), \dots, (x - z)^{d-1}.$$

Multiplication by x acts by

$$(x - z)^i \longrightarrow x(x - z)^i = (x - z)^{i+1} + z(x - z)^i.$$

Thus, the matrix for multiplication by x is

$$\begin{bmatrix} z & 1 & & & \\ & z & 1 & & \\ & & \ddots & \ddots & \\ & & & & 1 \\ & & & & z \end{bmatrix}$$

Corollary. *If k is algebraically closed, then any matrix $X \in M_n(k)$ is conjugate to one in Jordan normal form.*

Suppose that $A = A_1 \oplus \cdots \oplus A_n$ is a direct sum of rings. Let M_i be an A_i-module. Then $M = \bigoplus M_i$ has a natural A-module structure, via

$$(a_1, \dots, a_n)(m_1, \dots, m_n) = (a_1 m_1, \dots, a_n m_n).$$

Lemma. *Any module over $A = A_1 \oplus \cdots \oplus A_n$ has the form $M = \bigoplus M_i$ for some A_i modules M_i.*

Proof. We have orthogonal idempotents in A, i.e. elements $e_i \in A$ such that

- $1_A = e_1 + \cdots + e_n$,
- $e_i^2 = e_i$,
- $e_i e_j = 0$ if $i \neq j$, and
- the e_i are central in A.

Specifically, we have the identity elements $e_i = 1_{A_i}$. Now, given an A-module M, put $M_i = e_i M_i$. For any $m \in M$, we have

$$m = 1_A \cdot m = \sum e_i m$$

so that $M = \sum M_i$. If $0 = \sum_{i=1}^n e_i m$ holds in M, then $e_i m = 0$ for all i, because for each $j \neq i$,

$$0 = e_j \cdot 0 = e_j \sum_{i=1}^n e_i m = \sum_{i=1}^n e_j e_i m = e_j^2 m = e_j m. \qquad \square$$

Let X be a finite set, k is a field. Let $A = k\{X\} = k$-valued functions on X. We see that

$$k\{X\} \xrightarrow{\cong} \bigoplus_{\#X} k$$

via the map sending f to $\oplus_{x \in X} f(x)$. Our lemma says that a module over $k\{X\}$, for X finite, is the same as a direct sum of $\#X$ k-vector spaces.

Lecture 4 (2012-10-08)

Today we'll talk about simple and semisimple modules.

Simple modules

Definition. A module is simple if it is non-trivial and has no submodules except 0 and itself.

Example. If our ring is a field k, then a k-module M is simple if and only if M is cyclic, which is the case if and only if $\dim_k(M) = 1$.

Note that an A-module is simple if and only if $M = Am$ for any non-zero $m \in M$.

Definition. A (left) ideal $J \subsetneq A$ is called maximal if, for any ideal $I \supseteq J$, we have $A = I$.

Lemma. *M is a simple A-module if and only if $M \cong A/J$ for some maximal (left) ideal J of A.*

Proof. There is a bijection between left submodules $I/J \subseteq A/J$ and ideals $J \subseteq I \subseteq A$:

$$\begin{array}{ccc} A & \longrightarrow & A/J \\ \cup\!\shortmid & & \cup\!\shortmid \\ I & \longrightarrow & I/J \\ \cup\!\shortmid & & \cup\!\shortmid \\ J & \longrightarrow & 0 \end{array}$$

□

Proposition. *Any (left) ideal $I \subsetneq A$ is contained in a maximal ideal.*

Proof. Zorn's lemma. □

Corollary. *Any cyclic module has a simple quotient.*

Warning. If N is a submodule in M, it isn't necessarily true that there exists a maximal submodule N' of M with $N \subseteq N'$.

Exercise. Show that $(\mathbb{Q}/\mathbb{Z}, +)$ has no maximal subgroups.

Theorem (Schur's lemma)**.** *If M, N are simple A-modules, then any morphism $f : M \to N$ is either 0 or is an isomorphism.*

Proof. Assume that $f \neq 0$. Then $\mathrm{im}(f) \neq 0$ is a submodule in N, hence $\mathrm{im}(f) = N$, i.e. f is surjective. Because $\ker(f) \neq M$, we must have $\ker(f) = 0$, hence f is injective. □

Corollary. *For a simple module M, the ring $\mathrm{End}_A(M)$ is a division ring.*

Proof. Every $f \neq 0$ in $\mathrm{End}_A(M)$ is an isomorphism. □

Corollary. *If A is commutative, then an ideal $I \subset A$ is maximal if and only if A/I is a field.*

Proof. If I is maximal, then A/I is a simple A-module, so that $\mathrm{End}_A(A/I) \cong A/I$ is a division ring, and hence a field.

If A/I is a field, then A/I is generated by every non-zero element, hence A/I is simple, hence I is maximal (by our lemma). □

Corollary. *If A is commutative, and $n \neq m$, then $A^n \ncong A^m$ as A-modules.*

Proof. Pick a maximal ideal $I \subset A$. If M is an A-module, we can consider M/IM as an A/I-module. In particular we get

$$(A/I)^n \cong A^n/I \cdot A^n \cong A^m/I \cdot A^m \cong (A/I)^m$$

but these are vector spaces over A/I, so we must have $m = n$. ☐

This is false for non-commutative rings in general. A good counterexample can be obtained by taking an infinite dimensional vector space V over a field k, and letting $A = \mathrm{End}_k(V)$. Then $A^n \cong A$ for all $n \geq 1$.

Semisimple modules

Definition (and Proposition)**.** For M an A-module, the following are equivalent:

1. $M \cong \oplus$ simple modules
2. $M = \sum$ simple submodules
3. M is completely reducible, i.e. for any submodule $N \subset M$, there is an $N' \subset M$ such that $N \oplus N' = M$.

Proof. Zorn's lemma. ☐

If (1)-(3) hold then M is called semisimple.

Examples. If $A = k$ is a field, then any module is semisimple.

If A is a division ring, then any module is semisimple.

If $A = \mathrm{M}_n(D)$ where D is a division ring, then any A-module is semisimple.

Corollary. *Any direct sum, quotient, or submodule of a semisimple module is semisimple.*

Proof. The case of submodules follows from (3). The case of quotients follows from (2). The case of direct sums follows from (1). ☐

Notation. If $M = \bigoplus_i M_i$, where the M_i's are simple, then we set for a simple L

$$[M : L] = \#\{i \mid M_i \cong L\}.$$

It's not necessarily clear this is well-defined; an alternative is to write M as

$$M = \bigoplus_{L \in S_A} L^{[M:L]}$$

where S_A is the set of isomorphism classes of simple A-modules.

For any A-modules M and N, the ring $\mathrm{End}_A(N)$ acts (on the right) by composition on $\mathrm{Hom}_A(M, N)$.

Let L be a simple module. Then $D_L := \mathrm{End}_A(L)$ is a division ring by Schur's lemma, so that $\mathrm{Hom}_A(M, L)$ is a D_L-module.

Proposition (Multiplicity formula)**.** *For a semisimple module M,*

$$[M : L] = \mathrm{rank}_{D_L}(\mathrm{Hom}(M, L)).$$

Proof. Assume $M = \bigoplus M_i$, where M_i are simple. Then

$$\mathrm{Hom}_A(M, L) = \mathrm{Hom}_A\left(\bigoplus M_i, L\right) = \bigoplus \mathrm{Hom}_A(M_i, L) \cong \bigoplus_{\{i \mid M_i \cong L\}} \mathrm{End}_A(L) = D_L^{[M:L]}. \qquad \square$$

Let $M = L_1^{r_1} \oplus \cdots \oplus L_n^{r_n}$ where the L_i are simple and $L_i \ncong L_j$. Then

$$\begin{aligned} \mathrm{End}_A(M) &= \mathrm{Hom}(M, L_1^{r_1}) \oplus \cdots \oplus \mathrm{Hom}(M, L_n^{r_n}) \\ &= \mathrm{Hom}(M, L_1)^{r_1} \oplus \cdots \oplus \mathrm{Hom}(M, L_n)^{r_n} \\ &= \mathrm{M}_{r_1}(D_{L_1}) \oplus \cdots \oplus \mathrm{M}_{r_n}(D_{L_n}). \end{aligned}$$

Lecture 5 (2012-10-10)

A ring A is said to be semisimple when any A-module is semisimple.

Theorem (Wedderburn Theorem)**.** *For a ring A, the following conditions are equivalent:*

1. *A is a finite direct sum*
$$A = \mathrm{M}_{r_1}(D_1) \oplus \cdots \oplus \mathrm{M}_{r_n}(D_n)$$
where the D_i are division rings.
2. *A is semisimple.*
3. *The rank 1 free A-module is semisimple.*
4. *Any left ideal in A has the form Ae where $e^2 = e \in A$.*
5. *$A = Ae_1 + \cdots + Ae_n$ where $e_i^2 = e_i$ and $e_ie_j = 0$ for $i \neq j$, and each Ae_i is a simple A-module.*

($1 \Rightarrow 2$). The fact that any module over $\mathrm{M}_r(D)$ is semisimple is something that is from your homework. Now note that if $A = A_1 \oplus \cdots \oplus A_n$, then an A-module is equivalent to an n-tuple $\{M_i\}$ where M_i is an A_i-module, so that because each $\mathrm{M}_{r_i}(D_i)$ is semisimple, so is $\mathrm{M}_{r_1}(D_1) \oplus \cdots \oplus \mathrm{M}_{r_n}(D_n)$. ☐

($2 \Rightarrow 3$). Clear. ☐

($3 \Rightarrow 4$). A is completely reducible as an A-module, so for any left ideal $I \subset A$, there exists a left ideal $I' \subset A$ such that $A = I \oplus I'$. Thus, there are $e \in I$ and $e' \in I'$ such that $1 = e + e'$. Now note that for any $x \in I$,
$$\underbrace{x}_{\in I} = x \cdot 1 = \underbrace{x \cdot e}_{\in I} + \underbrace{x \cdot e'}_{\in I'}$$
which implies that $x \cdot e'$ and $x = xe$. Thus, I is of the form Ae, and $e = e^2$. ☐

($4 \Rightarrow 5$). Since any left ideal $I \subset A$ has the form $I = Ae$ where $e^2 = e$, we have for any ideal Ae that $A = Ae \oplus A(1-e)$. Thus, A is completely reducible.

This implies that $A = \bigoplus L_i$, a possibly infinite direct sum of simple A-modules. But then $1 = e_1 + \cdots + e_n$, hence $x = x \cdot 1 = xe_1 + \cdots + xe_n$ where $xe_i \in L_i$. Thus $A = L_1 \oplus \cdots \oplus L_n$. ☐

($5 \Rightarrow 1$). Reexpressing the statement of 5, we have that
$$A = \bigoplus_{j=1}^{m} L_i^{r_i}, \qquad L_i \ncong L_j \text{ for } i \neq j.$$
Therefore
$$A^{\mathrm{op}} = \mathrm{End}_A(A) = \bigoplus_{j=1}^{m} \mathrm{End}(L_j^{r_j}) = \bigoplus_{j=1}^{m} \mathrm{M}_{r_j}(\mathrm{End}_A(L_i))$$
and by Schur's lemma, $D_i = \mathrm{End}_A(L_i)$ is a division ring. But this gives a decomposition of A^{op}, not A. To fix this, note that
$$A = (A^{\mathrm{op}})^{\mathrm{op}} = \bigoplus_{j=1}^{m} \mathrm{M}_{r_j}(D_j)^{\mathrm{op}}$$
that $\mathrm{M}_r(D)^{\mathrm{op}} = \mathrm{M}_r(D^{\mathrm{op}})$, and that D^{op} is a division ring when D is. ☐

Corollary. *A commutative ring A is semisimple if and only if it is a finite direct sum of fields.*

Proof. There is no way to get a commutative ring if any of the $r_i > 1$, nor if any of the D_j are non-commutative division algebras. $\square$

From this point forward, let A be a k-algebra where k is a field.

Definition. An element $a \in A$ is called algebraic if there is some monic $p \in k[t]$ such that $p(a) = 0$.

Examples.

- Any idempotent or nilpotent element is algebraic.
- If $\dim_k(A) < \infty$ then any $a \in A$ is algebraic, because $1, a, a^2, \ldots$ cannot be linearly independent over k. Thus, there exist some $\lambda_i \in k$ such that $\sum \lambda_i a^{n_i} = 0$.

Let $a \in A$ be an algebraic element. Consider the k-algebra homomorphism $j : k[t] \to A$ defined by $j(f) = f(a)$. Because $k[t]$ is a PID, we have that $\ker(j) = (p_a)$ is a principal ideal. The monic polynomial p_a is called the minimal polynomial for a. Note that we get an induced homomorphism $j : k[t]/(p_a) \hookrightarrow A$.

Definition. For any $a \in A$, we define

$$\operatorname{spec}(a) = \{\lambda \in k \mid \lambda - a \text{ is not invertible}\}.$$

Examples.

- If $A = k\{X\}$, then $\operatorname{spec}(a) = \{\text{the values of } a\}$.
- If k is algebraically closed and $A = \mathrm{M}_n(k)$, then for an $a \in A$, $\operatorname{spec}(a) = \{\text{eigenvalues of } a\}$.

Lemma. *Let $a \in A$ be an algebraic element with minimal polynomial $p_a \in k[t]$. Then*

$$\lambda - a \textit{ is not invertible} \iff \lambda - a \textit{ is a zero divisor} \iff p_a(\lambda) = 0.$$

Thus, $\operatorname{spec}(a) = \{\textit{roots of } p_a\}$.

Proof. First, we make a general remark: for any $\lambda \in k$, we have

$$p(t) - p(\lambda) = q(t)(\lambda - t),$$

and because $\deg(q) < \deg(p)$, we must have $q \notin (p)$, hence $q(a) \neq 0$.

We have an injective homomorphism $j : k[t]/(p) \hookrightarrow A$ where we send f to $f(a)$. If $p(\lambda) = 0$, then

$$0 = p(a) = q(a)(\lambda - a)$$

implies that $\lambda - a$ is a zero-divisor. Clearly, if $\lambda - a$ is a zero-divisor, it is not invertible.

Now we want to show that $\lambda - a$ is not invertible $\implies p(\lambda) = 0$. Assume for the sake of contradiction that $p(\lambda) \neq 0$; then

$$\underbrace{p(a)}_{=0} - \underbrace{p(\lambda)}_{\neq 0} = q(a)(\lambda - a)$$

demonstrates that $\lambda - a$ is invertible. $\square$

Lecture 6 (2012-10-12)

Last time, we proved that for an algebraic element $a \in A$ in an algebra,

$$\operatorname{spec}(a) = \{\text{roots of the minimal polynomial } p_a \in k[t]\}.$$

Let $a^n = 0$, so that a is nilpotent. Then $p_a = t^n$, so that $\operatorname{spec}(a) = \{0\}$. This implies that $\lambda - a$ is invertible for any $\lambda \neq 0$. Let's see if we can find an explicit inverse.

$$\begin{aligned}
(\lambda - a)^{-1} &= [\lambda(1 - \lambda^{-1}a)]^{-1} \\
&= \lambda^{-1}(1 - \lambda^{-1}a)^{-1} \\
&= \lambda^{-1}(1 + (\lambda^{-1}a) + (\lambda^{-1}a)^2 + \cdots) \\
&= \sum_{i=0}^{\infty} \lambda^{-(i+1)} a^i \\
&= \sum_{i=0}^{n-1} \lambda^{-(i+1)} a^i
\end{aligned}$$

The intermediate steps aren't really allowed, but it gets us the right answer.

From now on we consider k-algebras over an algebraically closed field k.

Proposition. *Let A be a finite dimensional k-algebra.*

1. $\operatorname{spec}(a) \neq \varnothing$ *for any $a \in A$.*
2. *If A is a division algebra, then $A \cong k$.*

Proof. For part 1, note that $\dim(A) < \infty$ implies that any $a \in A$ is algebraic, so that $\operatorname{spec}(a) = \{\text{roots of } p_a\}$, which is non-empty because k is algebraically closed.

For part 2, note that for any k-algebra, we have an inclusion $k \hookrightarrow A$ by $\lambda \mapsto \lambda \cdot 1_A$. Suppose that $a \in A \setminus k$. Then for any $\lambda \in k$, we have that $\lambda - a \neq 0$, hence $\lambda - a$ is invertible for all $a \in k$, hence $\operatorname{spec}(a) = \varnothing$; but this contradicts part 1. □

Proposition (Schur lemma for algebras)**.** *Let M be a finite dimensional (over k) simple A-module. Then $\operatorname{End}_A(M) = k$, i.e. any endomorphism $f : M \to M$ is of the form $\lambda \cdot \mathrm{id}_M$ for some $\lambda \in k$.*

Proof. We know that $\operatorname{End}_A(M)$ is a division algebra. The A-action on M is the same as a map $A \to \operatorname{End}_k(M)$, which is a finite dimensional division algebra. Let $A' = \operatorname{im}(A)$, so $\dim(A') < \infty$ and M is a simple A'-module, which implies $\operatorname{End}_{A'}(M) = k$, but $\operatorname{End}_A(M) = \operatorname{End}_{A'}(M)$. □

Corollary.

1. *The center $Z(A)$ of A acts by scalars in any finite-dimensional simple A-module.*
2. *If A is commutative*[1]*, then any simple A-module has dimension 1 over k.*

Proof. Let M be a finite-dimensional simple A-module. Then consider the action map $\operatorname{act} : A \to \operatorname{End}_k(M)$. If $z \in Z(A)$, then $\operatorname{act}(z) \in \operatorname{End}_A(M) = k$ by the Schur lemma for algebras. Part 1 follows.

[1] A reader points out that A also needs to be finite dimensional; otherwise a transcendental field extension of k would provide a counterexample.

If $A = Z(A)$, then any element of A acts on M by scalars, so any vector subspace $N \subseteq M$ is A-stable. Thus, $\dim_k(M) = 1$. $\square$

Let S_A be the isomorphism classes of simple A-modules.

Let M be a finite direct sum of simple modules, so

$$M \cong \bigoplus_{L \in S_A} L^{n(L)}$$

For any A-module N, we have an evaluation map $\mathrm{ev} : \mathrm{Hom}_A(N, M) \otimes_k N \to M$, defined by sending $f \otimes n$ to $f(n)$.

Now M is a finite direct sum of simple modules, so we get an evaluation map

$$\bigoplus_{L \in S^A} \mathrm{Hom}_A(L, M) \otimes_k L \xrightarrow{\cong} M$$

by the Schur lemma.

Theorem (Wedderburn Theorem for Algebras)**.** *A is a finite-dimensional semi-simple k-algebra if and only if*

$$A \cong \mathrm{M}_{r_1}(k) \oplus \cdots \oplus \mathrm{M}_{r_n}(k).$$

Proof. By Wedderburn's theorem, we have

$$A \cong \mathrm{M}_{r_1}(D_1) \oplus \cdots \oplus \mathrm{M}_{r_n}(D_n)$$

where the D_i are division rings. The fact that $\dim_k(A) < \infty$ implies $\dim_k(D_i) < \infty$ which implies that $D_i = k$. $\square$

Corollary. *Let A be a finite-dimensional semisimple algebra. Then*

1. *S_A is a finite set and any $M \in S_A$ is finite dimensional over k. Moreover, $[A : L] = \dim(L)$ for all $L \in S_A$.*
2. $\dim(A) = \sum_{L \in S_A} \dim(L)^2$

Proof. Any simple A-module is cyclic, so that it is isomorphic to A/J for some J. We have $\dim_k(A/J) \leq \dim_k(A) < \infty$, so any simple A-module is finite dimensional.

Note that A satisfies a universal property, $\mathrm{Hom}_A(A, L) \xrightarrow{\cong} L$ is an isomorphism of k-vector spaces.

We can decompose $A = \bigoplus_{L \in S_A} L^{n_L}$. We get that, for any simple L',

$$\mathrm{Hom}_A(L', A) = \mathrm{Hom}_A\left(L', \bigoplus_{L \in S_A} L^{n_L}\right) = \bigoplus_{L \in S_A} \mathrm{Hom}(L', L)^{n_L} = \bigoplus_{L \in S_A} \begin{pmatrix} k \text{ if } L = L' \\ 0 \text{ if } L \neq L' \end{pmatrix}^{n_L} = k^{n_{L'}}.$$

By the same argument we also have

$$\mathrm{Hom}_A(A, L') = \mathrm{Hom}_A\left(\bigoplus_{L \in S_A} L^{n_L}, L'\right) = \bigoplus_{L \in S_A} \mathrm{Hom}(L, L')^{n_L} = \bigoplus_{L \in S_A} \begin{pmatrix} k \text{ if } L = L' \\ 0 \text{ if } L \neq L' \end{pmatrix}^{n_L} = k^{n_{L'}}.$$

Because $\mathrm{Hom}_A(A, L) \cong L$ as k-vector spaces, we therefore have that $\dim(L') = \dim(\mathrm{Hom}_A(A, L')) = n_{L'}$, and hence

$$\dim(A) = \sum n_L \dim(\mathrm{Hom}_A(L, A)) = \sum n_L \dim(L) = \sum \dim(L)^2. \qquad \square$$

Lecture 7 (2012-10-15)

Integration on topological groups

Let X be a locally compact topological space, i.e. any point has a compact neighborhood.

Let $C(X)$ be the space of continuous functions $X \to \mathbb{C}$. Let $C_c(X)$ be the subspace of $C(X)$ consisting of functions with compact support.

An integral on X is a linear functional $\int : C_c(X) \to \mathbb{C}$ satisfying

- If $f(x) \geq 0$ for all x, then $\int f \geq 0$, and $\int f = 0 \iff f = 0$.
- Continuity: for every compact $K \subseteq X$, there exists a constant $C_K \geq 0$ such that for all $f \in C_c(X)$ with $\operatorname{supp}(f) \subseteq K$, $|\int_K f| \leq C_K \cdot \max\limits_{x \in K} |f(x)|$.

If X is actually compact, then clearly $C_c(X) = C(X)$ and $\operatorname{vol}(X) = \int 1$. Moreover, Fubini's theorem guarantees that

$$\int_Y \left(\int_X f(x,y)\, dx \right) dy = \int_X \left(\int_Y f(x,y)\, dy \right) dx.$$

A topological group G is a group that is a topological space such that multiplication $m : G \times G \to G$ and inversion $i : G \to G$ are continuous.

Examples. $(\mathbb{R}, +)$, $(\mathbb{C}^\times, \cdot)$, $(\mathbb{S}^1, \cdot)$, $(\mathrm{GL}_n(\mathbb{R}), \cdot)$, $(\mathrm{U}(\mathbb{R}^n), \cdot)$

When we say that a topological group G acts on a topological space X, we require that the action map is continuous.

Given a function $f : X \to \mathbb{C}$ and a $g \in G$, define $g^* f(x) = f(g^{-1}x)$. We say that an integral on X is G-invariant if $\int_X g^*(f) = \int_X f$ for all $f \in C_c(X)$ and for all $g \in G$. Alternatively, when thinking about measures, we say that a measure μ is G-invariant if for all $S \subseteq X$ and $g \in G$, we have $\operatorname{vol}(gS) = \operatorname{vol}(S)$.

Theorem (Haar)**.** *Any locally compact topological group G has a left-invariant integral which is unique up to a constant factor.*

Examples. Some examples of integrals which can be obtained this way:

1. $(\mathbb{R}, +)$ with dx,
2. $(\mathbb{R}^+, \cdot)$ with $d\mu = \frac{dx}{x}$,
3. (S^1, θ) with $d\theta$.

Using differential forms (on Lie groups say), this theorem is obvious.

Note that a left-invariant integral is not necessarily right-invariant.

Proposition. *If G is a compact group, then G is unimodular (i.e. a left-invariant integral on G is automatically right-invariant).*

Proof. Let $\int_L$ be a left-invariant integral on a compact group G. Let $f \in C(G)$. Then define $\phi : G \to \mathbb{C}$ by $\phi(g) = \int_L f(xg)dx$. Notice that $\phi(g)$ is also a left-invariant integral. Therefore, there is a constant $c(g) \in \mathbb{C}$ such that

$$\int_L f(xg)dx = c(g) \int_L f(x).$$

Then $c(g)$ has the following properties,

1. $g \to c(g)$ is continuous on G (to see this, just plug in $f = 1$).
2. $c(g) > 0$ for all g.
3. $g \to c(g)$ is a group homomorphism into the multiplicative group of $\mathbb{R}$.

Thus, $c(g) = 1$ since the image of $c : G \to \mathbb{R}^+$ is a compact subgroup of $\mathbb{R}^+$, hence 1. $\square$

The group algebra

If G is a finite group and k is a field, then kG is a k-vector space with basis $g \in G$ and with obvious multiplication. Alternatively, the group algebra $k\{G\}$ is the set of functions $G \to k$ with convolution and addition, i.e.

$$(\phi * \psi)(x) = \sum_{g \in G} \phi(xg^{-1})\psi(g)$$

Proposition. *For a finite group G, $k\{G\} = kG$.*

Proof. The elements 1_g form a basis of $k\{G\}$, and $1_g * 1_h = 1_{gh}$. $\square$

Now let G be a locally compact topological group with left-invariant integral $\int$, and let k be a topological field. For $\phi, \psi \in C_c(G)$, define[2]

$$(\phi * \psi)(x) = \int_G \phi(xy^{-1})\psi(y)dy.$$

Comments.

1. Any discrete group is locally compact (discrete topology), but then $C_c(G)$ only includes functions with finite support.
2. If G is not discrete, then 1_g is not a continuous function.
3. If G is discrete (e.g. if G is finite), the unit of the group algebra is the function 1_e. If G is not discrete, then in fact there is no unit!

[2] A reader suggests that if G is not unimodular, convolution should be defined using $\phi(y)\psi(y^{-1}x)$, not the other way around, making the action on a representation a left action.

Lecture 8 (2012-10-17)

Let V be a vector space over k.

Definition. A representation of a group G is a group homomorphism $\rho : G \to \mathrm{GL}(V)$. This is equivalent to a linear G-action on V.

Observe that this is also equivalent to specifying a kG-module structure on V. If ρ is a group representation of G, then we declare that $a = \sum_{g\in G} c_g g \in kG$ will act on V via

$$\rho(a) = \sum_{g\in G} c_g \rho(g) : V \to V$$

or in other words, for all $v \in V$,

$$\rho(a)v = \sum_{g\in G} c_g \rho(g)v.$$

(Note that sometimes we'll just write av instead of $\rho(a)v$). Using this view, we have the notions of a subrepresentation, quotient representation, and direct sum of representations. An "irrep" is a simple kG-module, and an "intertwiner" is a morphism of kG-modules.

Theorem (Schur Lemma for Representations)**.** *Given an algebraically closed field k, let V_1, V_2 be finite-dimensional irreps. Let $f : V_1 \to V_2$ be an intertwiner. If $V_1 \not\cong V_2$, then $f = 0$, and if $V_1 \cong V_2$, then $f = \lambda \cdot \mathrm{id}_V$ for some $\lambda \in k$.*

Proof. Apply the Schur lemma for algebras to kG. □

From now on let $k = \mathbb{C}$. Let V be a vector space over $\mathbb{C}$ with a positive definite hermitian inner product $(\cdot, \cdot)$.

Definition. A unitary representation of G in V is a homomorphism $G \to \mathrm{U}(V) \subset \mathrm{GL}(V)$, or in other words, a linear G-action on V by isometries.

Lemma. *Any unitary representation is completely reducible.*

Proof. Let $W \subset V$ be a subrepresentation. We have that $V = W \oplus W^\perp$. We need to show that $W^\perp$ is G-stable.

Let $x \in W^\perp$. We need to check that $(\rho(g)x, W) = 0$. Note a very important fact:

$$\boxed{\rho \text{ is unitary } \iff \rho(g)^* = \rho(g)^{-1} = \rho(g^{-1})}$$

Thus

$$(\rho(g)x, W) = (x, \rho(g)^* W) = (x, \rho(g^{-1})W \subset (x, W) = 0,$$

and thus $W^\perp$ is a subrepresentation of V. □

Now let's consider representations of topological groups. Let G be a topological group, and let V be a finite dimensional vector space over $\mathbb{C}$. Then $\mathrm{GL}(V) \subset \mathrm{End}_{\mathbb{C}}(V) \cong \mathbb{C}^{\dim(V)^2}$, and this inclusion is in fact an open embedding.

Definition. A representation of G in V is a continuous representation of G.

More concretely, a representation of G in $\mathbb{C}^n$ is a homomorphism $\rho : G \to \mathrm{GL}_n(\mathbb{C})$, with $g \mapsto (\rho_{ij}(g))$, and this is continuous if and only if for each $1 \le i, j \le n$, $g \mapsto \rho_{ij}(g)$ is a continuous function from G to $\mathbb{C}$.

As we discussed last time, the natural candidate for the group algebra over a topological group is the algebra $C_c(G)$ with convolution as the product. Fix a left-invariant integral $\int$ on G. Then any representation $\rho : G \to \mathrm{GL}(V)$ gives V a $(C_c(G), *)$-module structure: for $f \in C_c(G)$, define

$$\rho(f) = \int f(g)\rho(g) \in \mathrm{End}_{\mathbb{C}}(V).$$

(Squirrels try to get into the classroom. Ginzburg relates that he once found a squirrel in his office that he gave nuts to.)

If $V = \mathbb{C}^n$, then

$$\rho(f)_{ij} = \int f(g)\rho_{ij}(g),$$

and

$$\rho(f)v = \int f(g)(\rho(g)v).$$

Lemma. *Let $\rho : G \to \mathrm{GL}(V)$ be a continuous representation, and let $W \subset V$ be a $C_c(G)$-stable subspace. Then in fact W is G-stable, so it is a subrepresentation.*

(Note that unless G is discrete, we have $1_g \notin C_c(G)$ for all $g \in G$, so this isn't obvious.)

Proof. Given $g \in G$, we could recover the action of the group element using a delta function,

$$\int \delta_{g_0}(g)\rho(g) = \rho(g_0).$$

Since we aren't doing functional analysis, we can't really use delta functions, but we will try to approximate them anyway.

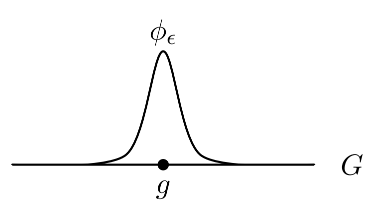
Let U_0 be a compact neighborhood of $g \in G$. Because U_0 is compact, there is some C such that

$$\left| \int_{U_0} f \right| \leq C \cdot \max_{x \in U_0} |f(x)|.$$

For any $\epsilon > 0$, find an open neighborhood U_ϵ of g and a function ϕ_ϵ such that[3]

1. $|\rho(x) - \rho(g)| \leq \epsilon$ for all $x \in U_\epsilon$
2. $\mathrm{supp}(\phi_\epsilon) =$ a compact subset of U_ϵ
3. $\phi_\epsilon \geq 0$
4. $\int \phi_\epsilon = 1$

The standard way of thinking about this is of course



[3]Multiple readers have suggested that G needs to be locally compact and Hausdorff in order to prove that such a function exists.

We claim that

$$\left|\int \phi_\epsilon(x)\rho(x) - \rho(g)\right| \le \epsilon C_0.$$

To see this, note that

$$\left|\int \phi_\epsilon(x)\rho(x) - \rho(g)\right| = \left|\int_G \rho_\epsilon(x)\rho(x) - \int_G \phi_\epsilon(x)\rho(g)\right| \le \int \phi_\epsilon(x)|\rho(x)-\rho(g)| \le C\epsilon$$

Finally,

$$\lim_{n\to\infty} \int \phi_{1/n}(x)\rho(x) = \rho(g).$$

Therefore W is $\rho(g)$-stable. $\square$

Given a G-action on X, we let X^G be the set of G-fixed points.

Lemma (Averaging Lemma)**.** *Let G be a compact group, and let $\rho : G \to \mathrm{GL}(V)$ be a representation. Then the map $V \to V$ defined by*

$$v \mapsto \frac{1}{\mathrm{vol}(G)} \int_G \rho(g)v$$

is a projection to $V^G \subseteq V$. In particular, given a continuous G-action on X and a function $f \in C(X)$, we can define $\mathrm{Av}(f)$ by

$$x \mapsto \int_G f(gx)\, dg = \mathrm{Av}(f)(x),$$

which is a G-invariant function on X.

Proof. We need to check that

1. If $v \in V^G$, then $\frac{1}{\mathrm{vol}(G)} \int \rho(g)v = v$.
2. For all $v \in V$, we have $\frac{1}{\mathrm{vol}(G)} \int \rho(g)v \in V^G$.

For 1, note that if $\rho(g)v = v$ for all g, then

$$\frac{1}{\mathrm{vol}(G)} \int v = \frac{1}{\mathrm{vol}(G)} \cdot \mathrm{vol}(G)v = v.$$

For 2, we have for any $h \in G$ that

$$\rho(h)\int_G \rho(g)v = \int_G \rho(h)\rho(g)v = \int_G \rho(hg)v$$

which, because our measure is left-invariant, is equal to

$$\int \rho(g)v.$$

$\square$

Lecture 9 (2012-10-19)

Last time, we discussed averaging.

Corollary. *Any finite-dimensional representation of a compact group G in a hermitian vector space can be made unitary, i.e. there is a positive definite hermitian form $(\,\cdot\,,\,\cdot\,)$ on V invariant under the group action.*

Proof. Let $\langle\,\cdot\,,\,\cdot\,\rangle : V \times V \to \mathbb{C}$ be the standard hermitian inner product. The group G acts on $V \times V$ diagonally, so we can define $(\,\cdot\,,\,\cdot\,) = \mathrm{Av}\langle\,\cdot\,,\,\cdot\,\rangle$. Explicitly,

$$(v, w) = \int_G \langle gv, gw\rangle\, dg.$$

The integral of a positive function is positive and $\langle\,\cdot\,,\,\cdot\,\rangle$ is positive definite so

$$(v, v) = \int_G \langle gv, gv\rangle\, dg > 0$$

for any $v \neq 0$. □

Theorem. *Any finite-dimensional representation of a compact group is completely reducible.*

Proof. Let $G \to \mathrm{GL}(V)$ be a finite-dimensional representation of a compact group. Let $\langle\,\cdot\,,\,\cdot\,\rangle$ be the standard positive definite inner product. Then the corollary implies that there exists a G-invariant inner product, and any unitary representation is completely reducible. □

Let $\widehat{G}$ be the set of isomorphism classes of finite dimensional irreps of G. Then $\widehat{G}$ is in bijection with $S_{\mathbb{C}G}$, the isomorphism classes of simple $\mathbb{C}G$-modules.

From now on G is finite.

Clearly, finite $\implies$ compact. We declare that $\int 1_x = 1$ for all $x \in G$, so that $\mathrm{vol}(G) = \#G$, and then we have

Theorem (Maschke's Theorem)**.** *$\mathbb{C}G$ is a semisimple algebra.*

This follows directly from our earlier theorem.

Given a group representation $\rho : G \to \mathrm{GL}(L)$, we can extend it to an algebra homomorphism from the group algebra $\rho : \mathbb{C}G \to \mathrm{End}_{\mathbb{C}}(L)$, where

$$\sum_{x \in G} c_x x \mapsto \sum_{x \in G} c_x \rho(x).$$

Applying the Wedderburn theorem, we see that there is an isomorphism

$$\left(\bigoplus_{\rho \in \widehat{G}} \rho\right) : \mathbb{C}G \xrightarrow{\cong} \bigoplus_{\rho \in \widehat{G}} \mathrm{End}_{\mathbb{C}}(L_\rho).$$

Corollary. *For any $\rho \in \widehat{G}$, we have that $[\mathbb{C}G : \rho] = \dim(L_\rho)$, and hence*

$$\sum_{\rho \in \widehat{G}} \dim(L_\rho)^2 = \#G = \dim_{\mathbb{C}}(\mathbb{C}G).$$

Proposition. *We have that $\#\widehat{G} = \#$ of conjugacy classes of G.*

Proof. Let $Z = Z(\mathbb{C}G)$ be the center of $\mathbb{C}G$. Then

$$\# \text{ of conjugacy classes of } G = \dim(\text{class functions on } G) = \dim(Z)$$

Now, noting the isomorphism

$$\left(\bigoplus_{\rho\in\widehat{G}} \rho\right) : \mathbb{C}G \xrightarrow{\cong} \bigoplus_{\rho\in\widehat{G}} \mathrm{End}_{\mathbb{C}}(L_\rho)$$

we can see that an element of $\mathbb{C}G$ commutes with all other elements if and only if the corresponding tuple of endomorphisms on the right all commute with the action of G. Therefore

$$\dim(Z) = \dim\left(\bigoplus_{\rho\in\widehat{G}} \mathrm{End}_G(L_\rho)\right) = \dim\left(\bigoplus_{\rho\in\widehat{G}} \mathbb{C}\right) = \#\widehat{G}. \qquad \square$$

Theorem. *It is the case that $\dim(L_\rho) \mid \#G$ for any $\rho \in \widehat{G}$.*

(We will prove this later.)

Definition. For any representation $\rho : G \to \mathrm{GL}(V)$, we define a function $\chi_\rho \in \mathbb{C}\{G\}$ by $\chi_\rho(x) = \mathrm{tr}(\rho(x))$.

Let X be a locally compact topological space, and $\int_X$ an integral on X. We define an inner product $(-,-) : C_c(X) \times C_c(X) \to \mathbb{C}$ by

$$(\phi, \psi) \mapsto \int_X \phi(x)\overline{\psi(x)}.$$

If X is a finite set with $\int 1_x = 1$ for all $x \in G$, then

$$(\phi, \psi) = \sum_{x\in X} \phi(x)\overline{\psi(x)}$$

is an inner product on $\mathbb{C}\{X\}$.

Theorem (Orthogonality Relations for Characters)**.** *Let ρ, ρ' be finite-dimensional irreps of a compact group G. Then*

$$\langle \rho, \rho' \rangle = \begin{cases} \mathrm{vol}(G) & \text{if } \rho \cong \rho', \\ 0 & \text{if } \rho \not\cong \rho'. \end{cases}$$

Now let's specialize to the case that G is a finite abelian group.

Corollary.

1. *A representation ρ is irreducible if and only if $\dim(L_\rho) = 1$, i.e. $\rho : G \to \mathrm{GL}_1(\mathbb{C}) = \mathbb{C}^\times$.*
2. *$\rho(x)$ is a root of 1 for any $\rho \in \widehat{G}$ and $x \in G$, so $\rho : G \to$ roots of unity $\subset \mathbb{S}^1 \subset \mathbb{C}^\times$.*
3. *We have a* canonical *algebra isomorphism $(\mathbb{C}G, *) \cong (\mathbb{C}\{\widehat{G}\}, \cdot)$.*

Proof. For part 1, note that G is abelian, so that $\mathbb{C}G$ is commutative, so that any simple $\mathbb{C}G$-module is 1-dimensional.

For part 2, note that any $x \in G$ has finite order; say x has order n. Then

$$\rho(x)^n = \rho(x^n) = \rho(1) = 1.$$

For part 3, note that

$$\mathbb{C}G \cong \bigoplus_{\rho \in \widehat{G}} \mathrm{End}_G(L_\rho) \cong \bigoplus_{\rho \in \widehat{G}} \mathbb{C} \cong \mathbb{C}\{G\}$$

where we have used that $\#G = \#\widehat{G}$ for G finite abelian. ☐

For G abelian, we have a natural abelian group structure on $\widehat{G}$, by defining the product of $\chi, \rho : G \to \mathbb{C}^\times$ to be $(\chi\rho)(x) = \chi(x) \cdot \rho(x)$.

Observe that $\#\widehat{G} = \#G$ by part 3 from earlier. For example, if $G = \mathbb{Z}/(n)$ and $g = 1 \bmod n$, then for any choice of nth root of unity ζ, we have that $\chi_\zeta : g^i \mapsto \zeta^i$ provides a bijection between $\widehat{\mathbb{Z}/(n)}$ and the group of nth roots of unity.

Define $\delta_{\widehat{G}} : \widehat{G} \to \mathbb{C}$ by

$$\delta_{\widehat{G}}(\chi) = \begin{cases} 1 & \text{if } \chi = 1, \\ 0 & \text{if } \chi \neq 1. \end{cases}$$

By orthogonality, we see that for any $\chi \in \widehat{G}$,

$$\sum_{x \in G} \chi(x) = \#G \cdot \delta_{\widehat{G}}(\chi).$$

Therefore

$$\sum_{x \in X} \chi(x) = \begin{cases} \#G & \text{if } \chi = 1, \\ 0 & \text{if } \chi \neq 1. \end{cases}$$

(this is orthogonality for characters). We are already done, but an easy check can be made directly:

Proof. Let $\chi \neq 1$, so that there is some $x_0 \in G$ with $\chi(x_0) \neq 1$. We have

$$\left(\sum_{x \in G} \chi(x) \right) = \sum_{x \in G} \chi(x_0 x) = \chi(x_0) \sum_{x \in G} \chi(x)$$

But because $\chi(x_0) \neq 1$, this is impossible unless $\sum_{x \in G} \chi(x) = 0$. ☐

Note that for each $x \in G$, we get an element of $\widehat{\widehat{G}}$ by $\chi \mapsto \chi(x)$. This defines a canonical map $G \mapsto \widehat{\widehat{G}}$, where $x \mapsto \mathrm{ev}_x$.

The corresponding maps of group algebras is $\mathbb{C}G \to \mathbb{C}\widehat{\widehat{G}}$, where

$$\chi(f) = \sum_{x \in G} \chi(x) f(x)$$

and

$$f \mapsto [\chi \mapsto \chi(f)].$$

Definition. The Fourier transform $\mathcal{F}_G : \mathbb{C}G \to \mathbb{C}\widehat{G}$ is defined to be the map

$$f \mapsto [\widetilde{f} : \chi \mapsto \tfrac{1}{\sqrt{\#G}}\, \chi(f)],$$

so that

$$\widetilde{f}(\chi) = \frac{1}{\sqrt{\#G}} \sum_{x \in G} f(x)\chi(x).$$

Note that $\mathrm{ev} : G \to \widehat{\widehat{G}}$ is injective. This is because, for any $x \in \ker(\mathrm{ev})$, we have that $\mathrm{ev}(x) = 1$, and hence $\chi(x) = 1$ for all χ. But this violates Wedderburn's theorem unless x is the identity.

Theorem (Plancherel)**.** *The Fourier transform is an isometry $\mathbb{C}\{G\} \to \mathbb{C}\{\widehat{G}\}$, i.e. $(f, g) = (\widetilde{f}, \widetilde{g})$ for all $f, g \in \mathbb{C}\{G\}$.*

Lecture 10 (2012-10-22)

Last time, we stated the Plancherel theorem. How is this related to what you know from analysis?

The whole theory works for an arbitrary locally compact abelian group G, with small modification: when G is finite, we let $\widehat{G}$ denote the collection of maps $\chi : G \to \mathbb{C}^\times$, and the image was always contained in the circle, but when G is arbitrary, we need to specify that $\widehat{G}$ consists of the unitary irreps. Thus, for G abelian,

$$\widehat{G} = \{\chi : G \to \mathbb{S}^1 = \mathrm{U}(1)\}.$$

For example, let $G = \mathbb{S}^1$. The maps $\mathbb{S}^1 \to \mathbb{S}^1$ are (as you saw on the homework) precisely of the form $e^{2\pi i\theta} \mapsto e^{2\pi i n\theta}$ for some $n \in \mathbb{Z}$. Thus, $\widehat{G} \cong \mathbb{Z}$.

Let $f \in C(\mathbb{S}^1)$ (note that there's no need to worry about compact support). Then we define

$$\widetilde{f}(n) = \int_g f(e^{2\pi i\theta})e^{2\pi in\theta}\,d\theta,$$

and we create a map $C(\mathbb{S}^1) \to \mathbb{C}\{\mathbb{Z}\}$ by sending f to $\widetilde{f} = \{\widetilde{f}(n)\}_{n\in\mathbb{Z}}$, which we call the Fourier coefficients of f.

Plancherel says that

$$\int_{\mathbb{S}^1} f_1(e^{2\pi i\theta})\overline{f_2(e^{2\pi i\theta})}\,d\theta = \sum_{n\in\mathbb{Z}} \widetilde{f}_1(n)\overline{\widetilde{f}_2(n)}.$$

Now take $G = (\mathbb{R}, +)$. The maps $\chi : \mathbb{R} \to \mathbb{S}^1$ are precisely the maps of the form $\chi_y : x \mapsto e^{2\pi iyx}$, where $y \in \mathbb{R}$. Thus, $\widehat{G} = (\mathbb{R}, +)$. For $f \in C_c(\mathbb{R})$,

$$\widetilde{f}(y) = \int_G f(x)e^{2\pi iyx}\,dx.$$

Remark. Note that you can think of finite as being an intersection of the properties of being compact and being discrete.

$$\text{compact} \xleftrightarrow{\text{Fourier}} \text{discrete}$$

Also, note that for finite groups, we proved $G \cong \widehat{\widehat{G}}$ (more or less) directly; however, it is cleaner (and generalizes more readily) to go through group algebras, i.e. to prove that $\mathbb{C}G \cong \mathbb{C}\{\widehat{G}\}$.

Theorem (Plancherel)**.** *For all $f, g \in \mathbb{C}\{G\}$, we have $(\widetilde{f}, \widetilde{g}) = (f, g)$.*

Proof. We compute that

$$\begin{aligned}
(\widetilde{f}, \widetilde{g}) &= \sum_\chi \widetilde{f}(\chi)\overline{\widetilde{g}(\chi)} \\
&= \sum_\chi \left(\frac{1}{\sqrt{\#G}}\sum_{x\in G} f(x)\chi(x)\right)\left(\frac{1}{\sqrt{\#G}}\sum_{y\in G}\overline{g(y)\chi(y)}\right) \\
&= \frac{1}{\#G}\sum_{\substack{x,y\in G,\\ \chi\in\widehat{G}}} f(x)\overline{g}(y)\chi(x)\overline{\chi(y)}
\end{aligned}$$

$$= \frac{1}{\#G} \sum_{x,y \in G} f(x)\overline{g}(y) \left(\sum_{\chi \in \widehat{G}} \chi(xy^{-1}) \right)$$

$$= \frac{1}{\#G} \sum_{x,y \in G} f(x)\overline{g(y)} \begin{pmatrix} \#G \text{ if } x = y \\ 0 \text{ if } x \neq y \end{pmatrix}$$

$$= \sum_{x \in G} f(x)\overline{g(x)}$$

$$= (f, g). \qquad \square$$

Now, we have $\mathcal{F}_G : \mathbb{C}\{G\} \to \mathbb{C}\{\widehat{G}\}$; how do we find $\mathcal{F}_G^{-1}$? For any group G, define an anti-involution $\tau : C_c(G) \to C_c(G)$ by $f^\tau(x) = f(x^{-1})$.

Theorem (Inversion theorem)**.** *For any* $f \in \mathbb{C}\{G\}$*, we have* $\widetilde{\widetilde{f}} = f^\tau$*.*

Proof. We have that

$$\begin{aligned}
\mathcal{F}_{\widehat{G}}(\widetilde{f})(x) &= \frac{1}{\sqrt{\#G}} \sum_{\chi \in \widehat{G}} \widetilde{f}(\chi)\chi(x) \\
&= \frac{1}{\sqrt{\#G}} \sum_{\chi \in \widehat{G}} \left(\frac{1}{\sqrt{\#G}} \sum_{y \in G} f(y)\chi(y) \right) \chi(x) \\
&= \frac{1}{\#G} \sum_{\substack{\chi \in \widehat{G}, \\ y \in G}} f(y)\chi(yx) \\
&= \frac{1}{\#G} \sum_{y \in G} f(y) \left(\sum_{\chi \in \widehat{G}} \chi(yx) \right) \\
&= \frac{1}{\#G} \sum_{y \in G} f(y) \begin{pmatrix} \#G \text{ if } y = x^{-1} \\ 0 \text{ if } y \neq x^{-1} \end{pmatrix} \\
&= f(x^{-1}) = f^\tau(x).
\end{aligned} \qquad \square$$

Now let G be a finite group, no longer necessarily abelian. Then the orthogonality relation for G says that

$$f(e) = \sum_{\rho \in \widehat{G}} \frac{\dim(L_\rho)}{\#G} \mathrm{tr}_{L_\rho}(\rho(f)).$$

Proof. Because this is a linear equation in f, it suffices to check it for $f = \mathbf{1}_g$ for each $g \in G$. Note that in the regular representation of G on $\mathbb{C}G$, we have that

$$\mathrm{tr}(g \circlearrowleft \mathbb{C}G) = \begin{cases} \#G & \text{if } g = e, \\ 0 & \text{if } g \neq e. \end{cases}$$

Hence

$$\#G \cdot f(e) = \mathrm{tr}(g \circlearrowright \mathbb{C}G) = \sum_{\rho \in \widehat{G}} \dim(L_\rho)\mathrm{tr}(\rho(g)) = \sum_{\rho \in \widehat{G}} \dim(L_\rho) \cdot \mathrm{tr}(\rho(\mathbf{1}_g)). \qquad \square$$

Lemma. *For any unitary representation ρ and $f \in \mathbb{C}\{G\}$, we have*

$$\rho(\overline{f^\tau}) = \rho(f)^*.$$

Proof. Note that

$$\rho(\overline{f^\tau}) = \sum_{x \in G} \overline{f(x^{-1})}\rho(x) = \sum_{y \in G} \overline{f(y)}\rho(y)^{-1},$$

and because ρ is a unitary representation, this equals

$$\sum_{y \in G} \overline{f(y)}\rho(y)^* = \sum_{y \in G} (f(y)\rho(y))^* = \rho(f)^*. \qquad \square$$

Given $f \in \mathbb{C}\{G\}$ for G a arbitrary (locally compact?) non-abelian group, $\widehat{G}$ is no longer a group, but for $\rho \in \widehat{G}$ we can still define

$$\widetilde{f}_\rho = \sqrt{\frac{\dim(L_\rho)}{\#G}}, \quad \rho(f) \in \mathrm{End}_{\mathbb{C}}(L_\rho).$$

Then the general Plancherel theorem says that, for $\phi, \psi \in \mathbb{C}\{G\}$,

$$(\phi, \psi) = \sum_{\rho \in \widehat{G}} \frac{\dim(\rho)}{\#G} \mathrm{tr}(\rho(\phi)\rho(\psi)^*).$$

Slogan: Any commutative algebra is an algebra of functions, any non-commutative algebra is an algebra of operators.

Lecture 11 (2012-10-24)

Just as a reminder, the midterm is today, 4:30 to 6:15, in Eckhart 312.

Theorem (Plancherel, general case). *For $\phi, \psi \in \mathbb{C}\{G\}$,*

$$\sum_{g \in G} \phi(g)\overline{\psi(g)} = \sum_{\rho \in \widehat{G}} \frac{\dim(\rho)}{\#G} \operatorname{tr}(\rho(\phi)\rho(\psi)^*).$$

Proof. Let $f = \phi * \overline{\psi^\tau}$. Apply the orthogonality relations to f:

$$(\phi * \overline{\psi^\tau})(e) = \sum_{\rho \in \widehat{G}} \frac{\dim(\rho)}{\#G} \operatorname{tr}(\rho(\phi * \overline{\psi^\tau})).$$

By definition of convolution, the LHS of the above orthogonality relation is equal to

$$\sum_{y \in G} \phi(ey^{-1})\overline{\psi^\tau}(y) = \sum_{y \in G} \phi(y^{-1})\overline{\psi(y^{-1})} \quad \text{(LHS of theorem)}.$$

We know that $\rho(\phi * \overline{\psi^\tau}) = \rho(\phi)\rho(\overline{\psi^\tau})$, and by the last lemma from Lecture 11, $\rho(\overline{\psi^\tau}) = \rho(\psi)^*$. Hence the RHS of orthogonality coincides with the RHS of the theorem, and we are done. $\square$

Recall from Wedderburn theory that the map

$$\Psi : \mathbb{C}G \to \bigoplus_{\rho \in \widehat{G}} \operatorname{End}_{\mathbb{C}}(L_\rho) : f \mapsto \underset{\rho \in \widehat{G}}{\oplus} \rho(f)$$

is an isomorphism. The inversion theorem gives a formula for the inverse:

Theorem (Inversion). *For $a = \underset{\rho \in \widehat{G}}{\oplus} a_\rho \in \bigoplus_{\rho \in \widehat{G}} \operatorname{End}_{\mathbb{C}}(L_\rho)$, the inverse map Ψ^{-1} is given by*

$$\Psi^{-1}(a)(g) = \sum_{\rho \in \widehat{G}} \frac{\dim(\rho)}{\#G} \operatorname{tr}(a_\rho \cdot \rho(g)^{-1}).$$

Proof. WLOG we can assume $a = \Psi(f) = \underset{\rho \in \widehat{G}}{\oplus} \rho(f)$ for some $f \in \mathbb{C}\{G\}$. We need to check

$$\sum_{\rho \in \widehat{G}} \frac{\dim(\rho)}{\#G} \operatorname{tr}(\rho(f)\rho(g)^{-1}) \overset{?}{=} f(g).$$

But the left side is just equal to

$$\sum_{\rho \in \widehat{G}} \frac{\dim(\rho)}{\#G} \operatorname{tr}(\rho(f) \cdot \rho(\mathbf{1}_g)^*) \overset{\text{Plancherel}}{=} \sum_{x \in G} f(x)\overline{\mathbf{1}_g(x)} = f(g).$$ $\square$

Recall that the character of a representation ρ is defined to be $\chi_\rho(f) = \operatorname{tr}(\rho(g))$.

Corollary. *The element $e_\rho = \frac{\dim(\rho)}{\#G} \sum_{g \in G} \overline{\chi_\rho(g)} \cdot g$ is a central idempotent in $\mathbb{C}G$. Moreover,*

$$\rho'(e_\rho) = \begin{cases} \mathrm{id}_{L_\rho} & \text{if } \rho' \cong \rho, \\ 0 & \text{if } \rho' \ncong \rho. \end{cases}$$

Proof. Take $a = \oplus_{\rho'} a_{\rho'}$, where $a_{\rho'} = \begin{cases} \mathrm{id}_{L_\rho} & \text{if } \rho' \cong \rho, \\ 0 & \text{if } \rho' \ncong \rho. \end{cases}$. Then

$$\Psi^{-1}(a)(g) \overset{\text{inversion}}{=} \frac{\dim(\rho)}{\#G} \mathrm{tr}(\rho(g^{-1}))$$

which implies that $\Psi^{-1}(a) = \frac{\dim(\rho)}{\#G} \sum_{g \in G} \mathrm{tr}(\rho(g)^*)$. But

$$\mathrm{tr}(\rho(g)^*) = \mathrm{tr}(\overline{\rho(g)}) = \overline{\mathrm{tr}(\rho(g))} = \overline{\chi_\rho(g)}$$

so we are done. □

Let $\mathbb{C}\{G\}^G$ be the collection of class functions on G.

Theorem (Classical orthogonality)**.** *The set $\{\chi_\rho \mid \rho \in \widehat{G}\}$ is an orthonormal basis of $\mathbb{C}\{G\}^G$, i.e.*

$$(\chi_\rho, \chi_{\rho'}) = \begin{cases} \#G & \text{if } \rho \cong \rho', \\ 0 & \text{if } \rho \ncong \rho'. \end{cases}$$

Proof.

$$\begin{aligned}
(\overline{\chi_\rho}, \overline{\chi_\rho}) = \sum_{g \in G} \overline{\chi_\rho(g)} \chi_{\rho'}(g) &= \left(\frac{\#G}{\dim(\rho)} e_\rho, \frac{\#G}{\dim(\rho')} e_{\rho'} \right) \\
&\overset{\text{Plancherel}}{=} \sum_{\sigma \in \widehat{G}} \frac{\dim(\sigma)}{\#G} \mathrm{tr} \left(\sigma \left(\frac{\#G}{\dim(\rho)} e_\rho \right) \cdot \sigma \left(\frac{\#G}{\dim(\rho')} e_{\rho'} \right)^* \right) \\
&= \sum_{\sigma \in \widehat{G}} \frac{\dim(\sigma)}{\#G} \frac{(\#G)^2}{\dim(\rho) \dim(\rho')} \mathrm{tr} \left(\delta_{\sigma\rho} \mathrm{id}_{L_\rho} \cdot \ \delta_{\sigma\rho'} \mathrm{id}_{L_{\rho'}} \right) \\
&= \begin{cases} 0 & \text{if } \rho \ncong \rho', \\ \frac{\dim(\rho)}{\#G} \cdot \frac{(\#G)^2}{\dim(\rho)^2} \dim(\rho) = \#G & \text{if } \rho \cong \rho'. \end{cases}
\end{aligned}$$

□

Tensor products

Let B be a ring. We can consider right B-modules, which are equivalent to left B^{op}-modules. If B is commutative, then left is the same as right. For example, we can think of the collection of column vectors

$$\begin{pmatrix} B \\ B \\ \vdots \\ B \end{pmatrix}$$

as a left $\mathrm{M}_n(B)$-module, and the collection of row vectors

$$\begin{pmatrix} B & B & \cdots & B \end{pmatrix}$$

as a right $\mathrm{M}_n(B)$-module.

Let A and B be rings. An (A, B)-bimodule is an abelian group M which is a left A-module and a right B-module such that the A-action and B-action commute.

Examples.

- A is an (A, A)-bimodule in the obvious way.
- The space of $m \times n$ matrices over A is an $(\mathrm{M}_m(A), \mathrm{M}_n(A))$-bimodule.

Definition. Let M be a right A-module, and N be a left A-module. Then we define

$$M \otimes_A N = \frac{\{\text{free abelian group on symbols } m \otimes n\}}{\left\langle \begin{matrix} (m_1 + m_2) \otimes n - m_1 \otimes n - m_2 \otimes n \\ m \otimes (n_1 + n_2) - m \otimes n_1 - m \otimes n_2 \\ ma \otimes n - m \otimes an \end{matrix} \right\rangle}$$

Comments.

- If A is a k-algebra, then $M \otimes_A N$ is a quotient of $M \otimes_k N$.
- $A \otimes_A N = N$ and $M \otimes_A A = M$
- If we have rings A, B, and if M is an (A, B)-bimodule, then for any left B-module N, there is still a left A-action on $M \otimes_B N$, making it into a left A-module.
- The tensor product $\otimes_A$ has a universal property,

$$\begin{tikzcd} M \times N \arrow[r, "\text{canonical}"] \arrow[dr, "f"'] & M \otimes_A N \arrow[d, dashed, "\exists! \widetilde{f}"] \\ & M \end{tikzcd}$$

where $\widetilde{f}$ is a map of abelian groups and f is a "middle A-linear" map.

Lecture 12 (2012-10-26)

We'll continue talking about tensor products today.

Recall that any abelian group can be considered as a $\mathbb{Z}$-module, and therefore we can tensor them over $\mathbb{Z}$. In particular, for any rings A and B, we can form the tensor product $A \otimes_{\mathbb{Z}} B$, which is a ring in the obvious way:

$$(a \otimes b)(a' \otimes b') = aa' \otimes bb'.$$

We can do the same for k-algebras; given k-algebras A, B, then $A \otimes_k B$ is a k-algebra, with the same operation as above.

A good way of thinking about (A, B)-bimodules is as left modules over $A \otimes_{\mathbb{Z}} (B^{\mathrm{op}})$.

Given a left A-module M and a left B-module N, we can form their "external tensor product" $M \otimes_{\mathbb{Z}} N$, sometimes denoted $M \boxtimes N$, which is a left $A \otimes_{\mathbb{Z}} B$-module.

Given two groups G and H, and a G-representation ρ and a H-representation ρ', then we can form an external tensor product $\rho \boxtimes \rho'$ which is a $(G \times H)$-representation. To describe it explicitly, given $\rho : G \to \mathrm{GL}(V)$ and $\rho' : H \to \mathrm{GL}(V')$, then $\rho \boxtimes \rho' : G \times H \to \mathrm{GL}(V \otimes_k V')$ maps $g \times h$ to $\rho(g) \otimes \rho'(h)$.

Note that the G-representation ρ is equivalent to the left kG-module V, and the H-represenation ρ' is equivalent to the left kH-module V'. We have a canonical isomorphism

$$k(G \times H) \cong kG \otimes_k kH,$$

and $\rho \boxtimes \rho'$ is the $(G \times H)$-represenation that corresponds to the $(kG \otimes_k kH)$-module $V \boxtimes V'$.

Given two representations ρ and ρ' of G, then we define $\rho \otimes \rho' : G \to \mathrm{GL}(V \otimes V')$ by mapping g to $\rho(g) \otimes \rho'(g)$. This is different than $\boxtimes$; for example, if ρ' is the regular representation $G \circlearrowright kG$, then $V \otimes_k kG$ won't be the same $V \otimes_{kG} kG = V$ (recall $M \otimes_A A \cong M$).

In other words, given two modules over an algebra, we can tensor them over the base field, but there won't be any canonical action of the algebra on it.

The special property kG has is that it is a Hopf algebra, i.e. there is an algebra morphism $\delta : kG \to kG \otimes_k kG$ mapping g to $g \otimes g$.

Proposition.

1. *If ρ is an irrep of a finite group G, and ρ' is an irrep of a finite group H, then $\rho \boxtimes \rho'$ is an irrep of $G \times H$.*
2. *Any irrep of $G \times H$ has the form $\rho \boxtimes \rho'$ for irreps $\rho \in \widehat{G}, \rho' \in \widehat{H}$.*

Proof. Recall that $\chi_\rho(g) = \mathrm{tr}(\rho(g))$ and $\chi_{\rho'}(h) = \mathrm{tr}(\rho'(h))$. Then

$$\chi_{\rho \boxtimes \rho'}(g, h) = \mathrm{tr}(\rho(g) \otimes \rho'(h)) = \mathrm{tr}(\rho(g))\mathrm{tr}(\rho'(h)) = \chi_\rho(g)\chi_{\rho'}(h).$$

Thus

$$(\chi_{\rho \boxtimes \rho'}, \chi_{\rho \boxtimes \rho'}) = (\chi_\rho, \chi_\rho) \cdot (\chi_{\rho'}, \chi_{\rho'}).$$

By the orthogonality relations, this is equal to $\#G \cdot \#H = \#(G \times H)$, and therefore $\rho \boxtimes \rho'$ is an irrep of $G \times H$.

To see part 2, we use a counting argument. The number of representations of the form $\rho \boxtimes \rho'$ with $\rho \in \widehat{G}, \rho' \in \widehat{H}$ is just $\#(\widehat{G} \times \widehat{H})$.

A priori, $\#(\widehat{G \times H}) = \#$ of conjugacy classes in $G \times H$, but a conjugacy class in $G \times H$ is just a product of conjugacy classes from G and H, so

$$\begin{aligned}\#(\widehat{G \times H}) &= \# \text{ of conjugacy classes in } G \times H \\ &= (\# \text{ of conjugacy classes in } G) \cdot (\# \text{ of conjugacy classes in } H) \\ &= \#\widehat{G} \cdot \#\widehat{H}.\end{aligned}$$

□

If A is a ring, and M is an A-bimodule, we can form

$$T_A(M) = A \otimes M \oplus (M \otimes_A M) \oplus (M \otimes_A M \otimes_A M) \oplus \cdots$$

which is an algebra where the operation on simple tensors in a single degree is just concatenation,

$$(m_1 \otimes \cdots \otimes m_k) \cdot (n_1 \otimes \cdots \otimes n_\ell) = m_1 \otimes \cdots \otimes m_k \otimes n_1 \otimes \cdots \otimes n_\ell.$$

Fix a finite set X, and let $A = k\{X\} = \bigoplus_{x \in X} k \cdot \mathbf{1}_x$. An A-module M decomposes as $M = \bigoplus_{x \in X} M_x$ where M_x is a k-vector space. Take another A-module N. How can we think about $M \otimes_A N$?

We know that $M \otimes_A N$ will be a quotient of $M \otimes_k N = \bigoplus_{x,y \in X} M_x \otimes_k N_y$. Specifically,

$$M \otimes_A N = \frac{\bigoplus_{x,y} M_x \otimes_k N_y}{\langle (m \cdot \mathbf{1}_z) \otimes n = m \otimes (\mathbf{1}_z n) \text{ for all } z \in X \rangle} \cong \bigoplus_{x \in X} M_x \otimes_k N_x.$$

More generally, if X and Y are finite sets, then

$$k\{X\} \otimes_k k\{Y\} = k\{X \times Y\},$$

via the map $\mathbf{1}_x \otimes \mathbf{1}_y \mapsto \mathbf{1}_{x,y}$.

Now let M, N be $k\{X\}$-bimodules. Then $M = (M_{x,y})_{(x,y) \in X \times X}$ because a $k\{X\}$-bimodule is just a left module over $k\{X\} \otimes k\{X\}^{\mathrm{op}} = k\{X\} \otimes k\{X\} = k\{X \times X\}$.

For any $m_{x',y'} \in M_{(x',y')}$, we have

$$\mathbf{1}_x \cdot m_{x',y'} \cdot \mathbf{1}_y = \begin{cases} m_{x,y} & \text{if } x = x', y = y', \\ 0 & \text{otherwise.} \end{cases}$$

Thus

$$M \otimes_A N = \bigoplus_{x_1, x_2 \in X} \left(\bigoplus_{y \in X} (M_{x_1,y} \otimes_k N_{y,x_2}) \right).$$

Let M be a bimodule over $A = k\{X\}$. Then

$$T_A M = A \oplus \left(\bigoplus_{x_1,x_2} M_{x_1,x_2} \right) \oplus \left(\bigoplus_{x_1,x_2,x_3} M_{x_1,x_2} \otimes M_{x_2,x_3} \right) \oplus \left(\bigoplus_{x_1,x_2,x_3,x_4} M_{x_1,x_2} \otimes M_{x_2,x_3} \otimes M_{x_3,x_4} \right) \cdots$$

We will now define a construction called the smash product. Let A be a ring, and let G be a group acting on A by automorphisms. For example, we might have $G \subset A^\times$, and $G \circlearrowright A$ via $g \cdot a = gag^{-1}$. Let's use the notation ${}^g a$ for g acting on a.

A G-equivariant A-module M is an A-module $A \otimes M \to M$ and a G-representation $G \times M \to M$ such that $g(am) = {}^g a g(m)$. In the case of $G \subset A^\times$, then this just says that

$$g(am) = (gag^{-1})(gm) = (ga)m.$$

The smash product $A\#G$ will be an algebra such that modules over $A\#G$ are equivalent to G-equivariant A-modules.

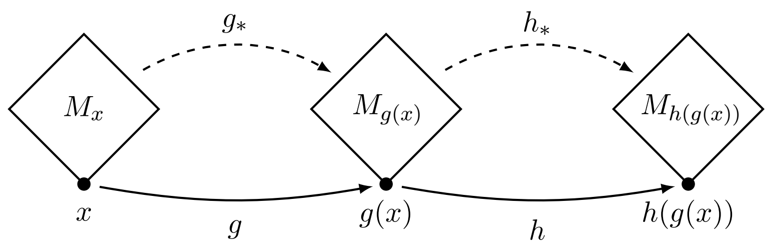
Lecture 13 (2012-10-29)

Last time, we finished with the definition of a G-equivariant A-module.

Examples.

- Let $A = k\{X\}$, and let $G \circlearrowright X$. Then there is an obvious induced action $G \circlearrowright A$: because g sends x to gx, it should send $\mathbf{1}_x$ to $\mathbf{1}_{gx}$, and hence it sends any $f = \sum_{x\in X} \lambda_x \mathbf{1}_x \in A$ to
$$gf = \sum_{x\in X} \lambda_x \mathbf{1}_{gx}.$$
Note that $(gf)(x) = \lambda_{g^{-1}(x)}$. Given an A-module M and a (possibly unrelated) k-linear G-action $G \circlearrowright M$, what does it mean for $M = \bigoplus_{x\in X} M_x$ to be a G-equivariant A-module?

  M is G-equivariant when, for any $g \in G$, the action of g on M consists of maps $g_* : M_x \to M_{g(x)}$ (in general, it could be any k-linear map, even one that doesn't respect the decomposition of M over the elements of X) with the property that, for any $f = \sum_{x\in X} \lambda_x \mathbf{1}_x = (\lambda_x)_{x\in X} \in A$ and $m = (m_x)_{x\in X} \in M$,
$$g_*((\lambda_x)(m_x)) = (\lambda_{g^{-1}(x)})g_*((m_x)).$$
Visualizing M as the vector space M_x attached to the corresponding point x,



- For any k-algebra A and any k-vector space V, we can make a free A-module $M = A \otimes_k V$. Then, for any action $G \circlearrowright A$ and any G-representation $G \to \mathrm{GL}(V)$, we can let G act on $M = A \otimes_k V$ by $g(a \otimes v) = {}^g a \otimes g(v)$. Let's do an example:

  Let $G \circlearrowright E$ where E is a set. Then $G \circlearrowright A = k[E]$, the polynomial ring in the elements of E. Let $M = k[E] \otimes V$. Then we get what in geometry would be called a vector bundle, and moreover one carrying a G-action:
$$\begin{tikzcd} E \times V \arrow[d] \\ E \end{tikzcd} \qquad\qquad \begin{tikzcd} (e, V) \arrow[r, "g_*"] \arrow[d] & (g(e), V) \arrow[d] \\ e \arrow[r, "g"'] & g(e) \end{tikzcd}$$
Because G acts on $k[E]$ by automorphisms, knowing how G acts on E tells us how it will act on any element of $k[E]$.

Question. Can we define an algebra $A\#G$ such that the data of a G-equivariant A-module is equivalent to the data of an $A\#G$-module?

Definition. Given a k-algebra A, the algebra $A\#G$ is defined to be a free A-module with basis G, so a general element looks like $\sum_{g\in G} a_g g$. We define

$$(ag)(bh) = (a \cdot {}^g b) \cdot (gh)$$

where $a, b \in A$, and $g, h \in G$. This construction answers the question in the affirmative.

Note the similarity to the definition of the semi-direct product.

Note that we have an inclusion $A \hookrightarrow A\#G$ defined by $a \mapsto a \cdot 1_G$.

When G is finite (so that we can speak of kG), we also have an inclusion $kG \hookrightarrow A\#G$ mapping $\lambda \cdot g \mapsto \lambda \cdot g$. In particular, if $A = k$, then $k\#G = kG$. Note that $A\#G \cong A \otimes_k kG$ as k-vector spaces, but **not** as k-algebras, and certainly not as A-algebras.

Now let A be a k-algebra with an action of a finite group $G \circlearrowright A$. Then $kG \hookrightarrow A\#G$, and therefore $A\#G$ is a kG-bimodule, i.e. $A\#G$ has a $G \times G$ action,

$$(g_1 \times g_2) : a \cdot h \mapsto g_1 \cdot (a \cdot h) \cdot g_2^{-1}.$$

Let

$$e = \frac{1}{\#G} \sum_{g\in G} g$$

be the standard averaging idempotent. Recall that e is central and $e^2 = e$ in $kG \subset A\#G$.

For any $ag \in A\#G$, we have that

$$(ag)e = \frac{1}{\#G} \sum_{h\in G} agh = \frac{1}{\#G} \sum_{h\in G} ah = ae.$$

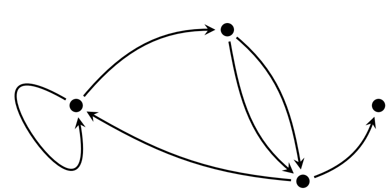
Thus, for any $\sum_{g\in G} a_g g \in A\#G$, we have

$$\left(\sum_{g\in G} a_g g\right) e = \left(\sum_{g\in G} a_g\right) e,$$

and hence $(A\#G)e \cong Ae$. Then, $e(Ae) = eAe$ consists of the elements of Ae fixed by g (recall that in general if G acts on V, then $eV = V^G$), so there is a canonical isomorphism $e(A\#G)e \cong eAe \cong A^G$.

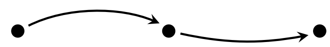
Quivers

Definition. A quiver is a finite oriented graph. We can write it as an ordered pair (Q, I) where I is the set of vertices and Q is the set of arrows.



We often denote a quiver just by the set of arrows Q.

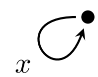
A path in Q is a finite sequence of arrows which meet head to tail.



Definition. The path algebra kQ of Q over a field k is a k-vector space with basis formed by paths in Q, with product given by concatenation of paths which can be concatenated (paths that can't be concatenated multiply to 0). The order in which paths are concatenated is apparently a delicate issue. There are also trivial paths $\mathbf{1}_i$ at each vertex $i \in I$; each trivial path is an idempotent, and acts as an identity when concatenated with paths that start or end at i.

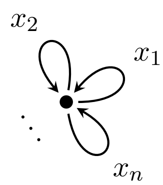
Examples.

- Consider the quiver Q with one vertex and one edge (the trivial path is implied),

  Then $kQ = k[x]$. Note that, without the trivial path at the vertex, we'd only get polynomials in x with no constant term.

- Consider the quiver Q with n loops around one vertex (the trivial path is implied),

  Then $kQ = k\langle x_1, \dots, x_n\rangle$, the free associative algebra on n generators.

- Consider the quiver Q with n vertices in a row with edges between them,

  $$\begin{tikzcd} \underset{\mathbf{1}_1}{\bullet} \arrow[r, "x_1"] & \underset{\mathbf{1}_2}{\bullet} \arrow[r, "x_2"] & \underset{\mathbf{1}_3}{\bullet} \arrow[r] & \cdots \arrow[r] & \underset{\mathbf{1}_{n-1}}{\bullet} \arrow[r, "x_{n-1}"] & \underset{\mathbf{1}_n}{\bullet} \end{tikzcd}$$

  Then we get $kQ =$ the algebra of upper triangular matrices over k. The trivial path $\mathbf{1}_i$ at vertex i corresponds to a matrix with 1 on the ith diagonal entry and 0 elsewhere.

Definition. Given a finite subgroup $G \subset \mathrm{GL}(V)$, we define the McKay quiver Q_G associated to it as follows. The vertex set of Q_G is in bijection with $\widehat{G}$, say with $i \leftrightarrow L_i$. Then we set the number of edges from i to j to be

$$\#\{i \to j\} = \dim(\mathrm{Hom}_G(L_i, V \otimes L_j)) = [V \otimes L_j : L_i].$$

Example. Let $G = \left\{ \left(\begin{smallmatrix} \zeta & 0 \\ 0 & \zeta^{-1}\end{smallmatrix}\right) \middle| \zeta^n = 1 \right\} \subset \mathrm{GL}(\mathbb{C}^2)$. Then $G \cong \mathbb{Z}/n\mathbb{Z}$. Letting z be a primitive nth root of unity, then the irreducible representations of G are the maps $L_i : G \to \mathbb{C}^\times$ defined by $\left(\begin{smallmatrix} z & 0 \\ 0 & z^{-1}\end{smallmatrix}\right) \mapsto z^i$ for $i = 0, 1, \dots, n-1$. Noting that $\mathbb{C}^2 = L_1 \oplus L_{-1}$, we get

$$\begin{tikzcd}
& & i \arrow[dl, shift left] \arrow[dr, shift left] & & \\
& i-1 \arrow[ur, shift left] \arrow[dl, shift left] & & i+1 \arrow[ul, shift left] \arrow[dr, shift left] & \\
\iddots \arrow[ur, shift left] & & & & \ddots \arrow[ul, shift left]
\end{tikzcd}$$

Lecture 14 (2012-10-31)

Let (Q, I) be a quiver. We want to understand its path algebra kQ over the field k. We can define E_{ij} to be a vector space with basis the edges $\{i \to j\}$ from i to j. Now define $E = \bigoplus_{i,j \in I} E_{ij}$. Since this is indexed in two elements of I, it is a $k\{I\}$-bimodule, via

$$\mathbf{1}_k \cdot e_{ij} \cdot \mathbf{1}_\ell = \begin{cases} e_{ij} & \text{if } k = i, j = \ell, \\ 0 & \text{otherwise.} \end{cases}$$

Proposition. *There is an isomorphism*

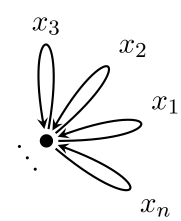
$$kQ \cong T_{k\{I\}}E = k\{I\} \oplus E \oplus \big(E \otimes_{k\{I\}} E\big) \oplus \big(E \otimes_{k\{I\}} E \otimes_{k\{I\}} E\big) \oplus \cdots$$

Proof. There is a well-defined notion of the length of a path; we can just take the number of edges in the path. Now note that

$k\{I\}$	has basis $\{\mathbf{1}_i\}$, all the paths of length 0
E	has basis $\{i \to j\}$, all the paths of length 1
$E \otimes_{k\{I\}} E$	generated by {pairs $(i_1 \to j_1) \otimes (i_2 \to j_2)$ of paths of length 1}, except pairs which do not meet head to tail ($j_1 \neq i_2$) are 0

Multiplication in $T_{k\{I\}}E$ corresponds to concatenation of paths. □

Example. Let Q be the quiver of n loops on one vertex.



As we saw last class, $kQ = k\langle x_1, \ldots, x_n \rangle$, the free associative algebra on n generators. For this quiver, I has one element, so $k\{I\} = k$, and every path can be concatenated. The edge set Q from the sole vertex to itself has n elements. The proposition then corresponds to the decomposition of $k\langle x_1, \ldots, x_n \rangle$ as a direct sum of the subspaces consisting of monomials of a given degree:

$$k\langle x_1, \ldots, x_n \rangle = k \oplus \left(\bigoplus_{x_i \in Q} kx_i \right) \oplus \left(\bigoplus_{x_i, x_j \in Q} k(x_i x_j) \right) \oplus \cdots$$

Now let V be a finite-dimensional vector space over $\mathbb{C}$. Let $G \subset \mathrm{GL}(V)$ be a finite subgroup. Recall that the McKay quiver Q_G has vertex set $I = \widehat{G}$, which we will label so that $\rho \in I$ corresponds to L_ρ. Note that the indicator function $\mathbf{1}_\rho \in \mathbb{C}\{\widehat{G}\}$ is just the trivial path for ρ in the path algebra $\mathbb{C}Q_G$. Let $0 \in I$ correspond to the trivial representation.

We will prove the following theorem:

Theorem 1. *There is an isomorphism* $(T_{\mathbb{C}}V)^G \cong \mathbf{1}_0 \mathbb{C}Q_G \mathbf{1}_0$.

However, we will need to prove another theorem before we can prove Theorem 1.

For each $\rho \in \widehat{G}$, choose a one-dimensional subspace of L_ρ, and let p_ρ be the projection of $\mathbb{C}G$ onto that subspace. Considered as an element of $\mathrm{End}_{\mathbb{C}}(L_\rho)$, the matrix of p_ρ is just

$$\begin{pmatrix} 1 & \cdot & \cdot \\ \cdot & \cdot & \cdot \\ \cdot & \cdot & \cdot \end{pmatrix}$$

Because $\mathbb{C}G$ contains $\dim(L_\rho)$ copies of L_ρ, we have that $L_\rho = \mathbb{C}G \cdot p_\rho$. Note that $p_\rho^2 = p_\rho \in \mathbb{C}G$. These are orthogonal idempotents, so that $p = \sum_{\rho \in \widehat{G}} p_\rho$ satisfies $p^2 = p$.

As a vector space, $T_{\mathbb{C}}V\#G = T_{\mathbb{C}}V \otimes_{\mathbb{C}} \mathbb{C}G$ with a "twisted" multiplication[4] via the action of G on V. Therefore $\mathbb{C}G \hookrightarrow T_{\mathbb{C}}V\#G$, and we can consider the projections p_ρ as living inside this larger algebra.

Theorem 2. *There exists an algebra isomorphism* $\Phi : p(T_{\mathbb{C}}V\#G)p \to \mathbb{C}Q_G$ *satisfying* $\Phi(p_\rho) = \mathbf{1}_\rho$ *(but this condition itself does not tell us the values of* Φ *on all of* $p(T_{\mathbb{C}}V\#G)p$*).*

To see that Theorem 2 implies Theorem 1, note that $p_0 = e = \frac{1}{\#G}\sum_{g \in G} g$ and that $p_0 p = p_0 = p p_0$. Now observe that

$$\begin{aligned} (T_{\mathbb{C}}V)^G &\cong e(T_{\mathbb{C}}V\#G)e \\ &= p_0(T_{\mathbb{C}}V\#G)p_0 \\ &= p_0[p(T_{\mathbb{C}}V\#G)p]p_0 \\ \text{(by Theorem 2)} \quad &\cong \mathbf{1}_0[\mathbb{C}Q_G]\mathbf{1}_0. \end{aligned}$$

Proof of Theorem 2. Let M be a G-representation. From the matrix description of p_ρ in $\mathrm{End}_{\mathbb{C}}(L_\rho) = L_\rho \boxtimes L_\rho^* \subset \mathbb{C}G$, we can deduce that $L_\rho = \mathbb{C}G \cdot p_\rho \subset \mathbb{C}G$ as left $\mathbb{C}G$-modules and $L_\rho^* \simeq p_\rho \mathbb{C}G$ as right $\mathbb{C}G$-modules. Therefore

$$\mathrm{Hom}_G(L_\rho, M) \cong \mathrm{Hom}_{\mathbb{C}G}(\mathbb{C}Gp_\rho, M) = p_\rho M.$$

Now let M be a $\mathbb{C}G$-bimodule, i.e. $(G \times G)$-representation. Then

$$\mathrm{Hom}_{G\times G}(L_\rho \boxtimes L_\sigma^*, M) \cong p_\rho M p_\sigma.$$

Thus applying Wedderburn's theorem,

$$\begin{aligned} p\mathbb{C}Gp &= \bigoplus_{\mu \in \widehat{G}} p(\mathrm{End}(L_\mu))p \\ &= \bigoplus_{\mu,\rho,\sigma \in \widehat{G}} p_\rho(\mathrm{End}(L_\mu))p_\sigma \\ &= \bigoplus_{\mu,\rho,\sigma \in \widehat{G}} p_\rho \left(L_\mu \boxtimes L_\mu^*\right) p_\sigma \\ &= \bigoplus_{\mu \in \widehat{G}} \mathbb{C} \otimes \mathbb{C} = \bigoplus_{\mu \in \widehat{G}} \mathbb{C} = \mathbb{C}\{\widehat{G}\}. \end{aligned}$$

[4] In fact we see later that there is an even cleaner definition $T_{\mathbb{C}}V\#G = T_{\mathbb{C}G}M$.

The isomorphism $p\mathbb{C}Gp \cong \mathbb{C}\{\widehat{G}\}$ is of algebras, where multiplication on $\mathbb{C}\{\widehat{G}\}$ is pointwise.

Now define $M = V \otimes_{\mathbb{C}} \mathbb{C}G$, and make it a $(G \times G)$-module (i.e. $\mathbb{C}G$-bimodule), where

$$g(v \otimes u) = gv \otimes gu, \qquad (v \otimes u)g = v \otimes ug.$$

We decompose $\mathbb{C}G$ in the same way as before to get an isomorphism of $\mathbb{C}G$-bimodules

$$M = V \otimes \left(\bigoplus_{\mu} \mathrm{End}(L_\mu) \right) = \bigoplus_{\mu} (V \otimes L_\mu) \boxtimes L_\mu^*.$$

We want to compute pMp. We have

$$pMp = \bigoplus_{\rho,\sigma \in \widehat{G}} p_\rho M p_\sigma = \bigoplus_{\rho,\sigma} \mathrm{Hom}_{G\times G}(L_\rho \boxtimes L_\sigma^*, M)$$

$$= \bigoplus_{\rho,\sigma,\mu} \mathrm{Hom}_{G\times G}(L_\rho \boxtimes L_\sigma^*, (V \otimes L_\mu) \boxtimes L_\mu^*)$$

A dimension argument shows that

$$\mathrm{Hom}_{G\times G}(L_\rho \boxtimes L_\sigma^*, (V \otimes L_\mu) \boxtimes L_\mu^*) = \mathrm{Hom}_G(L_\rho, V \otimes L_\mu) \otimes_{\mathbb{C}} \mathrm{Hom}_G(L_\sigma^*, L_\mu^*).$$

Now an application of Schur's lemma implies that

$$pMp = \bigoplus_{\rho,\sigma} \mathrm{Hom}_G(L_\rho, V \otimes L_\sigma) = \bigoplus_{\rho,\sigma} E_{\rho,\sigma} =: E$$

where E was introduced at the beginning of the lecture. It is an easy check that our isomorphisms $\mathbb{C}\{\widehat{G}\} \simeq p\mathbb{C}Gp$ and $E \simeq pMp$ are compatible with the module structures. Hence by the earlier proposition,

$$\mathbb{C}Q_G = T_{\mathbb{C}\{\widehat{G}\}} E = T_{p\mathbb{C}Gp}(pMp).$$

The following is a key lemma:

Lemma. *There is an isomorphism $p(T_{\mathbb{C}G}M)p \cong T_{p\mathbb{C}Gp}(pMp)$ as $p\mathbb{C}Gp$-algebras (so $\mathbf{1}_\rho$ still corresponds to p_ρ).*

Proof. Let $A = \mathbb{C}G$. Given an algebra A and and $p = p^2 \in A$ such that $ApA = A$, then for an A-bimodule M we have $M \otimes_A M = Mp \otimes_{pAp} pM$, by a result on your current homework.

Now, by induction,

$$M \otimes_A M \otimes_A \cdots \otimes_A M = Mp \otimes_{pAp} pMp \otimes_{pAp} \cdots \otimes_{pAp} pM$$

and then we can mulitply on the left and right by p to get something more symmetric,

$$p\,(M \otimes_A M \otimes_A \cdots \otimes_A M)\,p = pMp \otimes_{pAp} pMp \otimes_{pAp} \cdots \otimes_{pAp} pMp.$$

But to apply the lemma, we need to check that $\mathbb{C}Gp\mathbb{C}G = \mathbb{C}G$. Using that $\mathbb{C}G = \bigoplus_{\mu \in \widehat{G}} \mathrm{End}(L_\mu)$, we can see that

$$\mathrm{End}(L_\mu) p_\mu \mathrm{End}(L_\mu) = \mathrm{End}(L_\mu)$$

because this algebra has no two-sided ideals; alternatively you can directly check that you can express any matrix as a product with the matrix for p_μ in the middle. $\square$

For a left $\mathbb{C}G$-module N, we have

$$M \otimes_{\mathbb{C}G} N = (V \otimes_{\mathbb{C}} \mathbb{C}G) \otimes_{\mathbb{C}G} N = V \otimes_{\mathbb{C}} N$$

where $v \otimes x \otimes n \mapsto v \otimes x.n$ and the left G-action on $V \otimes_{\mathbb{C}} N$ is $g(v \otimes n) = gv \otimes gn$. Induction shows that $T_{\mathbb{C}G}M \cong T_{\mathbb{C}}V \otimes \mathbb{C}G$, where

$$(v_1 \otimes x_1) \otimes \cdots \otimes (v_i \otimes x_i) \mapsto v_1 \otimes x_1 v_2 \otimes x_1 x_2 v_3 \otimes \cdots \otimes (x_1 \cdots x_{i-1} v_i) \otimes (x_1 \cdots x_i).$$

This explicit formula shows that $T_{\mathbb{C}G}M = T_{\mathbb{C}}V \# G$ as $\mathbb{C}G$-algebras, and we are done. (End of proof of Theorem 2.) $\square$

Lecture 15 (2012-11-02)

Induced Representations

Suppose we have two rings A and B and a homomorphism $f : A \to B$. Given a B-module N, we can treat it as an A-module simply by composing $A \xrightarrow{f} B \to \mathrm{End}(N)$. We will denote the resulting A-module by f^*N, to distinguish it from N itself. (This may be confusing if you are an algebraic geometer, because it would be the pullback to you.) This is a functor from B-Mod to A-Mod.

Note that f makes B an A-bimodule, by

$$a_1 \cdot b \cdot a_2 = f(a_1)bf(a_2).$$

Given an A-module M, we can construct two functors A-$\mathsf{Mod} \to B$-Mod:

- Induction: $B \otimes_A M$ is a left B-module.
- Coinduction: $\mathrm{Hom}_A(B, M)$ is a left B-module.

There are important relations between these constructions:

$$\mathrm{Hom}_B(B \otimes_A M, N) \cong \mathrm{Hom}_A(M, f^*N)$$

$$\mathrm{Hom}_B(N, \mathrm{Hom}_A(B, M)) \cong \mathrm{Hom}_A(f^*N, M).$$

Since we won't be using these, I'll leave them as exercises. They follow easily using the relevant universal properties.

Let G be a group and $H \subset G$ a subgroup. Let $\rho : H \to \mathrm{GL}(M)$ be a representation over a field k. There are three ways of constructing an induced representation, and they all turn out to be equivalent when G is finite.

1. We construct a representation $\mathrm{Ind}_H^G(\rho)$ as follows. Define

   $$\mathrm{Ind}_H^G(\rho) = \left\{ f : G \to M \;\middle|\; \begin{array}{c} f(gh) = \rho(h)f(g) \\ \text{for all } g \in G, h \in H \end{array} \right\}$$

   and then let G act on it by

   $$(gf)(k) := f(g^{-1}k).$$

2. We called the following construction coinduction when we discussed it earlier. We consider $\mathrm{Hom}_H(k\{G\}, M)$ as a G-representation by letting G act on $k\{G\}$ by right translations.
3. When G is finite, we can also use the inclusion $kH \hookrightarrow kG$ to construct $kG \otimes_{kH} M$.

Remark. Any k-algebra B is a B-bimodule, and $B^* = \mathrm{Hom}_k(B, k)$. Left multiplication on the input gives a right action, and right multiplication on the input gives a left action. We say that B is Frobenius algebra if there is a B-bimodule isomorphism $B \cong B^*$.

Suppose that we have a Frobenius algebra. In an isomorphism $B \cong B^*$, look at where $1_B \in B$ goes; say it goes to $\phi \in B^*$. Then because 1_B has a special property, namely that $b \cdot 1 = 1 \cdot b$ for all $b \in B$, then ϕ must have the same property, so that $\phi(b_1 b_2) = \phi(b_2 b_1)$.

Thus, a finite-dimensional algebra B is Frobenius if and only if there exists a bilinear form $\mathrm{tr} : B \to k$ that is symmetric and non-degenerate.

For any finite G, the algebra kG is Frobenius.

If $B \cong B^*$ and B is finite-dimensional, then $\mathrm{Hom}_A(B, M) \cong B^* \otimes_A M \cong B \otimes_A M$.

Remark. Let's consider the first version of induction, in the case when M is the trivial 1-dimensional representation. Then $\mathrm{Ind}_H^G(\mathrm{triv}) = k\{G/H\}$ because it consists of functions from G to k such that $f(gh) = \rho(h)f(g) = f(g)$ for all $g \in G, h \in H$, so the function f is determined by what it does to the cosets G/H.

Observe that $\mathrm{Ind}_H^G(\rho)$ has a natrual structure of a $k\{G/H\}$-module. Since, for any $f \in \mathrm{Ind}_H^G(\rho)$ and $\psi \in k\{G/H\}$, we have $\psi f \in \mathrm{Ind}_H^G(\rho)$, we see that for any ρ, $\mathrm{Ind}_H^G(\rho)$ is a $(k\{G/H\}\#G)$-module. Thus, $\mathrm{Ind}_H^G(\rho)$ is a G-equivariant $k\{G/H\}$-module.

Remark. We have

$$\begin{tikzcd} G \circlearrowright G \times M \circlearrowleft \text{ diagonal } H\text{-action} \arrow[d, "pr_1"', "H\text{-equiv. map}"] \\ G \circlearrowright G \circlearrowleft \; H\text{-action by right mult.} \end{tikzcd}$$

and

$$\begin{tikzcd} G \circlearrowright G \times_H M := (G \times M)/H \supset M \arrow[d, "p"'] \\ G \circlearrowright G/H \ni H/H = \mathrm{pt} \end{tikzcd}$$

We claim that
$$\mathrm{Ind}_H^G(\rho) = \{s : G/H \to (G \times_H M) \text{ which are sections of } p\}.$$

Example. Let $G = \mathbb{R}$ and $H = \mathbb{Z}$, so that $G/H = \mathbb{R}/\mathbb{Z} \cong \mathbb{S}^1$. Let $\chi : \mathbb{Z} \to \mathrm{GL}(M)$ be a 1-dimensional representation of $\mathbb{Z}$ where $1 \mapsto q \in \mathbb{C}^\times$, and hence $n \mapsto q^n$. Then

$$\mathrm{Ind}_{\mathbb{Z}}^{\mathbb{R}}(\chi) = \{f : \mathbb{R} \to \mathbb{C} \mid f(x+1) = q \cdot f(x)\},$$

the space of quasi-periodic functions on $\mathbb{R}$. The fact that we don't get exactly periodic functions is related to the non-triviality of the vector bundles indicated above. If q is an nth root of unity, then we can lift a periodic function on $\mathbb{R}$ (i.e. a function on $\mathbb{S}^1$) to a quasi-periodic function on $\mathbb{R}$ (i.e. a function on an n-sheeted cover of $\mathbb{S}^1$).

Representation Theory of S_n

There is a natural action $S_n \circlearrowright k[x_1, \dots, x_n]$. You're probably all familiar with the following result:

Theorem. *The algebra of symmetric polynomials is the free commutative k-algebra on the elementary symmetric polynomials, i.e. $k[x_1, \dots, x_n]^{S_n} = k[\sigma_1, \dots, \sigma_n]$.*

Recall the Vandermonde polynomial:

$$D_n = \prod_{1 \le i < j \le n} (x_i - x_j) \in k[x_1, \dots, x_n], \quad \deg(D_n) = \frac{n(n-1)}{2}.$$

Let $s_{ij} = (i,j) \in S_n$. Then $s_{ij}(D_n) = -D_n$. The s_{ij} generate S_n, so for any $s \in S_n$, we have $s(D_n) = \pm D_n$. We conclude that there is a map $\operatorname{sign} : S_n \to \{\pm 1\}$ such that $\operatorname{sign}(s_{ij}) = -1$. Let

$$k[x_1, \ldots, x_n]^{\text{sign}} = \{f \in k[x_1, \ldots, x_n] \mid s(f) = \operatorname{sign}(s) \cdot f\}.$$

This is a $k[x_1, \ldots, x_n]^{S_n}$-module.

Proposition. *The module $k[x_1, \ldots, x_n]^{\text{sign}}$ is a rank 1 free $k[x_1, \ldots, x_n]^{S_n}$-module, generated by the Vandermonde polynomial D_n.*

Proof. Suppose that f is skew-symmetric. Then $f|_{x_i = x_j} = 0$ implies that $(x_i - x_j) \mid f$, and because $k[x_1, \ldots, x_n]$ is a UFD and all of the polynomials $x_i - x_j$ are coprime, we must have that

$$D_n = \prod_{i<j} (x_i - x_j) \mid f. \qquad \square$$

Lecture 16 (2012-11-05)

A partition of an integer $n \geq 1$ is an integer sequence $\lambda = (\lambda_1 \geq \lambda_2 \geq \cdots \geq 0)$ such that $\sum \lambda_i = n$. We define $|\lambda| := \sum \lambda_i$. Let $\mathcal{P}_n$ be the set of partitions of n.

Let $R_n^d = \mathbb{Z}^d[x_1, \ldots, x_n]^{S_n}$ denote the homogeneous integer polynomials of degree d in n variables. We use mutli-index notation, so that for $\alpha = (\alpha_1, \ldots, \alpha_n) \in \mathbb{Z}_{\geq 0}^n$, the symbol x^α denotes $x_1^{\alpha_1} \cdots x_n^{\alpha_n}$. We claim that R_n^d is a free $\mathbb{Z}$-module with basis

$$m_\lambda = \sum_{\substack{\alpha \text{ which are} \\ \text{a permutation} \\ \text{of } \lambda \in \mathcal{P}_d}} x^\alpha$$

as λ ranges over the elements of $\mathcal{P}_d$ with no more than n non-zero elements. These m_λ are called the monomial symmetric functions. In our discussion we will be assuming that $n \geq d$; otherwise, there will be $\lambda \in \mathcal{P}_d$ with more than n non-zero elements, so that no $\alpha \in \mathbb{Z}_{\geq 0}^n$ is a permutation of them. Because we would like to talk about R_n^d for every $d \geq 0$, it might seem that working in $\mathbb{Z}[x_1, x_2, \ldots]$ would be preferable, but we can't because symmetric functions in infinitely many variables would require infinite sums, which are nonsensical. Thus, for this class we will let the value of n be in limbo; some statements will technically only be true up to degree n, but since we can choose the value of n to be arbitrarily high, we will omit this issue.

Note that $R = \bigoplus_{d \geq 0} R^d$ is a ring, and that it has the structure of a graded ring. We see that

$$\sum_{d \geq 0} \operatorname{rank}(R^d) t^d = \sum_{d \geq 0} (\#\mathcal{P}_d) t^d = \prod_{k \geq 0} \frac{1}{1 - t^k},$$

by a theorem of Euler.

For each $r > 0$, we let e_r denote the rth elementary symmetric function (again, we are not specifying how many variables these symmetric functions are in; it is just arbitrarily large). Then their generating function is

$$E(t) = \sum_r e_r t^r = \prod_{i \geq 1} (1 + x_i t).$$

(This product is only true up to degree n if we are working with n variables.)

Reader suggestion: to avoid the confusion of n in limbo, perhaps we can consider $R_\infty = \varprojlim R_n$ where the transition maps $R_{n+1} \twoheadrightarrow R_n$ evaluates x_{n+1} to zero. Then $R_\infty \twoheadrightarrow R_n$ for any n. This agrees with (and is motivated by) the use of generating functions. Note that R_∞ is still a graded ring, and $R_\infty^d = R_n^d$ for $n \geq d$.

Now define h_r by

$$H(t) = \sum_{r \geq 0} h_r t^r = \prod_{i \geq 1} \frac{1}{1 - x_i t}.$$

These h_i are called the complete symmetric functions. We can see that in general

$$h_r = \sum_{\lambda \in \mathcal{P}_r} m_\lambda,$$

with $h_0 = 1$ and $h_1 = e_1$.

It is easy to see that $H(t) \cdot E(-t) = 1$. Therefore, looking at coefficients,

$$\sum_{r=0}^{n} (-1)^r e_r h_{n-r} = 0.$$

Because this gives a way of expressing h_n in terms of the e_i's and the h_k for $k < n$, the above result has as a corollary that $R = \mathbb{Z}[h_1, h_2, \ldots]$ (we already knew $R = \mathbb{Z}[e_1, e_2, \ldots]$). In fact, the h_i's freely generate R as a $\mathbb{Z}$-algebra, because if they satisfied any non-trivial relations between each other, we could use the result to turn that into a non-trivial relation between the e_i's, which we know is impossible.

In summary: the m_λ freely generate R as a $\mathbb{Z}$-module, the e_i's freely generate R as a $\mathbb{Z}$-algebra, and the h_i's freely generate R as a $\mathbb{Z}$-algebra.

For each $r \geq 1$, we define the power sum $p_r = \sum x_i^r$. Their generating function is

$$P(t) = \sum_{r \geq 1} p_r t^{r-1}.$$

It is a standard computation that

$$P(t) = \sum_{r \geq 1} p_r t^{r-1} = \sum_{i \geq 1} \sum_{r \geq 1} x_i^r t^{r-1} = \sum_{i \geq 1} \frac{x_i}{1 - x_i t} =$$

$$\sum_{i \geq 1} \frac{d}{dt}\left(\log\left(\frac{1}{1 - x_i t} \right) \right) = \frac{d}{dt}\left(\log\left(\prod_{i \geq 1} \frac{1}{1 - x_i t} \right) \right) = \frac{d\left(\log(H(t))\right)}{dt} = \frac{H'(t)}{H(t)}.$$

We can also then see that

$$P(-t) = \frac{E'(t)}{E(t)}.$$

In coefficents, these observations tell us that

$$n \cdot h_n = \sum_{r=1}^{n} p_r h_{n-r}, \qquad n \cdot e_n = \sum_{r=1}^{n} (-1)^{r-1} p_r e_{n-r}.$$

These are called Newton's identities. As a corollary, if we allow symmetric functions with coefficients in $\mathbb{Q}$ so that we can get rid of the n's, we see that

$$\mathbb{Q} \otimes_{\mathbb{Z}} R = \mathbb{Q}[p_1, p_2, \ldots].$$

Remark. Let $x = \operatorname{diag}(x_1, \ldots, x_n)$, and let $x \circlearrowright V = k^n$. Then $x \circlearrowright \underbrace{V \otimes \cdots \otimes V}_{r \text{ times}}$, via $x \otimes \cdots \otimes x$.

Taking the trace of this action,

$$\operatorname{tr}(x|_{\Lambda^r V}) = e_r(x_1, \ldots, x_n)$$

$$\operatorname{tr}(x|_{\operatorname{Sym}^r V}) = h_r(x_1, \ldots, x_n)$$

You might hope that there is some construction on V such that x has trace $p_r(x_1, \ldots, x_n)$ on it. There is no such thing, but Adams pretended there was such a thing, and his construction is important in topology.

$$\operatorname{tr}(x|_{\text{Adams}(V)}) = p_r(x_1, \ldots, x_n).$$

Given a partition $\lambda = (\lambda_1 \geq \lambda_2 \geq \cdots)$, we define

$$e_\lambda = e_{\lambda_1} e_{\lambda_2} \cdots, \quad h_\lambda = h_{\lambda_1} h_{\lambda_2} \cdots, \quad p_\lambda = p_{\lambda_1} p_{\lambda_2} \cdots.$$

The e_λ form a $\mathbb{Z}$-basis for R, the h_λ also form a $\mathbb{Z}$-basis for R, and the p_λ form a $\mathbb{Q}$-basis for $\mathbb{Q} \otimes_{\mathbb{Z}} R$.

Given a partition $\lambda = (\lambda_1 \geq \lambda_2 \geq \cdots)$, we define $d_i(\lambda) = \#\{s \mid \lambda_s = i\}$. and then define

$$z_\lambda = \prod_{i \geq 1} i^{d_i(\lambda)} \cdot (d_i(\lambda)!).$$

Now note that

$$H(t) = \exp\left(\sum_{r \geq 1} p_r \frac{t^r}{r}\right) = \prod_{r \geq 1} e^{p_r \frac{t^r}{r}} = \prod_{r \geq 1}\left(\sum_{d_r=0}^{\infty} (p_r t^r)^{d_r} \frac{1}{r^{d_r} \cdot d_r!}\right) = \sum_\lambda \frac{1}{z_\lambda} p_\lambda t^{|\lambda|}.$$

Thus,

$$\prod_{i \geq 1} \frac{1}{1 - x_i t} = \sum_\lambda \frac{1}{z_\lambda} p_\lambda t^{|\lambda|}.$$

Schur functions

Given $f \in \mathbb{Z}[x_1, \ldots, x_n]$, we define the alternation of f to be

$$a(f) = \sum_{\sigma \in S_n} \operatorname{sign}(\sigma)\, \sigma(f) \in \mathbb{Z}[x_1, \ldots, x_n]^{\text{sign}}.$$

By last time, we know $D_n \mid a(f)$. Thus, for any $\alpha = (\alpha_1, \ldots, a_n) \in \mathbb{Z}^n_{\geq 0}$, we have that $a(x^\alpha) = 0$ whenever there are any i, j such that $\alpha_i = \alpha_j$. Also note that letting $\rho = (n-1, n-2, \ldots, 0)$, we have $a(x^\rho) = D_n$.

Up to sign, we can rearrange a non-zero $a(x^\alpha)$ so that $\alpha_1 > \cdots > \alpha_n$. For any α, we can write $\alpha = \lambda + \rho$ for $\lambda = (\lambda_1 \geq \lambda_2 \geq \cdots)$. Define the Schur polynomial for λ to be

$$s_\lambda(x) = \frac{a(x^{\lambda+\rho})}{a(x^\rho)} = \frac{\det(x_i^{\lambda_j + n - j})_{i,j}}{\det(x_i^{n-j})_{i,j}}$$

(note that the numerator resembles the Vandermonde determinant, except that we added λ_j's to the powers).

The set $\{a(x^\alpha) \mid \alpha = (\alpha_1 > \cdots > \alpha_n)\}$ forms a $\mathbb{Z}$-basis of $\mathbb{Z}[x_1, \ldots, x_n]^{\text{sign}}$, which (as we proved last class) is a rank 1 free $\mathbb{Z}[x_1, \ldots, x_n]^{S_n}$-module with $\mathbb{Z}[x_1, \ldots, x_n]^{S_n}$-basis $\{D_n\}$. Because s_λ is just defined by dividing by $a(x^\rho) = D_n$, we have that $\{s_\lambda\}$ is a $\mathbb{Z}$-basis of R.

The Cauchy identities involve the expression

$$XY = \frac{1}{\prod_{i,j=1}^{n} (1 - x_i y_j)}$$

The first Cauchy identity states that

$$XY = \sum_\lambda \frac{p_\lambda(x) p_\lambda(y)}{z_\lambda}$$

This follows from the identity

$$\prod \frac{1}{1 - x_i t} = \sum_\lambda \frac{1}{z_\lambda} p_\lambda t^{|\lambda|},$$

where instead of $x_1, \ldots, x_n$, we introduce n^2 variables so that the left side becomes XY and the right side is what we want.

Lecture 17 (2012-11-07)

Let $\lambda \in \mathcal{P}_d$. Recall the various classes of symmetric polynomials we defined last time:

e_λ	elementary
m_λ	monomial
h_λ	complete
p_λ	power sum
s_λ	Schur

Last time, we defined the quantity

$$XY = \prod_{i,j\geq 1} \frac{1}{1 - x_i y_j}.$$

Proposition (2nd Cauchy identity)**.**

$$XY = \sum_\lambda h_\lambda(x) m_\lambda(y) = \sum_\lambda h_\lambda(y) m_\lambda(x).$$

Proof. Recall that the generating function for the complete symmetric polynomials was

$$H(t) = \prod_{i\geq 1} \frac{1}{1 - t x_i}.$$

Thus,

$$XY = \prod_j H(y_j) = \prod_j \sum_{r\geq 0} h_r(x) y_j^r = \sum_{\alpha \in \mathbb{Z}^n_{\geq 0}} h_\alpha(x) y^\alpha = \sum_\lambda h_\lambda(x) m_\lambda(y),$$

where in the last equality we grouped the α's according to which λ they are a permutation of. $\square$

Proposition (3rd Cauchy identity)**.**

$$XY = \sum_\lambda s_\lambda(x) s_\lambda(y).$$

Proof. The determinantal formula says that for any $\alpha \in \mathbb{Z}^n_{\geq 0}$,

$$a(x^\alpha) = a(x^\rho) \det(h_{\alpha_i - n + j})_{ij},$$

where h's with negative indices are declared to be 0, and ρ is as we defined last time,

$$\rho = (n-1, n-2, \ldots, 1, 0).$$

Thus,

$$a(x^\alpha) = a(x^\rho) \sum_{\substack{s \in S_n \\ \beta \in \mathbb{Z}^n_{\geq 0}}} \operatorname{sign}(s) h_{\beta - s(\rho)}(x).$$

Now we use the 2nd identity to see that

$$a(x^\rho) a(y^\rho) \cdot XY = a(x^\rho) \sum_{\substack{s \in S_n \\ \lambda}} h_\lambda(x) \operatorname{sign}(s) y^{s(p)} m_\lambda(y),$$

where we expanded $a(y^\rho)$ as an alternation explicitly. Then

$$a(x^\rho)a(y^\rho) \cdot XY = a(x^\rho) \sum_{\substack{\alpha \in \mathbb{Z}^n_{\geq 0} \\ s \in S_n}} h_\alpha(x) \mathrm{sign}(s) y^{\alpha + s(\rho)}.$$

Letting $\beta = \alpha + s(\rho)$,

$$a(x^\rho)a(y^\rho) \cdot XY = a(x^\rho) \sum_{\beta, s} \mathrm{sign}(s) h_{\beta - s(\rho)}(x) y^\beta,$$

which is precisely the expression in the determinental formula. Thus,

$$a(x^\rho)a(y^\rho) \cdot XY = \sum_{\beta \in \mathbb{Z}^n_{\geq 0}} a(x^\beta) y^\beta = \sum_{\substack{\mu \\ s \in S_n}} a(x^{s(\mu)}) y^{s(\mu)} = \sum_{\mu, s} a(x^\mu) \mathrm{sign}(s) y^{s(\mu)},$$

where in the last step we used that $a(x^{s(\mu)}) = \mathrm{sign}(s) \cdot a(x^\mu)$. Finally, letting $\mu = \lambda + \rho$, this is equal to

$$\sum_\mu a(x^\mu) a(y^\mu) = \sum_\lambda a(x^{\lambda+\rho}) a(y^{\lambda+\rho}).$$

Dividing both sides by $a(x^\rho)a(y^\rho)$ and applying the definition of the Schur polynomials, we are done. □

The Hall inner product $\langle \cdot, \cdot \rangle : R \times R \to \mathbb{Q}$ is defined by $\langle h_\mu, m_\lambda \rangle = \delta_{\lambda\mu}$.

Lemma. *Let $\{u_\lambda\}$ and $\{v_\lambda\}$ be a pair of bases of R. Then the following are equivalent:*

1. $\langle u_\lambda, v_\mu \rangle = \delta_{\lambda\mu}$
2. $\sum_\lambda u_\lambda(x) v_\lambda(y) = XY$.

Proof. Expanding in the basis,

$$u_\lambda = \sum_\nu a_{\lambda\nu} h_\nu, \qquad v_\mu = \sum_\sigma b_{\mu\sigma} m_\sigma.$$

Then 1 is equivalent to

$$\sum_\nu a_{\lambda\nu} b_{\mu\nu} = \delta_{\lambda\mu}$$

and 2 is equivalent to

$$\sum_\lambda u_\lambda(x) v_\lambda(y) = XY \overset{\text{Cauchy 2}}{=} \sum_\nu h_\nu(x) m_\nu(y).$$

But both of these are equivalent to the claim that the matrix of a's is inverse to the matrix of b's, i.e.,

$$\sum_\lambda a_{\lambda\nu} b_{\lambda\sigma} = \delta_{\nu\sigma}.$$ □

Applying the 1st Cauchy identity,

$$XY = \sum_\lambda \frac{1}{z_\lambda} p_\lambda(x) p_\lambda(y)$$

which we proved last time, we get as a corollary of this lemma that

$$\langle p_\lambda, p_\mu \rangle = z_\lambda \cdot \delta_{\lambda\mu}.$$

Another corollary is that $\langle s_\lambda, s_\mu \rangle = \delta_{\lambda\mu}$ (by the 3rd Cauchy identity, and the lemma). Lastly, we get as a corollary that $\langle \cdot, \cdot \rangle$ is a symmetric positive definite bilinear form (this is important because it is defined in an *a priori* non-symmetric way).

Now we define an involution $\tau : R \to R$.

Definition. Define $\tau : R \to R$ by $\tau(e_r) = h_r$. Because these generate R as an algebra, this then implies that $\tau(e_\lambda) = h_\lambda$ for all $\lambda \in \mathcal{P}_n$.

Proposition. *The map τ is an involution, and τ respects $\langle \cdot, \cdot \rangle$.*

Proof. The action of τ is as a matrix T, and Newton's identities tell us that

$$\sum_{r=0}^{n} (-1)^r e_r h_{n-r} = 0.$$

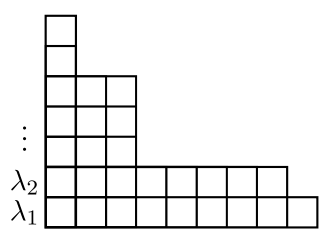
Because $T^2(e_r) = T(h_r)$ and because Newton's identities are symmetric under switching e's and h's, we must have that $T^2(e_r) = e_r$, and hence $T^2 = \mathrm{id}$.

You have equations expressing p_r in terms of e_λ's and h_λ's from last time. These equations and induction imply that $\tau(p_r) = (-1)^{r-1} p_r$. Thus,

$$\langle \tau(p_\lambda), \tau(p_\mu) \rangle = \begin{cases} \pm\langle p_\lambda, p_\mu \rangle = 0 & \text{if } \lambda \neq \mu, \\ \langle p_\lambda, p_\lambda \rangle & \text{if } \lambda = \mu. \end{cases} \qquad \square$$

Young diagrams

The Young diagram of a partition $\lambda = (\lambda_1, \lambda_2, \ldots)$ with $|\lambda| = n$ is



Thus, the total number of blocks in the diagram is n.

There is a natural involution on Young diagrams, $\lambda \mapsto \lambda^t$, defined by interchanging rows and columns.

There is another determinantal formula, which is symmetric with respect to this involution:

$$s_\lambda = \det(e_{\lambda_i^t - i + j}).$$

As a corollary, we get that $\tau(s_\lambda) = s_{\lambda^t}$ (apply involution to first determinantal formula; e's and h's are interchanged, and we flip λ).

Now we'll start relating this to the representation theory of S_n.

Fix a field k, and consider the polynomial ring $k[x_1, \dots, x_n]$.

Let $\{1, \dots, n\} = I_1 \sqcup \cdots \sqcup I_k$ be a partition with $\#I_j = \lambda_j$, which collectively we will call I. This naturally corresponds to λ, a partition in the sense we've been using. Then we define

$$S_I = S_{I_1} \times \cdots \times S_{I_k} \subset S_n.$$

We define D_I to be a product of certain Vandermonde determinants of various sizes,

$$D_I = D_{I_1} \times \cdots \times D_{I_k},$$

where

$$D_{I_m} := \prod_{i,j \in I_m} (x_i - x_j).$$

Theorem. *Let* $\operatorname{char}(k) = 0$, *and let* I *be a partition as above. Then* $V_\lambda := kS_n \cdot D_I$ *is an irrep of* S_n, *and in fact* $\{V_\lambda \mid \lambda \in \mathcal{P}_n\} \cong \widehat{S_n}$.

Lecture 18 (2012-11-09)

Recall some notation from last time: we let $\{1, \ldots, n\} = I_1 \sqcup \cdots \sqcup I_k$ be a partition, which collectively we will call I. This naturally corresponds to λ, a partition in the sense we've been using, by letting $\lambda_j = \# I_j$. We also defined a more general Vandemonde polynomial

$$D_I = D_{I_1} \cdots D_{I_k},$$

with

$$d_\lambda := \deg(D_I) = \sum \frac{\lambda_i(\lambda_i - 1)}{2}.$$

We then defined

$$V_\lambda = kS_n \cdot D_I \subset k^{d_\lambda}[x_1, \ldots, x_n],$$

a representation which is called the Specht S_n-module (Reader comment: this is actually what most references call the Specht module of λ^t. The module $V^\lambda = V_{\lambda^t}$ we later construct is the Specht module for λ). The subgroup

$$S_I = S_{I_1} \times \cdots \times S_{I_k} \subset S_n$$

is called a Young subgroup.

Theorem.

1. *V_λ is irreducible.*
2. *$V_\lambda \not\cong V_\mu$ for $\lambda \neq \mu$.*
3. *Any irrep of S_n is isomorphic to some V_λ.*

Proof. We'll assume that $k \subseteq \mathbb{C}$, though it holds in more generality. It will suffice to show that V_λ is simple for $k = \mathbb{C}$, since extending the field can only cause it to split more.

Suppose $V_\lambda = V \oplus V'$ is a non-trivial S_n-stable decomposition. Then $\mathrm{pr}_V \in \mathrm{End}_{\mathbb{C}}(V_\lambda)$. To reach a contradiction, we will show that every intertwiner $f : V_\lambda \to V_\lambda$ is a scalar operator. Let f be an intertwiner; then

$$f(D_I) = D' \in k^{d_\lambda}[x_1, \ldots, x_n]$$

for some D'. We have $s(D_I) = \mathrm{sign}(s) \cdot D_I$ for all $s \in S_I$, so $s(D') = \mathrm{sign}(s) \cdot D'$ for all $s \in S_I$ because f is an intertwiner. Thus, for all $i, j \in I_r$ for any r, we have that $s_{ij}(D') = -D'$, so D' vanishes on the set

$$\{(a_1, \ldots, a_n) \in \mathbb{C}^n \mid a_i = a_j\},$$

hence $(x_i - x_j) \mid D'$, and because we are working in a UFD,

$$\left(\prod_{p=1}^{k} \prod_{i,j \in I_p} (x_i - x_j) \right) \mid D',$$

so that $D_I \mid D'$. But D_I and D' are homogeneous polynomials of degree d_λ, so $D' = c \cdot D_I$ for some $c \in \mathbb{C}$. Thus $f(D_I) = c \cdot D_I$, and so for any $a \in \mathbb{C}S_n$, we have

$$f(aD_I) = a \cdot f(D_I) = c \cdot a \cdot D_I,$$

and hence $f = c \cdot \mathrm{id}$.

The same argument shows that there are no interwiners between V_λ and V_μ if $\lambda \neq \mu$.

The conjugacy classes of S_n are indexed by $\mathcal{P}_n$. Thus, the number of conjugacy classes is $\#\mathcal{P}_n = \#\widehat{S_n}$. This proves (3). $\square$

Corollary.

1. $[k^d[x_1, \ldots, x_n] : V_\lambda] = \begin{cases} 1 & \text{if } d = d_\lambda, \\ 0 & \text{if } d < d_\lambda. \end{cases}$
2. *The representation V_λ is defined over $\mathbb{Q}$.*
3. $V_\lambda \cong V_\lambda^*$.

Proof. There exists an S_n-invariant, positive definite $\mathbb{Q}$-bilinear form β on V_λ (considered as a vector space over $\mathbb{Q}$), and the map from $V \to V^*$ sending v to $\beta(-, v)$ is a $\mathbb{Q}$-linear function (we can't do this over $\mathbb{C}$ because it'd be skew-linear). $\square$

Fix a group G and a commutative ring Z (which in most cases will in fact be $\mathbb{Z}$).

Definition. The Grothendieck group $K_Z(G)$ is defined as follows. Take M, the free Z-module with basis consisting of isomorphism classes $[V]$ of finite-dimensional, completely reducible G-representations V, and quotient M by the relation $[V \oplus V'] - [V] - [V']$.

Note that, for example, if $V = L_1^{m_1} \oplus \cdots \oplus L_k^{m_k}$ where $L_i \in \widehat{G}$, we have

$$[V] = m_1[L_1] + \cdots + m_k[L_k].$$

Thus, we could also think of $K_Z(G)$ as being the free Z-module with basis $[L_i]$, for each $L_i \in \widehat{G}$. Note that any element of $K_Z(G)$ can be put in the form $[M] - [N]$ by looking at the terms with positive or negative coefficients and grouping them.

For an example, note that if $G = \{e\}$, then $K_Z(\{e\}) = \mathbb{Z}$, where $[V] \leftrightarrow \dim(V)$.

Let G be a finite group. We define an inner product $K_Z(G) \times K_Z(G) \to Z$ by

$$\langle [L], [L'] \rangle = \begin{cases} 1 & \text{if } L \cong L', \\ 0 & \text{if } L \not\cong L'. \end{cases}$$

Alternatively, we can define

$$\langle [M], [N] \rangle = \dim(\mathrm{Hom}_G(M, N)).$$

Moreover, $K_Z(G)$ has a commutative ring structure, by $[M][N] = [M \otimes N]$. This is valid because $M \otimes (N_1 \oplus N_2) \cong (M \otimes N_1) \oplus (M \otimes N_2)$. The unit for the multiplication is the trivial representation.

Define $\chi : K_{\mathbb{C}}(G) \to \mathbb{C}\{G\}^G$ by sending $[M]$ to χ_M. We know that $\chi_{M \otimes N} = \chi_M \cdot \chi_N$, so that χ is a ring homomorphism.

Proposition. *χ is in fact an isometric ring isomorphism.*

Proof. This follows directly from the orthogonality relations for irreducible characters, and the fact that the irreducible characters are a basis for the space of class functions. $\square$

Now let $G = S_d$, and let R^d be the homogeneous symmetric functions of degree d (in a large, unspecified number of variables). We define $\psi : S_d \to R^d$ by $\psi(s) = p_{\lambda(s)}$, where $\lambda(s)$ is the cycle type of s. Now we define a map on the space of class functions, $\Psi : \mathbb{C}\{S_d\}^{S_d} \to R^d$, by

$$\Psi(f) = \frac{1}{d!} \sum_{s \in S_d} f(s)\psi(s)$$

We often refer to this as $\langle f, \psi \rangle_{S_d}$, even though ψ is not the same kind of object as f.

Lemma. *If $s \in C_\lambda$ (i.e., s has cycle type λ) then*

$$\#(\text{centralizer of } s) = z_\lambda.$$

This then implies that $\#C_\lambda = \frac{\#S_d}{\#(\text{centralizer})} = \frac{d!}{z_\lambda}$.

Corollary. $\Psi(\mathbf{1}_{C_\lambda}) = z_\lambda^{-1} p_\lambda$

A key map we will talk about next class is the Frobenius characteristic map

$$\text{ch} : K_{\mathbb{C}}(S_d) \xrightarrow{\chi} \mathbb{C}\{S_d\}^{S_d} \xrightarrow{\Psi} R^d$$

defined by sending $[M]$ to $\langle \chi_M, \psi \rangle_{S_d}$.

Lecture 19 (2012-11-12)

Using the notation from last time, $K_Z(S_d)$ is the Grothendieck group of finite-dimensional S_d-representations over a commutative ring Z.

We can make a commutative ring structure on

$$K_Z = \bigoplus_{d \geq 0} K_Z(S_d)$$

by defining the circle product $\circ : K_Z(S_m) \times K_Z(S_n) \to K_Z(S_{m+n})$ as follows: we consider the natural inclusion $j : S_m \times S_n \to S_{m+n}$, and for any M and N (representations of S_m and S_n, respectively), we define

$$M \circ N = \operatorname{Ind}_{S_m \times S_n}^{S_{m+n}} M \boxtimes N.$$

More generally, given $\lambda = (\lambda_1 \geq \lambda_2 \geq \cdots) \in \mathcal{P}_n$, we define

$$S_\lambda = S_{\lambda_1} \times S_{\lambda_2} \times \cdots,$$

and given representations M_i over each S_{λ_i}, we can form

$$M_1 \circ M_2 \circ \cdots \circ M_k = \operatorname{Ind}_{S_\lambda}^{S_n}(M_1 \boxtimes M_2 \boxtimes \cdots \boxtimes M_k).$$

Lemma. *The circle product is associative and commutative, and thus K_Z is a commutative associative ring.*

Proof. Let M, N, and L be representations of S_m, S_n, and S_ℓ respectively. Then directly from the definition,

$$(M \circ N) \circ L = \operatorname{Ind}_{S_m \times S_n \times S_\ell}^{S_{m+n+\ell}}(M \boxtimes N \boxtimes L) = M \circ (N \circ L).$$

Commutativity follows from the fact that inducing from two subgroups which are conjugate to one another gives the same result, so

$$\operatorname{Ind}_{S_m \times S_n}^{S_{m+n}}(M \boxtimes N) = \operatorname{Ind}_{S_n \times S_m}^{S_{m+n}}(N \boxtimes M). \qquad \square$$

Frobenius characteristic

We define the Frobenius characteristic map $\mathrm{ch}_n : K_{\mathbb{C}}(S_n) \xrightarrow{\chi} \mathbb{C}\{S_n\}^{S_n} \xrightarrow{\Psi} \mathbb{C} \otimes_{\mathbb{Z}} R$ (where R is the ring of symmetric functions[5], complexified by tensoring with $\mathbb{C}$) by sending $[M]$ to

$$\frac{1}{n!} \sum_{s \in S_n} \chi_M(s) \cdot p_{\lambda(s)}.$$

Then we let ch be the sum of all these maps,

$$\mathrm{ch} = \left(\bigoplus_{n \geq 0} \mathrm{ch}_n \right) : K_{\mathbb{C}} \to \mathbb{C} \otimes_{\mathbb{Z}} R.$$

[5]Reader believes that everything works out if we take R to be R_∞ as defined in Lecture 16

Theorem.

1. *The map* ch *restricts to a ring isomorphism* $(K_{\mathbb{Z}}, \circ) \to R$.
2. *The map* ch *is an isometry.*
3. *The map* ch *takes* $\mathrm{sign} \otimes (-)$ *to* τ*, i.e.* $\mathrm{ch}(\mathrm{sign} \otimes M) = \tau(\mathrm{ch}(M))$.
4. *The map* ch *acts as follows, for all* $\lambda \in \mathcal{P}_n$*:*
   - $V_\lambda \longmapsto s_{\lambda^t}$
   - $\mathrm{Ind}_{S_\lambda}^{S_n}(\mathrm{triv}) \longmapsto h_\lambda$
   - $\mathrm{Ind}_{S_\lambda}^{S_n}(\mathrm{sign}) \longmapsto e_\lambda$

Remark. Let $j : H \hookrightarrow G$ be a group embedding. Let E and F be representations of H and G, respectively. Then there is a canonical isomorphism

$$\mathrm{Hom}_G(\mathrm{Ind}_H^G E, F) \cong \mathrm{Hom}_H(E, j^* F).$$

Thus, for any class function $f \in \mathbb{C}\{G\}^G$,

$$\langle \chi_{\mathrm{Ind}_H^G E}, f \rangle_G = \langle \chi_E, f|_H \rangle_H.$$

This is the key ingredient in the proof of the first statement; the rest is just the definitions.

Proof of 1 (ring homomorphism). Let M and N be representations of S_m and S_n, respectively. Then

$$\begin{aligned}
\mathrm{ch}(M \circ N) &= \Psi(\chi(\mathrm{Ind}_{S_m \times S_n}^{S_{m+n}}(M \boxtimes N))) \\
&= \langle \chi_{\mathrm{Ind}_{S_m \times S_n}^{S_{m+n}}(M \boxtimes N)}, \psi \rangle_{S_{m+n}} \\
\text{(by remark)} \quad &= \langle \chi_{M \boxtimes N}, \psi|_{S_m \times S_n} \rangle_{S_m \times S_n} \\
&= \frac{1}{m!}\frac{1}{n!} \sum_{\substack{s \in S_m \\ s' \in S_n}} \chi_{M \boxtimes N}(s \times s') \cdot \psi(s \times s') \\
&= \frac{1}{m!n!} \sum_{s,s'} \chi_M(s) \chi_N(s') p_{\lambda(s \times s')}.
\end{aligned}$$

Note that, for any $\mu \in \mathcal{P}_m$ and $\nu \in \mathcal{P}_n$, we have $p_{\mu \sqcup \nu} = p_\mu \cdot p_\nu$. The cycle type $\lambda(s \times s')$ is just $\lambda(s) \sqcup \lambda(s')$, and therefore $p_{\lambda(s \times s')} = p_{\lambda(s)} \cdot p_{\lambda(s')}$.

$$\begin{aligned}
&= \frac{1}{m!n!} \sum_{s,s'} \chi_M(s) \chi_N(s') p_{\lambda(s)} p_{\lambda(s')} \\
&= \left[\frac{1}{m!} \sum_{s \in S_m} \chi_M(s) p_{\lambda(s)} \right] \left[\frac{1}{n!} \sum_{s' \in S_n} \chi_N(s') p_{\lambda(s')} \right]
\end{aligned}$$

so we have shown ch is a ring homomorphism. We will show it is an isomorphism next lecture. $\square$

Proof of 2. We showed that χ was an isometry last time, so it will suffice to show that Ψ is an isometry because $\mathrm{ch} = \chi \circ \Psi$.

For any $\lambda, \mu \in \mathcal{P}_n$, we take the Hall inner product

$$\langle \Psi(\mathbf{1}_{C_\lambda}), \Psi(\mathbf{1}_{C_\mu}) \rangle_{\mathrm{Hall}}.$$

We know that $\Psi(\mathbf{1}_{C_\lambda}) = z_\lambda^{-1} \cdot p_\lambda$, so we compute

$$\begin{aligned}\langle \Psi(\mathbf{1}_{C_\lambda}), \Psi(\mathbf{1}_{C_\mu}) \rangle_{\mathrm{Hall}} &= \langle z_\lambda^{-1} \cdot p_\lambda, z_\mu^{-1} \cdot p_\mu \rangle = z_\lambda^{-1} z_\mu^{-1} \langle p_\lambda, p_\mu \rangle \\ &= \begin{cases} z_\lambda^{-1} & \text{if } \lambda = \mu, \\ 0 & \text{if } \lambda \neq \mu \end{cases} = \langle \mathbf{1}_{C_\lambda}, \mathbf{1}_{C_\mu} \rangle\end{aligned}$$

□

Proof of 3. Write the character $\chi_M = \sum_{\lambda \in \mathcal{P}_n} \chi(C_\lambda) \cdot \mathbf{1}_{C_\lambda}$ so that

$$\mathrm{ch}(M) = \sum_{\lambda \in \mathcal{P}_n} \chi(C_\lambda) \cdot z_\lambda^{-1} \cdot p_\lambda.$$

We have $\tau(p_d) = (-1)^{d-1} \cdot p_d$ and taking product, $\tau(p_\lambda) = (-1)^{\sum(\lambda_i - 1)} \cdot p_\lambda$. Thus,

$$\tau(\mathrm{ch}(M)) = \sum_{\lambda \in \mathcal{P}_n} \chi(C_\lambda) \cdot z_\lambda^{-1} (-1)^{\sum \lambda_i - 1} \cdot p_\lambda$$

Note that

$$\mathrm{sign}(\text{cycle of length } d) = (-1)^{d-1},$$

so

$$\mathrm{sign}|_{C_\lambda} = (-1)^{\sum(\lambda_i - 1)}.$$

Thus

$$\chi_{\mathrm{sign} \otimes M} = \sum_{\lambda \in \mathcal{P}_n} \chi_{\mathrm{sign} \otimes M}(C_\lambda) \mathbf{1}_{C_\lambda} = \sum_\lambda \chi_M(C_\lambda) \cdot (-1)^{\sum(\lambda_i - 1)} \mathbf{1}_{C_\lambda},$$

and therefore

$$\mathrm{ch}(\mathrm{sign} \otimes M) = \sum_\lambda \chi(C_\lambda)(-1)^{\sum \lambda_i - 1} \Psi(\mathbf{1}_{C_\lambda}) = \sum_\lambda \chi(C_\lambda)(-1)^{\sum(\lambda_i - 1)} z_\lambda^{-1} p_\lambda$$

which is exactly the expression we wanted. □

Proof of 4. Let's compute the Frobenius character of the trivial representation.

$$\mathrm{ch}(\mathrm{triv}_n) = \sum_{\lambda \in \mathcal{P}_n} z_\lambda^{-1} p_\lambda = h_n \in R.$$

For the sign representation, we just get

$$\mathrm{ch}(\mathrm{sign}) = \tau(h_n) = e_n.$$

Using the fact that ch is a homomorphism (which we just proved),

$$\begin{aligned}\mathrm{ch}(\mathrm{Ind}_{S_\lambda}^{S_n}(\mathrm{triv})) &= \mathrm{ch}(\mathrm{triv}_{\lambda_1} \circ \mathrm{triv}_{\lambda_2} \circ \cdots) \\ &= \mathrm{ch}(\mathrm{triv}_{\lambda_1}) \mathrm{ch}(\mathrm{triv}_{\lambda_2}) \cdots\end{aligned}$$

$$
\begin{aligned}
&= h_{\lambda_1} h_{\lambda_2} \cdots \\
&= h_\lambda. \qquad \square
\end{aligned}
$$

For any $\lambda \in \mathcal{P}_n$, we define an alternating sum in the Grothendieck group,

$$V^\lambda = \sum_{s \in S_n} \operatorname{sign}(s) \left[\operatorname{Ind}_{S_{\lambda+\rho-s(\rho)}}^{S_n}(\text{triv})\right]$$

so that

$$
\begin{aligned}
\operatorname{ch}(V^\lambda) &= \sum_{s \in S_n} \operatorname{sign}(s) \operatorname{ch}(\operatorname{Ind} \cdots) \\
&= \sum_{s \in S_n} \operatorname{sign}(s) \cdot h_{\lambda+\rho-s(\rho)} \overset{\substack{\text{determinantal} \\ \text{identity}}}{=} s_\lambda.
\end{aligned}
$$

Therefore

$$\langle V^\lambda, V^\mu \rangle = \langle \operatorname{ch}(V^\lambda), \operatorname{ch}(V^\mu) \rangle_{\text{Hall}} = \langle s_\lambda, s_\mu \rangle_{\text{Hall}} = \delta_{\lambda\mu},$$

and in particular,

$$\langle V^\lambda, V^\lambda \rangle = 1$$

which implies that either V^λ or $-V^\lambda$ (this sign is in the Grothendieck group) is an actual irrep. Next time we will see that $V_\lambda = V^{\lambda^t}$, which finishes the proof.

Lecture 20 (2012-11-14)

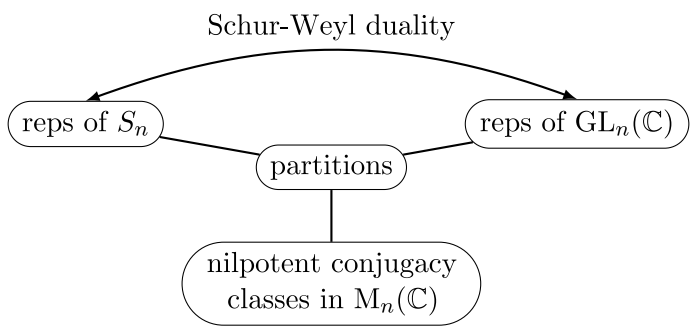
Last time we constructed a ring homomorphism from the Grothendieck group $K_{\mathbb{Z}} = \bigoplus_n K_{\mathbb{Z}}(S_n)$ to the ring R by sending V^λ to s_λ. We showed that for all $\lambda \in \mathcal{P}_n$, either $\pm V^\lambda \in \widehat{S_n}$.

It remains to show that this map is an isomorphism. We see that ch is surjective, since the Schur functions form a $\mathbb{Z}$-basis of R, and $s_\lambda \in \operatorname{im}(\mathrm{ch})$. The map ch is injective, as it is an isometry.

Corollary. $\chi_{V^\lambda}(c_\mu) = \langle s_\lambda, p_\mu \rangle_{\text{Hall}}$

Proof. We have
$$s_\lambda = \mathrm{ch}(V^\lambda) = \sum_{\mu \in \mathcal{P}_n} z_\mu^{-1} \chi_{V^\lambda}(c_\mu) p_\mu,$$
so
$$\langle s_\lambda, p_\nu \rangle = \sum_\mu z_\mu^{-1} \chi_{V^\lambda}(c_\mu) \langle p_\mu, p_\nu \rangle = \chi_{V^\lambda}(c_\mu).$$
□

There are three main ways partitions come up in what we've been doing.



We define a partial order on partitions. Given $\lambda = (\lambda_1, \ldots), \mu = (\mu_1, \ldots) \in \mathbb{Z}^n$, we say $\lambda \leq \mu$ if $\lambda_1 \leq \mu_1$, and $\lambda_1 + \lambda_2 \leq \mu_1 + \mu_2$, ..., and $\lambda_1 + \cdots + \lambda_n \leq \mu_1 + \cdots + \mu_n$.

Define O_λ to be the nilpotent conjugacy class with Jordan blocks $\lambda_1, \ldots, \lambda_n$.

Proposition.

1. *$O_\lambda \subseteq \overline{O_\mu} \iff \lambda \leq \mu$.*
2. *$\lambda \leq \mu \iff \mu^t \leq \lambda^t$.*
3. *$s(\rho) < \rho$ for all non-identity $s \in S_n$.*

Proposition.

1. $[\mathrm{Ind}_{S_\mu}^{S_n} \mathrm{triv} : V^\lambda] = \begin{cases} 0 & \textit{unless } \mu \leq \lambda, \\ 1 & \textit{if } \mu = \lambda. \end{cases}$
2. $[\mathrm{Ind}_{S_\mu}^{S_n} \mathrm{sign} : V^\lambda] = \begin{cases} 0 & \textit{unless } \mu \leq \lambda^t, \\ 1 & \textit{if } \mu = \lambda^t. \end{cases}$
3. $V^\lambda = V_{\lambda^t}$

Proof.

$$V^\lambda = \sum_{s\in S_n} \mathrm{sign}(s)\cdot \left[\mathrm{Ind}_{S_{\lambda+\rho-s(p)}}^{S_n}(\mathrm{triv})\right]$$

$$= \mathrm{Ind}_{S_\lambda}^{S_n}(\mathrm{triv}) + \sum_{\mu>\lambda} a_{\lambda\mu}\left[\mathrm{Ind}_{S_\mu}^{S_n}(\mathrm{triv})\right]$$

The transition matrix from $\mathrm{Ind}_{S_\mu}^{S_n}$ to V^λ is of the form

$$\begin{pmatrix} 1 & * & \cdots & * \\ & 1 & \ddots & \vdots \\ & & \ddots & * \\ & & & 1 \end{pmatrix}$$

with respect to the partial ordering. The inverse of a strict upper triangular matrix is also strictly upper triangular, so

$$\mathrm{Ind}_{S_\lambda}^{S_n}(\mathrm{triv}) = V^\lambda + \sum_{\mu>\lambda} b_{\lambda\mu}\cdot V^\mu$$

which proves part 1. Part 2 follows from part 1 by applying ch and τ.

Thus V^λ is the unique irrep of S_n which occurs both in $\mathrm{Ind}_{S_\lambda}^{S_n}(\mathrm{triv})$ and $\mathrm{Ind}_{S_{\lambda^t}}^{S_n}(\mathrm{sign})$.

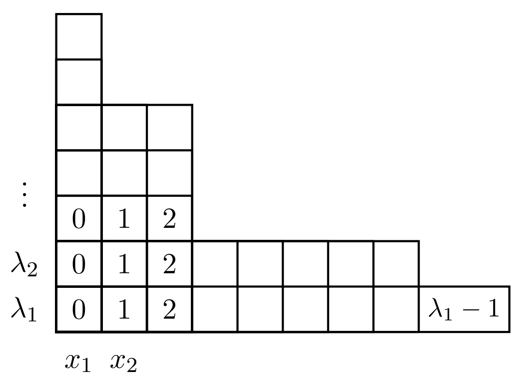
Now we claim that V_λ occurs in $\mathrm{Ind}_{S_{\lambda^t}}^{S_n}(\mathrm{triv})$ and $\mathrm{Ind}_{S_\lambda}^{S_n}(\mathrm{sign})$. Recall that a $\lambda\in\mathcal{P}_n$ corresponds to

$$D_\lambda = D_{\lambda_1}\cdot D_{\lambda_2}\cdots$$

and $s(D_\lambda) = \mathrm{sign}(s)\cdot D_\lambda$ for all $s\in S_\lambda$, so there exists a surjective map $\mathrm{Ind}_{S_\lambda}^{S_n}(\mathrm{sign})\to V_\lambda$, sending 1 to D_λ. Because V_λ is simple, this implies that V_λ occurs in $\mathrm{Ind}_{S_\lambda}^{S_n}(\mathrm{sign})$.

In our notation, $D_n = a(x^\rho)$, so that

$$D_\lambda = a(x^{\rho_{\lambda_1}})a(x^{\rho_{\lambda_2}})\cdots$$



Expanding the product and counting along columsn instead of rows (see diagram), we have

$$D_\lambda = (x_1x_{\lambda_1+1}x_{\lambda_1+\lambda_2+1}\cdots)^0(x_2x_{\lambda_1+2}x_{\lambda_1+\lambda_2+2}\cdots)^1\cdots$$

Therefore S_{λ^t} acts trivially on D_λ with coordinates transposed, i.e., we get a nonzero map $j: Ind_{S_{\lambda^t}}^{S_n}(\mathrm{triv})\to V_\lambda$. This shows Part 3. $\square$

Representation theory of S_n and GL_m

Let V be a finite-dimensional $\mathbb{C}$-vector space. For any $n \geq 1$, we have a natural action $S_n \circlearrowright V^{\otimes n}$. We let $j : \mathrm{End}_{\mathbb{C}}(V) \to \mathrm{End}_{\mathbb{C}}(V^{\otimes n})$ be the Lie algebra action defined by

$$a(v_1 \otimes v_2 \otimes \cdots \otimes v_n) = (av_1) \otimes v_2 \otimes \cdots \otimes v_n + v_1 \otimes (av_2) \otimes \cdots \otimes v_n + \cdots$$

Lemma. $\mathrm{End}_{S_n}(V^{\otimes n})$ *is the algebra generated by* $\mathrm{im}(j)$*.*

Proof. The inclusion $\supseteq$ is clear.

Now we will show the other inclusion. First, we claim

$$\mathrm{End}(V^{\otimes n}) \cong \mathrm{End}(V)^{\otimes n}$$

$$\supseteq$$

$$\begin{aligned} \mathrm{End}(V^{\otimes n}) &= V^{\otimes n} \otimes (V^{\otimes n})^* \\ &= V^{\otimes n} \otimes (V^*)^{\otimes n} \\ &= (V \otimes V^*)^{\otimes n} \\ &= (\mathrm{End}(V))^{\otimes n} \end{aligned}$$

Second, we see that

$$\mathrm{End}_{S_n}(V^{\otimes n}) = (\mathrm{End}(V^{\otimes n}))^{S_n} = ((\mathrm{End}(V))^{\otimes n})^{S_n}.$$

Third, we know from the homework that $(A^{\otimes n})^{S_n}$ is generated by elements of the form

$$(a \otimes 1 \otimes \cdots \otimes 1) + (1 \otimes a \otimes \cdots \otimes 1) + \cdots$$

for any algebra A, and thus this is true in particular for $A = \mathrm{End}(V)$. $\square$

Lecture 21 (2012-11-16)

Let V be a finite-dimensional vector space over $\mathbb{C}$, and consider the tensor power $V^{\otimes n}$. We have two natural actions, $S_n \circlearrowright V^{\otimes n} \circlearrowleft \mathrm{GL}(V)$, where S_n permutes tensorands, and $g \in \mathrm{GL}(V)$ acts by

$$g(v_1 \otimes \cdots \otimes v_n) = gv_1 \otimes \cdots \otimes gv_n.$$

This gives us maps

$$S_n \xrightarrow{j_1} \mathrm{End}_{\mathbb{C}}(V^{\otimes n}) \xleftarrow{j_2} \mathrm{GL}(V)$$

Let $A(S_n)$ be the $\mathbb{C}$-linear span of $\mathrm{im}(j_1)$, and similarly let $A(\mathrm{GL})$ be the $\mathbb{C}$-linear span of $\mathrm{im}(j_2)$.

Theorem (Schur-Weyl duality)**.**

1. *Inside* $\mathrm{End}_{\mathbb{C}}(V^{\otimes n})$, *we have* $A(S_n)^! = A(\mathrm{GL})$ *and* $A(\mathrm{GL})^! = A(S_n)$.
2. *If* $\dim(V) \geq n$, *then each irrep of* S_n *occurs in* $V^{\otimes n}$, *and in particular,*

$$V^{\otimes n} = \bigoplus_{\lambda \in \mathcal{P}_n} V_\lambda \otimes L_\lambda$$

where the V_λ *are the Specht modules and the* L_λ *are mutually non-isomorphic* $\mathrm{GL}(V)$*-irreps.*

Proof of 1. Clearly, $A(\mathrm{GL}) \subseteq A(S_n)^!$; the non-trivial part is the other inclusion. The argument we will use is an illustration of Lie theory.

Consider $a \in \mathrm{End}_{\mathbb{C}}(V)$. Then $e^{ta} \in \mathrm{GL}(V)$ for any $t \in \mathbb{C}$, so that $j_2(e^{ta}) \in A(\mathrm{GL})$ for all $t \in \mathbb{C}$. Applying it to a simple tensor,

$$\begin{aligned} j_2(e^{ta})(v_1 \otimes \cdots \otimes v_n) &= e^{ta}(v_1) \otimes \cdots \otimes e^{ta}(v_n) \\ &= (v_1 + ta(v_1) + o(t)) \otimes \cdots \otimes (v_n + ta(v_n) + o(t)) \\ &= (v_1 \otimes \cdots \otimes v_n) + t\left(\sum_{i=1}^n (v_1 \otimes \cdots \otimes av_i \otimes \cdots \otimes v_n)\right) + o(t) \end{aligned}$$

Taking the derivative with respect to t and evaluating at 0, we see that

$$(a \otimes 1 \otimes \cdots \otimes 1) + (1 \otimes a \otimes \cdots \otimes 1) + \cdots \in A(\mathrm{GL})$$

for all $a \in \mathrm{End}(V)$. (Since $A(\mathrm{GL})$ is a finite dimensional vector space, it is topologically closed.) By the lemma from last time, the elements of the above form generate the algebra $\mathrm{End}_{S_n}(V^{\otimes n}) = A(S_n)^!$.

Since $\mathbb{C}S_n$ is a semisimple algebra, we have that $A(S_n)$ is a semisimple algebra, and you will show on the homework that this implies $A(S_n)^!$ is semisimple, hence $A(\mathrm{GL})$ is semisimple, hence $A(S_n) = A(S_n)^{!!} = A(\mathrm{GL})^!$. □

Proof of 2. We want to show that there is a copy of the regular representation of S_n on $V^{\otimes n}$ if $\dim(V) \geq n$. Let $\{v_1, \ldots, v_d \mid d \geq n\}$ be a $\mathbb{C}$-basis of V, and let $s \in S_n$. Then the elements

$$v_{s(1)} \otimes \cdots \otimes v_{s(n)} \in V^{\otimes n}$$

span a copy of $\mathbb{C}S_n$. □

Jacobson density

Let X and Y be sets, and consider $\mathrm{Map}(X,Y)$. We equip this with the pointwise topology, which is defined as follows. For $f \in \mathrm{Map}(X,Y)$, a basis of open neighborhoods of f is given by, for all $n \geq 1$ and $x_1, \dots, x_n \in X$,

$$\mathcal{U}_{x_1,\dots,x_n} = \{f' : X \to Y \mid f'(x_i) = f(x_i) \text{ for all } i = 1, \dots, n\}.$$

Thus, $f_i \to f$ if and only if, for any $x \in X$, we have $f_i(x) = f(x)$ for all $i \gg 0$.

Let A be a ring, and let M be an A-module; equivalently, we have an action map $A \to \mathrm{End}_{\mathbb{Z}}(M)$. We have

$$A \to A_M := \mathrm{im}(\text{action}) \hookrightarrow A^{!!}_M.$$

Theorem (Jacobson density)**.** *If M is a semisimple A-module, then A_M is pointwise dense in $A^{!!}_M$; in other words, for any $A^!_M$-linear map $f : M \to M$ and any collection $m_1, \dots, m_n \in M$, there is an $a \in A$ such that $f(m_1) = am_1$ for all $i = 1, \dots, n$.*

Example. Let $A = k$, so that M is a vector space over k, say with $\dim(M) = n$. Then $k^! = A^!_M = \mathrm{M}_n(k)$, and so $k^{!!} = A^{!!}_M = \mathrm{M}_n(k)^! = k$.

Lemma. *Let A be a ring, and let L be an A-module. Let $M = L^n$. Then $A^{!!}_{L^n} \cong A^{!!}_L$.*

Example. Let $L = A$. Then $A^!_L = A^{\mathrm{op}}$, so that $A^{!!}_L = (A^{\mathrm{op}})^{\mathrm{op}} = A$. Thus, the lemma implies that $(A_{A^n})^{!!} = A$, so we see that the fact that k was a field in our earlier example was unnecessary.

Proof of Lemma. First, recall that we proved a long time ago,

$$A^!_{L^n} = \mathrm{End}_A(L^n) = \mathrm{M}_n(\mathrm{End}_A(L)) = \mathrm{M}_n(A^!_L).$$

Second, note that, if L is a B-module, then L^n has a $\mathrm{M}_n(B)$-module structure, and

$$\mathrm{End}_{\mathrm{M}_n(B)}(L^n) = \{\mathrm{diag}(a, \dots, a) \mid a \in \underbrace{\mathrm{End}_B(L)}_{:=B^!_L}\}.$$

Third, we therefore have that $(A_{L^n})^{!!} = (\mathrm{M}_n(A^!_L))^!$. We have $B = A^!_L$, and by our second observation,

$$(A_{L^n})^{!!} = (\mathrm{M}_n(A^!_L))^! = \{\mathrm{diag}(a, \dots, a) \mid a \in (A^!_L)^! = A^{!!}_L\}. \qquad \square$$

Example. Let $A = \mathrm{M}_d(k)$, and let $L = k^d$. Let $n \geq 1$, so that $L^n = (k^d)^n$ can be identified with the $d \times n$ matrices over k. Then $A = \mathrm{M}_d(k)$ acts on the left on L^n, and $A^! = \mathrm{M}_n(k)$ acts on the right, and

$$(k^d)^n = (k^n)^d \implies A^{!!} = \mathrm{M}_d(k).$$

Let L be a finite-dimensional vector space over k. Let $A = \mathrm{End}_k(L)$, and let M be a finitely generated A-module (we know $M \cong L^n$ for some n, but we ignore this for now). We have an evaluation map

$$\mathrm{ev} : L \otimes \underbrace{\mathrm{Hom}_A(L, M)}_{L^\diamond} \xrightarrow{\sim} M,$$

and

$$\mathrm{End}_k(L \otimes L^\diamond) = \mathrm{End}(L) \otimes \mathrm{End}(L^\diamond).$$

Then $A = \mathrm{End}(L) \otimes 1$ and $A^! = 1 \otimes \mathrm{End}(L^\diamond)$.

Lecture 22 (2012-11-19)

Now let's prove the theorem we stated last time,

Theorem (Jacobson density)**.** *If M is a semisimple A-module, then A_M is pointwise dense in $A^{!!}_M$; in other words, for any $A^!_M$-linear map $f : M \to M$ and any collection $m_1, \ldots, m_n \in M$, there is an $a \in A$ such that $f(m_1) = am_1$ for all $i = 1, \ldots, n$.*

Proof. Let M be a semisimple A-module, $f : M \to M$ an $A^!_M$-module map, and $m_1, \ldots, m_n \in M$ a collection of elements. We want to find $a \in A$ such that $f(m_i) = am_i$ for all i.

First, consider the case $n = 1$: the submodule $Am \subset M$ has a direct summand $M' \subset M$ such that $M = Am \oplus M'$ since M is semisimple. Let $p : M \to Am$ denote the first projection, which is A-linear and hence $p \in A^!_M$. Therefore f and p commute, so $f(m) = f(p(m)) = p(f(m))$ implies $f(m) \in Am$, i.e., there exists $a \in A$ such that $f(m) = am$.

In the general case, we use a diagonal trick. Consider M^n, which is still a semisimple A-module, and let $x = (m_1, \ldots, m_n) \in M^n$. By the lemma from last lecture, the map $f \mapsto \operatorname{diag}(f, \ldots, f) =: F$ is an isomorphism $A^{!!}_M \xrightarrow{\cong} A^{!!}_{M^n}$. The $n = 1$ case implies there exists $a \in A$ such that $F(x) = ax$. Equivalently, $f(m_i) = am_i$ for all i. □

Corollary 1. *Let M be a semisimple A-module. Assume that M is finitely generated over $A^!_M$. Then $A^{!!}_M = A_M$.*

Proof. Let $M = A^!_M m_1 + \cdots + A^!_M m_n$. Let $f \in A^{!!}_M$. By Jacobson density, there exists $a \in A$ such that $f(m_i) = am_i$ for $i = 1, \ldots, n$. Given $m \in M$ we can write $m = b_1 m_1 + \cdots + b_n m_n$ for $b_i \in A^!_M$. Hence $f(m) = f(\sum b_i m_i) = \sum b_i f(m_i) = \sum b_i a m_i = \sum a b_i m_i = am$. □

Corollary 2. *Let A be an algebra over $k = \bar{k}$. Let M be a simple finite dimensional A-module. Then $\operatorname{act}_M : A \to \operatorname{End}_k(M)$ is surjective.*

Proof. Since M is simple and k is algebraically closed, $A^!_M = k$ by Schur's lemma. Corollary 1 implies $A^{!!}_M = A_M$ but $A^{!!}_M = k^! = \operatorname{End}_k(M)$, so $A_M = \operatorname{End}_k(M)$. □

Theorem (Burnside's theorem)**.** *Let M be a finite-dimensional vector space over an algebraically closed field k. Let $A \subset \operatorname{End}_k(M)$ be a subalgebra such that there is no A-stable subspace in M other than 0 and M itself. Then $A = \operatorname{End}_k(M)$.*

Proof. Corollary 2 implies $\operatorname{act}_M : A \to \operatorname{End}_k(M)$ is surjective, hence it is an isomorphism. □

The Jacobson radical

The following page was included in Homework 8:

1. The Jacobson Radical

Let A be an arbitrary ring. Given a left A-module M, and $m \in M$, define $\mathtt{Ann}_M(m) = \{a \in A \mid a \cdot m = 0\}$. This is a left ideal in A. The map $a \mapsto a \cdot m$ gives a morphism $A \to M$, of left A-modules. Hence, we obtain an A-module embedding $A/\mathtt{Ann}_M(m) \to M$.

We put $\mathtt{Ann}_M = \bigcap_{m \in M} \mathtt{Ann}_M(m)$. Equivalently, $\mathtt{Ann}_M$ is the kernel of the ring homomorphism $A \to \mathrm{End}_{\mathbb{Z}} M,\ a \mapsto \mathrm{act}_M(a)$. Thus, $\mathtt{Ann}_M$ is a two-sided ideal in A.

Let S_A be the set of isomorphism classes of simple A-modules. The following result gives various equivalent definitions of the Jacobson Radical:

Theorem 1. *For any ring A, the following 7 sets are equal:*

- *(1): $\{a \in A \mid \forall x, y \in A,\ 1 + xay$ is invertible$\}$*
- *(2L) $\{a \in A \mid \forall x \in A,\ 1 + xa$ has a left inverse$\}$*
- *(2R) $\{a \in A \mid \forall x \in A,\ 1 + ax$ has a right inverse$\}$*
- *(3L) The intersection of all maximal left ideals in A.*
- *(3R) The intersection of all maximal right ideals in A.*
- *(4L) $\bigcap_{L \in S_A} \mathtt{Ann}_L$*
- *(4R) The intersection of the annihilators of all simple right A-modules.*

The set $J(A)$ defined by these conditions is a two-sided *ideal in A, thanks to (4L)-(4R), called the* Jacobson Radical *of A.*

Proof. We will prove $4L \iff 3L \iff 2L \iff 1$. The corresponding claims for 'R' will follow.

($4L \iff 3L$): Let $\mathcal{M} = \{(M, m) \mid M \in S_A,\ m \in M \smallsetminus \{0\}\}$. Define a map from $\mathcal{M}$ to the set of maximal left ideals by $(M, m) \mapsto \mathtt{Ann}_M(m)$. This map is surjective since simple A-modules are precisely the A-modules of the form A/I for a maximal left ideal I of A. Hence, the intersection of all maximal left ideals of A is equal to

$$\bigcap_{(M,m) \in \mathcal{M}} \mathtt{Ann}_M(m) = \bigcap_{M \in S_A} \bigcap_{m \in M \smallsetminus \{0\}} \mathtt{Ann}_M(m) = \bigcap_{M \in S_A} \mathtt{Ann}_M.$$

We note that the rightmost intersection above is clearly a two-sided ideal.

($3L \iff 2L$): $a \in A$ has no left inverse iff it is contained in a proper left ideal iff it is contained in a maximal left ideal.

Let $\mathcal{L}$ be the set of elements $a \in A$ such that $1 + xa$ has a left inverse for all $x \in A$. Let $a \in \mathcal{L}$ and assume there is a maximal left ideal I not containing a. Then $Aa + I = A \Rightarrow 1 = xa + y$ (for some $x \in A, y \in I$) $\Rightarrow y = 1 + xa$. Since $a \in \mathcal{L}$, then y has a left inverse, which is impossible since it is in I. Therefore, $\mathcal{L} \subseteq I$ for all maximal left ideals I.

Conversely, assume a is in all maximal left ideals, but there is x such that $1 + xa$ has no left inverse. Then $1 + xa$ is in some maximal left ideal I. But xa is also in this ideal, so 1 is in this ideal, a contradiction.

From above, we deduce that the set $\mathcal{L}$ is a two-sided ideal. We will use this in the next step:

($2L \iff 1$): Let $a' \in \mathcal{L}$ and for arbitrary $x, y \in A$ set $a = xa'y$. Then $a \in \mathcal{L}$ since $\mathcal{L}$ is a two-sided ideal. Hence, $1 + a$ has a left inverse b, so $b(1 + a) = 1 \Rightarrow b = 1 - ba$. Since $a \in \mathcal{L}$, then b has a left inverse c, so that $cb = 1$. But $c = c \cdot 1 = c(b(1+a)) = cb(1+a) = 1+a$. Thus $(1+a)b = 1$, so $1 + a$ has a two-sided inverse, whence $(2L) \Rightarrow (1)$. The reverse inclusion is clear. □

Lemma 2 (Nakayama lemma). *Let M be a finitely-generated A-module such that $J(A) \cdot M = M$. Then $M = 0$.*

Proof. Find a minimal generating set $m_1, \ldots, m_n$. Then we have $M = J(A) \cdot M = \sum J(A) m_i$. Then we may write $m_n = j_1 m_1 + \ldots + j_{n-1} m_{n-1} + j_n m_n$ for $j_i \in J(A)$. But then we have $(1 - j_n) m_n = j_1 m_1 + \ldots + j_{n-1} m_{n-1}$. Since $j_n \in J(A)$, then $1 - j_n$ is invertible, so that m_n is actually in the span of $\{m_i \mid i < n\}$, so we have a smaller generating set, a contradiction. □

Lemma. $J(A/J(A)) = 0$.

Proof. Simple A-modules are also simple $A/J(A)$-modules, so we are done by definition (4L). $\square$

Definition. Given a left/right/2-sided ideal $I \subset A$,

1. we say I is nil if any $a \in I$ is nilpotent, and
2. we say I is nilpotent if there exists n such that $I^n = 0$, which is equivalent to requiring $a_1 \cdots a_n = 0$ for all $a_1, \ldots, a_n \in I$.

Lemma.

1. *If I, J are nilpotent, then $I + J$ is also nilpotent.*
2. *Any nil ideal is contained in $J(A)$.*

Proof of 1. Suppose $I^m = 0$ and $J^n = 0$. We claim that $(I+J)^{m+n} = 0$. We can see this as follows: if we take $a_1, \ldots, a_{m+n} \in I \cup J$, then there will be either $\geq m$ elements $a_i \in I$ or $\geq n$ elements in J. Assume WLOG that $a_{i_1}, \ldots, a_{i_m} \in I$. Then $a_1 \cdots a_{m+n} = (\cdots a_{i_1})(\cdots a_{i_2}) \cdots (\cdots a_{i_m}) \cdots a_{m+n} = 0$ since I is an ideal. $\square$

Proof of 2. If I is a left nil ideal, then $a \in I$ implies that $xa \in I$ for all $x \in A$. Hence xa is nilpotent, so $1 + xa$ is invertible. Therefore by (2L) $a \in J(A)$. $\square$

Lecture 23 (2012-11-21)

Theorem. *Let A be a finite-dimensional algebra over k. Then*

1. *$J(A)$ is the maximal nilpotent ideal of A, i.e., $J(A)$ is a nilpotent ideal and it contains any other nilpotent ideal.*
2. *$A/J(A)$ is a semisimple algebra.*
3. *A has only finitely many maximal two-sided ideals.*
4. *$J(A) = \bigcap$ maximal two-sided ideals.*

Proof of 1. Let $J := J(A)$. We have a decreasing chain of two-sided ideals $A \supset J \supset J^2 \supset J^3 \supset \cdots$, which must stabilize since A is finite-dimensional (hence Artinian). Therefore there exists $N \gg 0$ such that $J^{N+1} = J^N$. Since J^N is a finitely generated A-module, Nakayama's lemma implies that $J^N = 0$, so J is nilpotent. □

Proof of 2. $J(A/J(A)) = 0$ so by Problem 6 of Homework 8, we know $A/J(A)$ is semisimple. □

Proof of 3. Wedderburn's theorem implies that $A/J(A) = A_1 \oplus \cdots \oplus A_n$ where $A_i = \mathrm{M}_{r_i}(D_i)$ is a simple algebra. Any two-sided ideal $I \subset \bigoplus A_i$ has the form $I = I_1 \oplus \cdots \oplus I_n$ where I_n is a two-sided ideal in A_i. The maximal ideals in $A/J(A)$ are $A_1 \oplus \cdots \oplus A_{i-1} \oplus 0 \oplus A_{i+1} \oplus \cdots \oplus A_n$.

We claim that if $\mathfrak{a}$ is a maximal two-sided ideal in A, then $J(A) \subset \mathfrak{a}$. If this were not the case, then $J(A) + \mathfrak{a} = A$. Hence $1 = j + a$ for some $j \in J(A), a \in \mathfrak{a}$. But then $a = 1 - j$ is invertible, a contradiction.

In general, we have a bijection

$$\{\text{maximal two-sided ideals of } A \text{ containing } J(A)\} \longleftrightarrow \{\text{maximal two-sided ideals of } A/J(A)\}.$$

Thus, the number of maximal two-sided ideals is finite. □

Proof of 4. This is clear from our description of maximal ideals in $A/J(A)$ from part 3. □

Remark. Let A be a ring, $J \subset A$ a two-sided ideal, and M a left (resp. right) A-module. Then $M/JM = (A/J) \otimes_A M$ (resp. $M/MJ = M \otimes_A (A/J)$) is a left (resp. right) (A/J)-module.

Theorem. *Let A be a finite-dimensional algebra over an algberaically closed field k. Let $J = J(A)$, and define $\bar{A} := A/J$. Then $A \cong (T_{\bar{A}}(J/J^2))/I$ where I is a two-sided ideal in the tensor algebra satisfying*

$$T^{\geq 2}(J/J^2) \supseteq I \supseteq T^{\geq N}(J/J^2)$$

for sufficiently large N.

Corollary. *Let A be finite-dimensional over an algebraically closed field k such that*

$$\bar{A} = A/J(A) = \underbrace{k \oplus \cdots \oplus k}_{n \text{ times}}.$$

Then there exists a finite quiver Q with vertex set $\{1, \ldots, n\}$ such that $A = kQ/I$ with $(kQ)_{\geq 2} \supseteq I \supseteq (kQ)_{\geq N}$ for some sufficiently large N.

Proof. By the remark, $E := J/J^2$ is an A/J-bimodule. Since A/J is a direct sum of fields, we have a decomposition $E = \bigoplus E_{ij}$. Define the quiver Q so that E corresponds to the paths. □

Proof of Theorem 2. The proof proceeds in several steps.

Step 1: We claim that there exists a section $\varepsilon : \bar{A} \to A$, i.e. that there exists a subalgebra $A' \subset A$ such that $A' \hookrightarrow A \to \bar{A}$ is an isomorphism.

> **Lemma** (Lifting of idempotents)**.** *If $J \subset A$ is a nilpotent two-sided ideal, let $\bar{e}_1, \dots, \bar{e}_n$ be a collection of orthogonal idempotents, i.e., $\bar{e}_i \cdot \bar{e}_j = \delta_{ij}\bar{e}_i$. Then there exist orthogonal idempotents $e_i \in A$ such that $e_i \bmod J = \bar{e}_i$ for all $i = 1, \dots, n$.*

The above is Corollary 7.5 of Etingof's *Introduction to representation theory* and we omit the proof.

Since $\bar{A}$ is semisimple over an algebraically closed field, it is a direct sum of matrix algebras $\bigoplus_\ell \mathrm{M}_{n_\ell}(k)$. Let $\bar{e}_{\ell,ij}$ denote the matrix with a 1 in the (i,j) position as an element of $\mathrm{M}_{n_\ell}(k)$. Then $\{\bar{e}_{\ell,ii}\}$ forms a collection of orthogonal idempotents in $\bar{A}$, so by the lemma we can lift them to orthogonal idempotents in $e_{\ell,ii} \in A$. Since $\sum_{\ell,i} e_{\ell,ii} \in 1 + J$ is idempotent and invertible, it is 1. Let $e_\ell = \sum_i e_{\ell,ii}$. Then $e_\ell A e_\ell$ are orthogonal subalgebras of A for distinct ℓ. Hence it suffices to lift each $\mathrm{M}_{n_\ell}(k)$ to $e_\ell A e_\ell$. We therefore drop the ℓ subscript and assume $\sum e_{ii} = 1$.

Suppose that for I a two-sided square-zero ideal of A, we can lift a matrix subalgebra of A/I to A. Then applying this to the sequence $A = A/J^N \to A/J^{N-1} \to \cdots \to A/J = \bar{A}$ with $I = J^i/J^{i+1} \subset A/J^{i+1}$, we are done. To prove the square-zero case, i.e., $\bar{A} = A/I$ and $I^2 = 0$: first take an arbitrary lift $e_{i,i+1} \in A$ of $\bar{e}_{i,i+1} \in \bar{A}$. By multiplying on the left by $1 - e_{jj}$ for $j \neq i$ and on the right by $1 - e_{jj}$ for $j \neq i+1$, we get $e_{jj}e_{i,i+1} = \delta_{ij}$ and $e_{i,i+1}e_{jj} = \delta_{i+1,j}$. Do the same for $e_{i+1,i}$. Then $e_{i,i+1}e_{i+1,i} - e_{ii} \in I$ implies

$$(e_{i,i+1}e_{i+1,i} - e_{ii})^2 = e_{i,i+1}(r - e_{i+1,i}) + e_{ii} = 0$$

where $r = e_{i+1,i}e_{i,i+1}e_{i+1,i} - e_{i+1,i} \in I$. Thus $e_{i,i+1}(e_{i+1,i} - r) = e_{ii}$. The analogous computation shows that $(e_{i+1,i} - r)e_{i,i+1} = e_{i+1,i+1}$. Replacing $e_{i+1,i}$ with $e_{i+1,i} - r$, we can assume that

$$e_{i+1,i}e_{i,i+1} = e_{i+1,i+1}, \quad e_{i,i+1}e_{i+1,i} = e_{ii}.$$

Now set $e_{ij} = e_{i,i+1}e_{i+1,i+2} \cdots e_{j-1,j}$ and $e_{ji} = e_{j,j-1} \cdots e_{i+1,i}$ for $i < j$. One sees that the span of $\{e_{ij}\}$ is isomorphic to $\mathrm{M}_n(k)$ as algebras.

Step 2: The projection $J \to J/J^2$ is an $\bar{A}$-bimodule map, where $\bar{A}$ acts on J via ε. We want to show that there exists an $\bar{A}$-bimodule section $J/J^2 \to J$.

Let $M = J/J^2$. Keeping the notation from Step 1, it suffices to lift $e_\ell M e_m$ to $e_\ell J e_m$. Note that an $(\mathrm{M}_{n_\ell}(k), \mathrm{M}_{n_m}(k))$-bimodule is the same as an $\mathrm{M}_{n_\ell}(k) \otimes \mathrm{M}_{n_m}(k)^{\mathrm{op}} \cong \mathrm{M}_{n_\ell}(k) \otimes \mathrm{M}_{n_m}(k) \cong \mathrm{M}_{n_\ell n_m}(k)$-module. Any such module is a direct sum of the simple module $k^{n_\ell n_m}$. Decompose M into a direct sum of simple modules and lift one vector from each summand. The $\bar{A} \otimes \bar{A}^{\mathrm{op}}$-span of these lifts gives the desired section.

Step 3: Let $f : \widetilde{A} \to A$ be an algebra homomorphism. Let $\widetilde{J} \subset \widetilde{A}$ and $J \subset A$ be two-sided nilpotent ideals such that (i) $f(\widetilde{J}) \subset J$, (ii) $\widetilde{A}/\widetilde{J} \to A/J$ is surjective, and (iii) $\widetilde{J}/\widetilde{J}^2 \to J/J^2$ is surjective. Then f is surjective.

This claim just follows by induction (think J-adic completion).

Finishing the proof: Steps 1 and 2 give maps $\varepsilon : \bar{A} \to A$ and $J/J^2 \hookrightarrow J \hookrightarrow A$. The universal property of tensor algebras[6] gives an algebra map $f : T := T_{\bar{A}}(J/J^2) \to A$. Then $f(T^{\geq 1}) \subset J$ implies $f(T^{\geq i}) \subset J^i$ for all $i \geq 1$. In particular, since $J^N = 0$ for some N, we get $f(T^{\geq N}) \subset J^N = 0$. Hence $T^{\geq N} \subset \ker(f) =: I$. On the other hand, our construction of f gives a commutative diagram

$$\begin{tikzcd}
T/T^{\geq 2} \arrow[r, "f"] \arrow[d, "\cong"'] & A/J^2 \arrow[r, equal] & (\bar{A} \oplus J)/J^2 \arrow[d, "\cong"] \\
\bar{A} \oplus (J/J^2) \arrow[rr, "\mathrm{id}"'] & & \bar{A} \oplus (J/J^2)
\end{tikzcd}$$

which shows that if $a \in I$, then $f(a \bmod T^{\geq 2}) = 0$ implies $a \bmod T^{\geq 2} = 0$, i.e. that $a \in T^{\geq 2}$. Hence $I \subset T^{\geq 2}$.

Lastly, apply Step 3 to $\widetilde{A} = T$ and $\widetilde{J} = T^{\geq 1}$ to conclude the theorem. $\square$

[6]The universal property says that if $\bar{A} \to A$ is an algebra homomorphism, M an $\bar{A}$-bimodule, and $f : M \to A$ an $\bar{A}$-bimodule map, then there exists a unique algebra map $T_{\bar{A}}M \to A$ extending f.

Lecture 24 (2012-11-26)

Today, we'll discuss a trick that will let us extend some of our results about finite-dimensional algebras to some infinite-dimensional algebras.

Definition. An algebra is said to be "nice" (this isn't standard terminology) if it is a $\mathbb{C}$-algebra of at most countable dimension over $\mathbb{C}$.

Clearly, a subalgebra or a quotient of a nice algebra is nice, and any finitely generated $\mathbb{C}$-algebra is nice because it is a quotient of some $\mathbb{C}\langle x_1, \ldots, x_n\rangle$, which has a countable basis.

Recall that for an algebra A and $a \in A$, we defined $\operatorname{spec}(a) = \{\lambda \in \mathbb{C} \mid a - \lambda \text{ is not invertible}\}$.

Theorem (Spectral theorem)**.** *Let A be a nice algebra, and let $a \in A$. Then*

1. *a is nilpotent* $\iff \operatorname{spec}(a) = \{0\}$.
2. *a is algebraic* $\iff \operatorname{spec}(a)$ *is a non-empty finite set.*
3. *a is non-alegbraic* $\iff \mathbb{C} \setminus \operatorname{spec}(a)$ *is at most countable.*

Let $\mathbb{C}(t)$ be the field of rational functions in t.

Lemma. *Let $\lambda_1, \ldots, \lambda_n \in \mathbb{C}$ be distinct. If $\sum \frac{c_i}{t-\lambda_i} = 0$ in $\mathbb{C}(t)$, then all of the c_i are 0.*

Proof of lemma. Clearing denominators, we get that $\frac{f(t)}{\prod(t-\lambda_i)} = 0$ for some $f(t) \in \mathbb{C}[t]$, hence $f(t) = 0$. But for any i, the fact that $f(\lambda_i) = 0$ implies that $c_i = 0$. □

Proof of theorem. Given an $a \in A$, define

$$R_a = \{\tfrac{f}{g} \in \mathbb{C}(t) \mid f, g \text{ are coprime, and } g \text{ is non-zero on } \operatorname{spec}(a)\}.$$

Thus, for any $g_1, \ldots, g_n \in \mathbb{C} \setminus \operatorname{spec}(a)$, we have $\frac{1}{g} \in R_a$ where

$$g(t) = (t - g_1) \cdots (t - g_n) \in R_a$$

and any denominator has this form. Note that R_a is a subring of $\mathbb{C}(t)$. Now, we can define an evaluation map $j_a : R_a \to A$ by

$$\frac{f}{g} \mapsto f(a) \cdot g(a)^{-1} = f(a)(a - g_1)^{-1} \cdots (a - g_n)^{-1}.$$

Observe that if a is not algebraic, then for any $\frac{f}{g} \in R_a$, if $j_a(\frac{f}{g}) = 0$, we have $f(a)g(a)^{-1} = 0$, hence $f(a) = 0$, hence $f = 0$ because a is not algebraic. Thus, j_a is injective when a is not algebraic.

Our lemma demonstrates that $\{\frac{1}{t-\lambda} \mid \lambda \in \mathbb{C} \setminus \operatorname{spec}(a)\}$ is a $\mathbb{C}$-linearly independent subset of R_a, and our observation above implies that $\{(a - \lambda)^{-1} \mid \lambda \in \mathbb{C} \setminus \operatorname{spec}(a)\}$ is linearly independent (when a is not algebraic). Because $\dim_{\mathbb{C}}(A) \le$ countable, we must have that $|\mathbb{C} \setminus \operatorname{spec}(a)| \le$ countable.

We also know that if a is algebraic, then $\operatorname{spec}(a) = \{\text{roots of the minimal polynomial of } a\}$, which must be a finite set, and which is non-empty because $\mathbb{C}$ is algebraically closed.

It is impossible to have $\operatorname{spec}(a)$ be finite and $\mathbb{C} \setminus \operatorname{spec}(a)$ to be at most countable at the same time, so parts 2 and 3 follow.

Now we will prove part 1. We clearly know that a is nilpotent $\iff$ a is algebraic and $\operatorname{spec}(a) = \{0\}$, but we want to drop the assumption that a is algebraic. We can do this because $\operatorname{spec}(a) = \{0\}$ implies that $\operatorname{spec}(a)$ is finite, hence a is algebraic by part 2. □

Corollary. *If A is nice and $a \in A$, then* $\operatorname{spec}(a)$ *is non-empty.*

Proof. Obviously, a is either algebraic or not algebraic; apply the theorem. $\square$

Corollary. *If A is a nice division algebra, then $A = \mathbb{C}$.*

Proof. Let $a \in A \setminus \mathbb{C}$, so that $a - \lambda \neq 0$ for all $\lambda \in \mathbb{C}$. Because A is a division algebra, this implies that $a - \lambda$ is invertible for all $\lambda \in \mathbb{C}$, hence $\operatorname{spec}(a) = \varnothing$, which is a contradiction. $\square$

Theorem (Schur lemma for nice algberas)**.** *If A is a nice algebra and M is a simple A-module, then* $\operatorname{End}_A(M) = \mathbb{C}$.

Proof. Pick a non-zero $m \in M$. We have a diagram

$$A \xrightarrow[\ell]{a \mapsto am} M \xleftarrow[i]{f(m) \leftarrow\!\shortmid f} \operatorname{End}_A(M)$$

but because M is simple, ℓ is surjective. Again because M is simple, if $f(m) = 0$ then $f(A \cdot m) = 0$, hence $f = 0$, so that i is injective.

The fact that A is nice then implies that $\operatorname{End}_A(M)$ is nice, hence $\operatorname{End}_A(M)$ is a nice division algebra, hence $\operatorname{End}_A(M) = \mathbb{C}$. $\square$

Proposition. *Let A be a nice algebra. Then $J(A)$ is the unique maximal nil-ideal.*

Remark. We know that if A is finite-dimensional, then $J(A)$ is nilpotent.

Proof. If $a \in J(A)$, then $1 - xa$ is invertible for all $x \in A$, so $1 - \lambda a$ is invertible for all $\lambda \in \mathbb{C}$. Therefore, $a - \lambda$ is invertible for all $\lambda \neq 0$, so we must have $\operatorname{spec}(a) \subseteq \{0\}$. By the spectral theorem, a is nilpotent. Thus, $J(A)$ is a nil-ideal. But we have proved in a previous class that any nil-ideal is contained in $J(A)$; this implies the claim. $\square$

Theorem. *Let A be a nice algebra with trivial Jacobson radical, i.e. $J(A) = 0$. The action map $A \to \prod_{M \in S_A} \operatorname{End}_{\mathbb{C}}(M)$ is an embedding of A as a pointwise dense subalgebra, i.e. for any finite subset $S \subset S_A$, any $m_1, \ldots, m_n \in \bigoplus_{M \in S} M$, and any $f \in \bigoplus_{M \in S} \operatorname{End}_{\mathbb{C}}(M)$, there is some $a \in A$ such that $f(m_i) = am_i$ for all $i = 1, \ldots, n$.*

Proof. Because

$$J(A) = \bigcap_{M \in S_A} \operatorname{Ann}(M) = 0,$$

we have that the action map j is injective. Because M is simple, $A^!_M = \operatorname{End}_A(M) = \mathbb{C}$, and thus $A^{!!}_M = \operatorname{End}_{\mathbb{C}}(M)$. Now the result follows from the Jacobson density theorem. $\square$

Commutative case

Theorem. *Let A be a nice commutative algebra. Then $J(A) = \{$nilpotent $a \in A\}$. Given an algebra homomorphism $\chi : A \to \mathbb{C}$, let $\mathbb{C}_\chi$ be $\mathbb{C}$ considered as an A-module via χ. Then the natural maps*

$$\{\text{algebra homomorphisms } A \to \mathbb{C}\} \xrightarrow{\chi \mapsto \mathbb{C}_\chi} S_A \xrightarrow{M \mapsto \operatorname{Ann}(M)} \{\text{maximal ideals in } A\}$$

are bijections.

Proof. If $a \in A$ is nilpotent, then Aa is a nil ideal, so that $Aa \subseteq J(A)$. Conversely, any $a \in J(A)$ is nilpotent by our proposition.

Let $M \in S_A$ be a simple A-module. Since A is commutative, $A_M \subset A^!_M$ (A obviously commutes with itself). Because M is simple, we have $A^!_M = \mathbb{C}$ by Schur's lemma, so that $A_M = \mathbb{C}$, hence $\dim_{\mathbb{C}}(M) = 1$, hence there is some χ such that $am = \chi(a)m$.

Next we need to show that any maximal ideal I in a commutative algebra A is the annihilator of a simple module. Take $M = A/I$ so that $\mathrm{Ann}(M) = I$. Then I is a maximal left ideal iff M is simple. $\square$

Lecture 25 (2012-11-28)

Recall that A is a nice commutative algebra. Let $\widehat{A}$ be the collection of algebra homomorphisms from A into $\mathbb{C}$. We already showed that $\widehat{A} \cong S_A$ given by $\chi \mapsto \mathbb{C}_\chi$. Let $\mathrm{Nil}(A)$ be the collection of nilpotent elements of A. Let $\mathrm{ev} : A \to \mathbb{C}\{\widehat{A}\}$ be the evaluation algebra homomorphism $\mathrm{ev}(a)(\chi) = \chi(a)$. We will also denote $\widehat{a} = \mathrm{ev}(a)$.

Theorem. *Let A be a nice commutative algebra. Then*

1. $\ker(\mathrm{ev}) = \mathrm{Nil}(A)$.
2. $\mathrm{im}(\mathrm{ev})$ *is pointwise dense.*
3. *For $a \in A$,* $\mathrm{spec}(a)$ *is the set of values of $\widehat{a}$.*

Proof. We know parts 1 and 2, but not 3 yet. This holds if and only if $\mathrm{spec}(a) = \{\chi(a) \mid \chi \in \widehat{A}\}$. For any $\lambda \in \mathbb{C}$, $\lambda \in \mathrm{spec}(a)$ if and only if $a - \lambda$ is not invertible, which is the case if and only if $A(a-\lambda)$ is contained in a maximal ideal (by Zorn's lemma), which we know is the kernel of some χ. Thus, $a - \lambda \in A(a-\lambda) \subseteq \ker(\chi)$ if and only if $0 = \chi(a-\lambda)$, if and only if $\lambda = \chi(a)$. □

Theorem (Hilbert's Nullstellensatz)**.** *Let A be a finitely generated commutative $\mathbb{C}$-algebra. Let $I \subseteq A$ be an ideal; then $a \in \bigcap\{$maximal ideals of A containing $I\}$ if and only if $a^n \in I$ for some sufficiently large n.*

Proof. $a \bmod I$ is contained in the intersection of maximal ideals in A/I if and only if it lies in $\mathrm{Nil}(A/I)$, i.e. a^n is eventually in I. □

Corollary. *Let $A = \mathbb{C}[x_1, ..., x_n]$. Let $V(I) = \{c \in \mathbb{C}^n \mid p(c) = 0$ for all $p \in I\}$. Then $f|_{V(I)} = 0$ if and only if $f^n \in I$ for some n.*

Proof. $f|_{V(I)} = 0$ if and only if $\mathrm{ev}_c(f) = 0$ for all $c \in V(I)$. The latter condition is equivalent to saying that $f \in \bigcap_{\{c|\ker(\mathrm{ev}_c)\supset I\}} \ker(\mathrm{ev}_c) = \bigcap\{$maximal ideals in A containing $I\}$, which the theorem shows is the case if and only if $f^n \in I$ for some n. □

Topological Versions of These Results

Definition. Let A be a $\mathbb{C}$-algebra. A norm on A is a function $|\cdot| : A \to \mathbb{R}_{\geq 0}$ such that

1. $|a| = 0$ if and only if $a = 0$.
2. $|\lambda a| = |\lambda| \cdot |a|$ for all $\lambda \in \mathbb{C}$.
3. $|a + b| \leq |a| + |b|$.
4. $|ab| \leq |a||b|$.

Examples.

1. $C(X)$ where X is a compact topological space and $|f| = \|f\|_\infty = \max_{x\in X}|f(x)|$.
2. $A = \mathrm{End}_{\mathbb{C}}(V)$ where $|a| = \sup_{|v|=1} |av|$.

A *Banach algebra* is an algebra A with norm $|\cdot|$ which is complete as a metric space.

Lemma. *Let A be a Banach algebra. Fix an element $a \in A$. Then*

1. $\mathrm{spec}(a)$ *is a closed subset of the disk of radius* $|a|$.
2. *The function* $f : \mathbb{C} \setminus \mathrm{spec}(a) \to A$ *given by* $z \mapsto (a-z)^{-1}$ *is a holomorphic function.*
3. $|(a-z)^{-1}| \to 0$ *as* $|z| \to \infty$.

Proof. The idea is just to factor a out of the resolvent to get $a^{-1}(1-a^{-1}z)^{-1} = \frac{1}{a}\sum_k (a^{-1}z)^k$, which is absolutely continuous, hence convergent in the Banach algebra. Therefore, it is continuous and one can differentiate termwise. This lemma is Homework 9, Problem 7. □

Theorem (Gelfand)**.** *For any Banach algebra A and $a \in A$,* $\mathrm{spec}(a) \neq \varnothing$.

Proof. Suppose that $\mathrm{spec}(a) = \varnothing$; then $z \mapsto (a-z)^{-1}$ is a holomorphic function $\mathbb{C} \to A$. It is also bounded by (3). By Liouville, this must be constant, which is a contradiction. □

Remark. All of our results on nice algebras in Lecture 24 only relied on the fact that A nice implies $\mathrm{spec}(a) \neq \varnothing$ (in particular, so we get Schur's Lemma). Thus all of those results also hold for Banach algebras by Gelfand's theorem.

Now equip $\widehat{A}$ with the topology of pointwise convergence. This is called the *Gelfand representation.*

Theorem. *Let A be a commutative Banach algebra.*

1. *For all $a \in A$, $\widehat{a} = \mathrm{ev}(a)$ is a continuous function on $\widehat{A}$ and* $\sup_{\chi \in \widehat{A}} |\widehat{a}(\chi)| \leq |a|$.
2. $\widehat{A}$ *is compact and* $\mathrm{ev} : A \to C(\widehat{A})$ *is a weak contraction.*
3. $\ker(\mathrm{ev})$ *is the set of elements that are topologically nilpotent, i.e.* $\limsup |a^n|^{1/n} \to 0$.

Proof. (1) The topology of pointwise convergence is (by definition) the weakest topology such that $\widehat{a}$ is continuous for all $a \in A$. By Gelfand's theorem, $\mathrm{spec}(a)$ is a nonempty compact set contained in the disk of radius $|a|$ and is equal to $\mathrm{ev}_a(\widehat{A})$ by the remark.

(3) The kernel of the evaluation map is exactly $\{a \in A | \chi(a) = 0 \text{ for all } \chi \in \widehat{A}\}$, which happens if and only if $\mathrm{spec}(a) = \{0\}$, which is equivalent to $\limsup |a^n|^{1/n} = \max\{|z|, z \in \mathrm{spec}(a)\} = 0$ by Homework 9, Problem 7.

(2) Let D be the unit disk in $\mathbb{C}$ and let D_A be the unit disk in A. For every $\chi \in \widehat{A}$, χ maps D_A to D by part (1). Therefore χ is a weak contraction, hence continuous; and $\widehat{A}$ is a pointwise closed subset in $\mathrm{Maps}(D_A, D) = D^{D_A}$, which is a compact set by Tychonoff (pointwise convergence topology is exactly the product topology). Therefore, $\widehat{A}$ is compact and the map is a weak contraction. □

Lecture 26 (2012-11-30)

Last time, we discussed Banach algebras, and now we'll add a new piece of structure to them.

Definition. A $*$-algebra is a Banach algebra A equipped with an anti-involution $*$, sending a to a^*, such that $(ab)^* = b^* a^*$, $(a^*)^* = a$, $(\lambda a)^* = \overline{\lambda} a^*$, and $|a^*| = |a|$ for all $a, b \in A$ and $\lambda \in \mathbb{C}$.

Examples.

- Let X be a compact Hausdorff space, and let $A = C(X)$, with norm $|f| = \max_{x \in X} |f(x)|$. Then the map $f \mapsto f^*$ defined by $f^*(x) = \overline{f(x)}$ makes A a $*$-algebra.
- Let V be a finite-dimensional hermitian vector space, and let $A = \mathrm{End}(V)$, with norm $|a| = \max_{v \in V \setminus \{0\}} \frac{|a(v)|}{|v|}$. Then the map $a \mapsto a^*$ (the hermitian adjoint) makes A a $*$-algebra.

Remark. Let $\widehat{A} = \mathrm{Hom}_{\mathrm{alg}}(A, \mathbb{C})$, which is a compact Hausdorff space. There is a natural evaluation map $\mathrm{ev} : A \to C(\widehat{A})$. If $A = C(X)$, then $\widehat{A} = X$, using our identification of the points of X with maximal ideals. Specifically, the map

$$\mathrm{ev} : C(X) \to C(\widehat{C(X)}) = C(X)$$

is the identity.

Theorem. *Let A be a* ***commutative*** *$*$-algebra. Then*

1. *The evaluation map $\mathrm{ev} : A \to C(\widehat{A})$ commutes with anti-involution, i.e. for all $\chi \in \widehat{A}$,*
$$\overline{\mathrm{ev}(a)(\chi)} = \mathrm{ev}(a^*)(\chi).$$
2. $\mathrm{im}(\mathrm{ev})$ *is dense in* $C(\widehat{A})$.

Proof. First, we'll show that 1 implies 2. We use the Stone-Weierstrass theorem:

> **Theorem** (Stone-Weierstrass)**.** *Let X be a compact Hausdorff space, and let $B \subset C(X)$ be a subalgebra that separates points, and that is stable under the involution of complex conjugation. Then B is dense (with respect to the uniform convergence norm) in $C(X)$.*

In our setting, statement 1 implies that $\mathrm{im}(\mathrm{ev})$ is stable under conjugation, and $\mathrm{im}(\mathrm{ev})$ separates points essentially by definition. Thus, statement 2 follows from statement 1.

Now we will prove statement 1. First, we will need the following fact: if $u \in A$ is invertible, then $\lambda \in \mathrm{spec}(u) \iff \lambda^{-1} \in \mathrm{spec}(u^{-1})$. This is clear: $u - \lambda$ is invertible $\iff$ $u^{-1} - \lambda^{-1}$ is invertible.

Recall that for a Banach algebra A, we can define $\exp : A \to A$ by

$$\exp(a) = 1 + a + \frac{a^2}{2} + \cdots,$$

and the fact that $|a^n| \leq |a|^n$ ensures that this is absolutely convergent. We claim that $\lambda \in \mathrm{spec}(a) \implies e^\lambda \in \mathrm{spec}(\exp(a))$. This follows from the fact that

$$\frac{\exp(a) - e^\lambda}{a - \lambda} = 1 + \cdots$$

as a formal power series absolutely convergent in a (take the Taylor series of the holomorphic function $\frac{e^z - e^\lambda}{z - \lambda}$). Therefore if $\exp(a) - e^\lambda$ is invertible, we can define $(a - \lambda)^{-1}$.

Let A be a $*$-algebra. We say that a is hermitian (respectively, skew-hermitian) if $a^* = a$ (respectively, if $a^* = -a$). We say that u is unitary if $u^*u = uu^* = 1$. Clearly a is hermitian $\iff$ $\sqrt{-1}\,a$ is skew-hermitian. Let $H(A)$ be the set of hermitian elements of A (which is a sub-$\mathbb{R}$-vector space of A), and let $U(A)$ be the set of unitary elements (which is a subgroup of $A^\times$). It is easy to see that $u \in U(A)$ implies $|u| = 1$. Observe that

$$A = H(A) \oplus \sqrt{-1}\,H(A),$$

and specifically, for $a \in A$, we have $a = x + iy$ where $x = \frac{a+a^*}{2}, y = \frac{a-a^*}{2i} \in H(A)$.

We claim that $a \in H(A) \iff \exp(ita) \in U(A)$ for any $t \in \mathbb{R}$. This holds because

$$(e^{ita})^* = 1^* + (ita)^* + (i^2t^2a^2/2)^* + \cdots = e^{-ita},$$

proving the $\implies$ direction, and the $\impliedby$ direction follows from considering the derivative

$$a = \frac{1}{i}\left(\frac{d}{dt}\,e^{ita}\right)\bigg|_{t=0}.$$

Because $|u| = 1$ for any $u \in U(A)$, for any $\lambda \in \operatorname{spec}(u)$ we have $|\lambda| \le |u| = 1$. But $u^* = u^{-1}$ is also unitary, so for any $\lambda^{-1} \in \operatorname{spec}(u^{-1})$, we have $|\lambda^{-1}| \le |u^{-1}| = 1$. Therefore $|\lambda| = 1$, so that $\operatorname{spec}(u) \subseteq \mathbb{S}^1 \subset \mathbb{C}$ for any unitary u.

Now, we observe that for any $a \in H(A)$, we have $\operatorname{spec}(a) \subseteq \mathbb{R}$. We can see this as follows. For any $t \in \mathbb{R}$, we know that $e^{ita} \in U(A)$, and therefore for any $\mu \in \operatorname{spec}(e^{ita})$, we must have $|\mu| = 1$. But $\lambda \in \operatorname{spec}(a)$ implies that $e^{it\lambda} \in \operatorname{spec}(e^{ita})$, so that $|e^{it\lambda}| = 1$, and therefore $\lambda \in \mathbb{R}$.

We claim that for any $\chi : A \to \mathbb{C}$ in $\widehat{A}$, we have $\chi(a^*) = \overline{\chi(a)}$ for any $a \in A$. We write $a = x + iy$ where $x, y \in H(A)$, and recall that we proved last time $\operatorname{spec}(b) = \{\chi(b) \mid \chi \in \widehat{A}\}$ (this is where we need commutativity of A). Then $\chi(x) \in \operatorname{spec}(x) \subset \mathbb{R}$, $\chi(y) \in \operatorname{spec}(y) \subset \mathbb{R}$, and

$$\chi(a) = \chi(x + iy) = \chi(x) + i\chi(y)$$

implies that

$$\chi(a^*) = \chi(x - iy) = \chi(x) - i\chi(y) = \overline{\chi(x) + i\chi(y)}.$$

Thus, we have proven statement 1 in our theorem. $\square$

Note that if $a \in H(A)$, then $|\operatorname{ev}(a)| = \limsup |a^n|^{\frac{1}{n}} = |a|$ since $|a^2| = |a|^2$. For general $a \in A$, we have using part (1) of the Theorem that $|\operatorname{ev}(a)|^2 = |\operatorname{ev}(a^*a)| = |a^*a| = |a|^2$. It follows that ev is an isometry.

Example. Let G be a locally compact group, and $\int$ be a left invariant integral. We can consider $L^1(G)$, which is the closure of the space of continuous functions with compact support. We claim that $L^1(G)$ together with the convolution product

$$(f_1 \star f_2)(g) = \int f_1(h) f_2(h^{-1}g)\,dh$$

(we can't use $*$ for convolution, it'd be too confusing) and the anti-involution $f^*(g) = \overline{f(g^{-1})}$ makes $L^1(G)$ into a $*$-algebra.

Suppose that G is abelian. Then $L^1(G)$ is commutative under $\star$, so all of our previous work applies (sort of). We can consider the evaluation map $\operatorname{ev} : L^1(G) \to C(\widehat{L^1(G)})$. We first suggest that

$\widehat{L^1(G)} = \widehat{G}$. Here $\widehat{G}$ denotes the Pontryagin dual of G, i.e. the continuous group homomorphisms $G \to \mathbb{S}^1$. We can see that there may be an issue because the Gelfand representations we have considered are always compact[7], while $\widehat{G}$ may only be locally compact in general. The issue arises because $L^1(G)$ is not quite a [unital] algebra, since it need not have a unit (the unit under convolution is not the function 1, but rather the Dirac delta, which is not in L^1 unless G is discrete, that is, unless $\widehat{G}$ is compact). We fix this by formally adjoining a unit (even if there was one already in it) by defining

$$L^1(G)^{\sim} = \mathbb{C}1 \oplus L^1(G)$$

such that $L^1(G)$ is an ideal in $L^1(G)^{\sim}$ and $|c \oplus a| = |c| + |a|$. This makes $L^1(G)^{\sim}$ a unital Banach $*$-algebra.

Proposition. *The Fourier transform defines a group homeomorphism*

$$\widehat{G} \cup \{\infty\} \cong \widehat{L^1(G)^{\sim}}$$

where the LHS is a one-point compactification of $\widehat{G}$.

Proof. Let $\zeta : L^1(G)^{\sim} \to \mathbb{C}$ be an algebra homomorphism. We proved that ev is an isometry, so ζ restricted to $L^1(G)$ is a bounded linear functional with $\|\zeta\|_1 = 1$. The dual of $L^1(G)$ is $L^\infty(G)$ so ζ may be considered as an almost everywhere bounded function on G. Pick $f \in L^1(G)$ such that $\zeta(f) = \int_G \zeta(h)f(h)dh \neq 0$. Then define $\chi(g) = \frac{\int \zeta(gh)f(h)dh}{\int \zeta(h)f(h)dh}$. The fact that ζ is an algebra homomorphism and has norm 1 implies that $\chi : G \to \mathbb{S}^1$ is a unitary character of G, i.e. $\chi \in \widehat{G}$. Then one sees that ζ as a functional corresponds to the Fourier transform of χ. See Bourbaki, Vol IX, *Théories spectrales*, Ch 2, §1, Proposition 1.1 for details. $\square$

Theorem (N.W.)**.** *If $f \in C(\mathbb{S}^1)$ and f nowhere vanishes, then Fourier(f) is absolutely convergent implies that Fourier$(\frac{1}{f})$ is absolutely convergent.*

Proof. We let $G = \mathbb{Z}$, so that $\widehat{G} = \mathbb{S}^1$. Consider $\ell^1(\mathbb{Z})$, and the evaluation map $\mathrm{ev} : \ell^1(\mathbb{Z}) \to C(\mathbb{S}^1)$ sending φ to Fourier$(\varphi) \in C(\mathbb{S}^1)$. There exists some $\varphi \in \ell^1(\mathbb{Z})$ such that Fourier$(\varphi) = \mathrm{ev}(\varphi) = f$, and

$$0 \notin \{\text{values of } f\} = \{\text{values of } \mathrm{ev}(\varphi)\}.$$

Therefore $0 \notin \mathrm{spec}(\varphi)$, and therefore there exists a $\varphi^{-1} \in \ell^1(\mathbb{Z})$ (inverse with respect to convolution). We have Fourier$(\varphi^{-1}) = \frac{1}{f}$. $\square$

[7] In fact one can define $\widehat{A}$ for a commutative Banach algebra A without unit, in which case $\widehat{A}$ is not guaranteed to be compact.

Lecture 27 (2012-12-03)

Today, we'll start discussing Lie theory.

First, I want to raise some philosophical questions: in what sense can $\mathbb{C}^\times$ be thought of as a complexification of $\mathbb{S}^1$? How can we complexify the symmetric group S_n?

We have the map $\exp : \mathbb{C} \to \mathbb{C}^\times$, defined by $a \mapsto e^a$, and the line $i\mathbb{R}$ maps onto $\mathbb{S}^1$. We can think of $\mathbb{C}$ as a complexification of the line $i\mathbb{R}$, and so the exponential map tells us that $\mathbb{C}^\times$ should be thought of as a complexification of $\mathbb{S}^1$.

More generally, if we have a $*$-algebra and the exponential map $\exp : A \to A^\times$, then the skew-hermitian operators $iH(A)$ are mapped to the unitary operators $U(A)$, and because $A = iH(A) \oplus H(A)$ is a complexification of $iH(A)$, we ought to think of $A^\times$ as a complexification of $U(A)$.

For example, if $A = \mathrm{M}_n(\mathbb{C})$ with $*$ being the hermitian adjoint, then $A^\times = \mathrm{GL}_n(\mathbb{C})$, $U(A) = U_n$, and $\mathrm{GL}_n(\mathbb{C})$ is to be thought of as a complexification of U_n.

Definition. A finite-dimensional representation $\rho : \mathrm{GL}_n(\mathbb{C}) \to \mathrm{GL}_N(\mathbb{C})$ is called holomorphic if $g \mapsto \rho_{ij}(g)$ is a holomorphic function on $\mathrm{GL}_n(\mathbb{C}) \subset \mathrm{M}_n(\mathbb{C})$ for all $1 \le i, j \le N$.

Proposition. *Let $\rho : \mathrm{GL}_n(\mathbb{C}) \to \mathrm{GL}(V)$ be a holomorphic representation, and suppose we have a subspace $W \subset V$ that is U_n-stable. Then in fact W is $\mathrm{GL}_n(\mathbb{C})$-stable.*

Corollary (The "unitary trick")**.** *Any finite-dimensional holomorphic representation of $\mathrm{GL}_n(\mathbb{C})$ is completely reducible.*

Proof of corollary. Let V be a holomorphic representation of $\mathrm{GL}_n(\mathbb{C})$. Because U_n is compact, we know that any unitary representation is completely reducible, so considering V now as a U_n-representation, we have a decomposition $V = V_1 \oplus \cdots \oplus V_k$ into U_n-irreps, and the proposition implies these are also $\mathrm{GL}_n(\mathbb{C})$-irreps (enlarging the group can't make reducible something irreducible). □

Lemma. *Let $f : \mathbb{C}^r \to \mathbb{C}$ be a holomorphic function such that $f|_{\mathbb{R}^n} = 0$. Then $f = 0$.*

Proof of lemma. This is easy - use the Cauchy-Riemann equations and induction on r. □

Proof of proposition. Suppose that $W \subset V$ is a U_n-stable subspace that is not $\mathrm{GL}_n(\mathbb{C})$-stable. Thus, we can find $g \in \mathrm{GL}_n(\mathbb{C})$ and $v \in W$ such that $gv \notin W$. Choose $\phi \in V^*$ such that $\phi|_W = 0$ and $\phi(gv) \neq 0$.

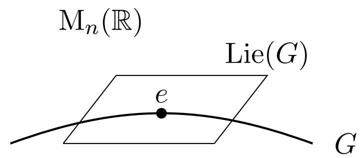
Let $f : \mathrm{M}_n(\mathbb{C}) \to \mathbb{C}$ be the map defined by $a \mapsto \phi(\rho(\exp(ia))v)$. For any $a \in H(\mathrm{M}_n(\mathbb{C}))$, we have $\exp(ia) \in U_n$, hence $\rho(\exp(ia))v \in W$, and therefore $f(a) = 0$. By the lemma, we must have that $f = 0$, but this is a contradiction; for example, there is an $x \in \mathrm{M}_n(\mathbb{C})$ such that $g = e^{ix}$, and then we must have $f(x) \neq 0$. □

This was a demonstration of a Lie theory argument. Now let's move to a more general setting.

Definition. Let $G \subset \mathrm{GL}_n(\mathbb{R})$ be a closed subgroup, and denote the unit element by e. The Lie algebra of G is defined to be $\mathrm{Lie}(G) = \{a \in \mathrm{M}_n(\mathbb{R}) \mid e^{ta} \in G \text{ for all } t \in \mathbb{R}\}$.

Lemma.

1. *$\mathrm{Lie}(G)$ is a vector subspace of $\mathrm{M}_n(\mathbb{R})$.*
2. *G is a submanifold in $\mathrm{M}_n(\mathbb{R})$ with tangent space $\mathrm{Lie}(G)$.*



Proof of 1. For any $a \in \mathrm{Lie}(G)$, we know that $za \in \mathrm{Lie}(G)$ for any $z \in \mathbb{R}$ (this is clear from the definition). For any $a, b \in \mathrm{Lie}(G)$, we can consider the map $f : \mathbb{R} \to G$ defined by $t \mapsto e^{ta}e^{tb}$ (we have $e^{ta}e^{tb} \in G$ because $a, b \in \mathrm{Lie}(G)$, so their product is as well). Clearly,

$$\left.\frac{df}{dt}\right|_{t=0} = a + b.$$

We claim that $\frac{df}{dt}|_{t=0} \in \mathrm{Lie}(G)$. We can deduce this from the fact that

$$\lim_{n\to\infty} (e^{\frac{1}{n}a}e^{\frac{1}{n}b})^n = e^{a+b}.$$

Indeed, it is more generally true that for any $a, b \in M_n(\mathbb{R})$ with $|a|, |b| \ll 1$, we have

$$\log(e^a e^b) = a + b + \frac{1}{2}(ab - ba) + o(|a|^2 + |b|^2).$$

[This is similar to the calculation of $\frac{\partial^2}{\partial t \partial s}(e^{ta}e^{sb}e^{-ta}e^{-sb})$ on a previous homework.] We then conclude that

$$e^{ta+tb+\frac{t^2}{2}(ab-ba)+o(t^2(|a|^2+|b|^2))} = e^{ta}e^{tb} \in G.$$

This doesn't seem to be enough to prove? □

Since this is not really a course on Lie theory, proof of 2 is omitted.

Examples.

- $\mathrm{Lie}(\mathrm{GL}_n(\mathbb{R})) = M_n(\mathbb{R})$
- $\mathrm{Lie}(\mathbb{S}^1) = i\mathbb{R}$
- $\mathrm{Lie}(U_n) = iH(M_n(\mathbb{C}))$
- $\mathrm{Lie}(\mathrm{SL}_n(\mathbb{C})) = \{a \in M_n(\mathbb{C}) \mid \mathrm{tr}(a) = 0\}$ (you showed on a homework that $e^{t\mathrm{tr}(a)} = \det(e^{ta})$)
- Let $G = \mathrm{O}_n(\mathbb{R}) = \{g \in M_n(\mathbb{R}) \mid (g^T)^{-1} = g\}$. Then

$$\begin{aligned}\mathrm{Lie}(\mathrm{O}_n) &= \{a \mid ((e^{ta})^T)^{-1} = e^{ta} \text{ for all } t\} \\ &= \{a \mid e^{-ta^T} = e^{ta} \text{ for all } t\} \\ &= \{a \mid -a^T = a\} \\ &= \{\text{skew-symmetric matrices}\}.\end{aligned}$$

Remark. Let N be the orthogonal complement of $\mathrm{Lie}(G)$ in $M_n(\mathbb{R})$.

$$\exp : \underbrace{M_n(\mathbb{R})}_{\mathrm{Lie}(G)\oplus N} \longrightarrow \mathrm{GL}_n(\mathbb{R}).$$

Then exp restricts to a homeomorphism of a neighborhood of the origin in $\mathrm{Lie}(G)$ to a neighborhood of the identity in G.

Let $\rho : G \to \mathrm{GL}(V)$ be a continuous representation, where $G \subset \mathrm{GL}_n(\mathbb{C})$ is a closed subgroup. For any $a \in \mathrm{Lie}(G)$, we can form the composition

$$\begin{aligned} \mathbb{R} &\xrightarrow{\exp} G \xrightarrow{\rho} \mathrm{GL}(V) \\ t &\longmapsto e^{ta} \longmapsto \rho(e^{ta}) \end{aligned}$$

which is a continuous map from $\mathbb{R}$ to $\mathrm{GL}(V)$, and by a previous homework assignment, we know that this implies there is a unique $d\rho(a) \in \mathrm{End}(V)$ such that $\rho(e^{ta}) = e^{t \cdot d\rho(a)}$. We get a map $d\rho : \mathrm{Lie}(G) \to \mathrm{End}(V)$.

Proposition.

1. *Any continuous representation $G \to \mathrm{GL}(V)$ is a C^∞ map.*
2. *$d\rho(ab - ba) = d\rho(a)d\rho(b) - d\rho(b)d\rho(a)$ for all $a, b \in \mathrm{Lie}(G)$.*
3. *If G is connected and there is no subspace $W \subset V$, $W \neq 0, V$ such that $d\rho(a)(W) \subseteq W$ for all $a \in \mathrm{Lie}(G)$, then ρ is an irrep of G.*

Lecture 28 (2012-12-05)

Let's review what we did last time.

Given a closed subgroup $G \subset \mathrm{GL}_n(\mathbb{R})$, we consider a continuous representation $\rho : G \to \mathrm{GL}(V)$. For any $a \in \mathrm{Lie}(G)$, we define $d\rho(a)$ by

$$\rho(e^{ta}) = e^{td\rho(a)}.$$

We have a diagram

$$\begin{tikzcd} \mathrm{Lie}(G) \arrow[r, "d\rho"] \arrow[d, "\exp"'] & \mathrm{End}(V) \arrow[d, "\exp"] \\ G \arrow[r, "\rho"'] & \mathrm{GL}(V) \end{tikzcd}$$

which commutes essentially by the definition of $d\rho$.

Recall that the commutator of two elements of a ring $a, b \in R$ is $[a, b] := ab - ba$.

Proposition. *Let $\rho : G \to \mathrm{GL}(V)$ be a continuous representation.*

1. *ρ is a C^∞ map.*
2. *$d\rho$ is a linear map.*
3. *If $a, b \in \mathrm{Lie}(G)$, then $[a, b] \in \mathrm{Lie}(G)$ where the commutator is defined just by consdiering a and b as matrices, and moreover, $d\rho$ respects the commutator, i.e.*

$$d\rho([a, b]) = [d\rho(a), d\rho(b)].$$

4. *Suppose G is connected. If $W \subseteq V$ is a vector subspace stable under $d\rho(a)$ for all $a \in \mathrm{Lie}(G)$, then W is also stable under $\rho(g)$ for all $g \in G$.*
5. *If $\rho' : G \to \mathrm{GL}(V)$ is another continuous representation on the same vector space V, if $d\rho = d\rho'$, then $\rho = \rho'$.*

Proof of 1. We know that exp is smooth, so that a neighborhood of 0 in $\mathrm{Lie}(G)$ is mapped diffeomorphically to a neighborhood of $e \in G$. Assuming $d\rho$ is linear, it is smooth, so ρ is smooth near identity. For any $g_0 \in G$, the map $g \mapsto \rho(g_0 \cdot g) = \rho(g_0)\rho(g)$ is smooth, so we can translate to get ρ smooth everywhere. □

Proof of 2. First, we will need the following lemma:

Lemma. *Let $f : \mathbb{R} \to G$ is a smooth path with $f(0) = e$, then*

1. $\frac{df}{dt}\big|_{t=0} \in \mathrm{Lie}(G)$
2. *If* $\frac{df}{dt}\big|_{t=0} = 0$, *then* $\frac{d^2 f}{dt^2}\big|_{t=0} \in \mathrm{Lie}(G)$.

For any $A, B \in \mathrm{M}_n(\mathbb{R})$ and $t \in \mathbb{R}$, we have

$$e^{tA}e^{tB} = e^{t(A+B) + \frac{t^2}{2}[A,B] + o(t^2)}.$$

Let $a, b \in \mathrm{Lie}(G)$. Then

$$\rho(e^{ta})\rho(e^{tb}) = \rho(e^{ta}e^{tb}) = \rho(e^{t(a+b)+\frac{t^2}{2}[a,b]+o(t^2)})$$

because ρ is a representation, but we also have that

$$\rho(e^{ta})\rho(e^{tb}) = e^{td\rho(a)}e^{td\rho(b)} = e^{t(d\rho(a)+d\rho(b))+\frac{t^2}{2}[d\rho(a),d\rho(b)]+o(t^2)}.$$

Both sides must be the identity when $t = 0$, so we can apply the lemma to get

$$\left.\frac{d(\text{right side})}{dt}\right|_{t=0} \underset{\substack{\text{chain}\\\text{rule}}}{=} d\rho(a+b).$$

and

$$\left.\frac{d(\text{left side})}{dt}\right|_{t=0} = d\rho(a) + d\rho(b)$$

so $d\rho$ is linear. To avoid circular reasoning, we need to justify use of chain rule (since we don't want to assume part 1); see next lecture. □

Proof of 3. Consider the map $f : \mathbb{R} \to G$ defined by $t \mapsto e^{ta}e^{tb}e^{-t(a+b)}$. As we showed last time, for any $a, b \in \mathrm{Lie}(G)$, we also have $a + b \in \mathrm{Lie}(G)$. By part 2 (?), we have that $\frac{df}{dt}\big|_{t=0} = 0$, so the second part of the lemma implies that $\frac{d^2f}{dt^2}\big|_{t=0} = [a, b] \in \mathrm{Lie}(G)$. □

Proof of 4. We will need the following lemma:

Lemma. *Let G be a connected topological group, and let U be an open neighborhood of $e \in G$. Then the subgroup generated by U is G.*

Proof of lemma. We improve our open neighborhood a bit by defining $\mathcal{U} = U \cap U^{-1}$, where $U^{-1} = \{g^{-1} \mid g \in U\}$. Because U^{-1} is open and contains e, $\mathcal{U}$ is an open neighborhood of e. Thus, it suffices to show that the subgroup generated by $\mathcal{U}$, which we will write $G' = \bigcup_{k\geq 1}\mathcal{U}^k$, is equal to G.

We will show that G' is open, as a union of open sets, and G' is closed, because for any $g \in \overline{G}$, □

Now, recall that we showed that the exponential map $\exp : \mathrm{Lie}(G) \to G$ is a local isomorphism. Then the image of exp contains an open neighborhood U of $e \in G$. Let $W \subset V$ be stable under $d\rho(a)$ for all $a \in \mathrm{Lie}(G)$. Then W is stable under $e^{d\rho(a)} = \rho(e^a)$ because $e^{d\rho(a)}$ is just a sum of powers of $d\rho(a)$, and therefore W is stable under $\rho(g)$ for any $g \in \mathrm{im}(\exp)$. Thus, W is stable under $\rho(g)$ for any $g \in \mathcal{U}$, hence stable under $\rho(g)$ for any $g \in \mathcal{U}^k$, hence stable under $\rho(g)$ for any $g \in G$. □

Proof of 5. By assumption, $d\rho = d\rho'$. Exponentiate both sides. Then the same argument as in proof of 4 shows $\rho = \rho'$ everywhere. □

Let $G \subset \mathrm{GL}_2(\mathbb{C})$. There is a natural action $G \circlearrowright \mathbb{C}^m[u, v]$ for each $m = 0, 1, \ldots$

Theorem. *For each $m \geq 0$, $\mathrm{SL}_2(\mathbb{C})$ has a unique (up to isomorphism) holomorphic irrep L_m of $\dim(L_m) = m + 1$ and $L_m = \mathbb{C}^m[u, v]$.*

Proof. First, we need to compute $\mathrm{Lie}(\mathrm{SL}_2(\mathbb{C}))$. As we showed last time,

$$\mathrm{Lie}(\mathrm{SL}_2(\mathbb{C})) = \{A \in \mathrm{M}_2(\mathbb{C}) \mid \mathrm{tr}(A) = 0\} = \left\{ \begin{pmatrix} a & b \\ c & -a \end{pmatrix} \,\middle|\, a, b, c \in \mathbb{C} \right\}.$$

Thus, $\mathrm{Lie}(\mathrm{SL}_2(\mathbb{C}))$ has as a basis

$$e = \begin{pmatrix} 0 & 1 \\ 0 & 0 \end{pmatrix}, \quad h = \begin{pmatrix} 1 & 0 \\ 0 & -1 \end{pmatrix}, \quad f = \begin{pmatrix} 0 & 0 \\ 1 & 0 \end{pmatrix}.$$

As you've shown on a homework,

$$[e, f] = h, \quad [h, e] = 2e, \quad [h, f] = 2f.$$

Let $\rho : \mathrm{SL}_2(\mathbb{C}) \to \mathrm{GL}(V)$ be a holomorphic representation. Consider the map $d\rho : \mathrm{Lie}(G) \to \mathrm{End}(V)$, and let $E = d\rho(e)$, $H = d\rho(h)$, $F = d\rho(f)$. Then E, H, F satisfy the same commutation relations.

This gives V the structure of a $\mathcal{U}$-module, where $\mathcal{U}$ is the algebra defined on the same homework assignment.

We claim that if V is irreducible as an $\mathrm{SL}_2(\mathbb{C})$-representation, then V is simple as a $\mathcal{U}$-module. Suppose otherwise; then let $W \subset V$ be a non-trivial $\mathcal{U}$-submodule. Then part 4 of our proposition implies that, since W is stable under $d\rho(a)$ for any $a \in \mathrm{Lie}(G)$, we must have that W is a subrepresentation of V, but this is a contradiction with the assumption that V is irreducible.

As you showed on your homework, this means that $V \cong \mathbb{C}^m[u, v]$ as a $\mathcal{U}$-module for some m.

Thus, we get some representation $\rho : \mathrm{SL}_2(\mathbb{C}) \to \mathrm{GL}(\mathbb{C}^m[u, v])$, which we can compare with the natural representation. But by construction, their differentials are equal since the $\mathcal{U}$-action on $\mathbb{C}^m[u, v]$ is the natural one. Because $\mathrm{SL}_2(\mathbb{C})$ is connected, we are done by part 5 of the proposition. □

Next time, we will look at $\mathrm{SU}_2(\mathbb{C})$, $\mathrm{SO}_3(\mathbb{R})$.

Lecture 29 (2012-12-07)

Let's finish up the computation of $\frac{d(\text{left side})}{dt}$ from last time, where

$$\text{left side} = \rho(e^{t(a+b)+\frac{t^2}{2}[a,b]+o(t^2)}) = \rho(e^{t\cdot f(t)}) = e^{t\cdot d\rho(f(t))},$$

letting $f(t) = a+b+\frac{t}{2}[a,b]+\frac{o(t^2)}{t}$. Note that $f(t)\to a+b$ as $t\to 0$.

We have

$$\frac{e^{t\,d\rho(f(t))}-1}{t} = \frac{e^{t\,d\rho(f(t))}-1}{t\cdot d\rho(f(t))}\cdot\frac{td\rho(f(t))}{t}.$$

Because ρ is continuous, we also have that $d\rho$ is continuous, hence the first factor $\frac{e^{t\,d\rho(f(t))}-1}{t\cdot d\rho(f(t))}$ goes to 1 as $t\to 0$, and hence the limit of the entire expression as $t\to 0$ is $d\rho(a+b)$.

Now we will consider the action of $\mathrm{SL}_2(\mathbb{C}) \circlearrowright \mathbb{C}^m[u,v]$, and the action of SU_2 obtained by the inclusion $\mathrm{SU}_2 \hookrightarrow \mathrm{SL}_2(\mathbb{C})$.

Theorem. *For each $m\geq 0$, restricting the $\mathrm{SL}_2(\mathbb{C})$-action on $\mathbb{C}^m[u,v]$ to SU_2 yields an irrep of SU_2, and these are all irreps of SU_2 up to isomorphism.*

Proof. Because $\mathrm{SU}_2 = \mathrm{SL}_2(\mathbb{C})\cap \mathrm{U}_2$, we have

$$\mathrm{Lie}(\mathrm{SU}_2) = \{A\in \mathrm{M}_2(\mathbb{C}) \mid A^* = -A, \mathrm{tr}(A)=0\} = \left\{\begin{pmatrix} ia & b+ic \\ -b+ic & -ia\end{pmatrix} \;\middle|\; a,b,c\in\mathbb{R}\right\}.$$

We can decompose $\mathrm{M}_2(\mathbb{C})$ as a direct sum of the hermitian and skew-hermitian matrices:

$$\mathrm{M}_2(\mathbb{C}) = H(\mathrm{M}_2(\mathbb{C}))\oplus iH(\mathrm{M}_2(\mathbb{C})),$$

and therefore

$$\underbrace{\{A\in \mathrm{M}_2(\mathbb{C})\mid \mathrm{tr}(A)=0\}}_{\mathrm{Lie}(\mathrm{SL}_2(\mathbb{C}))} = \{A\in H(\mathrm{M}_2(\mathbb{C}))\mid \mathrm{tr}(A)=0\}\oplus \underbrace{i\{A\in H(\mathrm{M}_2(\mathbb{C}))\mid \mathrm{tr}(A)=0\}}_{\mathrm{Lie}(\mathrm{SU}_2)}.$$

We can express this as

$$\mathrm{Lie}(\mathrm{SL}_2(\mathbb{C})) = i\mathrm{Lie}(\mathrm{SU}_2)\oplus \mathrm{Lie}(\mathrm{SU}_2) = \mathbb{C}\otimes_{\mathbb{R}}\mathrm{Lie}(\mathrm{SU}_2),$$

so that $\mathrm{Lie}(\mathrm{SU}_2)$ is like the "real part" of the vector space $\mathrm{Lie}(\mathrm{SL}_2(\mathbb{C}))$, and $\mathrm{Lie}(\mathrm{SL}_2(\mathbb{C}))$ is like the complexification of $\mathrm{Lie}(\mathrm{SU}_2)$.

Let $\rho:\mathrm{SU}_2\to \mathrm{GL}(V)$ be a irrep. The differential map is $d\rho:\mathrm{Lie}(\mathrm{SU}_2)\to\mathrm{End}_{\mathbb{C}}(V)$. Because ρ is a irrep, there is no proper subspace $W\subset V$ that is stable under $\mathrm{im}(d\rho)$. Because $\mathrm{Lie}(\mathrm{SU}_2)$ is a real vector space and $\mathrm{End}_{\mathbb{C}}(V)$ is a complex vector space, we can always extend an $\mathbb{R}$-linear map from $\mathrm{Lie}(\mathrm{SU}_2)$ to $\mathrm{End}_{\mathbb{C}}(V)$ to a $\mathbb{C}$-linear map from the complexification of $\mathrm{Lie}(\mathrm{SU}_2)$ to the same vector space $\mathrm{End}_{\mathbb{C}}(V)$,

$$(\mathbb{C}\otimes_{\mathbb{R}} d\rho):\underbrace{\mathbb{C}\otimes_{\mathbb{R}}\mathrm{Lie}(\mathrm{SU}_2)}_{\mathrm{Lie}(\mathrm{SL}_2(\mathbb{C}))}\to\mathrm{End}_{\mathbb{C}}(V).$$

Because $\mathrm{Lie}(\mathrm{SL}_2(\mathbb{C})) = \langle e,h,f\rangle$, we see that V acquires the structure of a simple $\mathcal{U}$-module. □

Now let's discuss $\mathrm{SO}(\mathbb{R}^3)$. There is a natural action $\mathrm{SO}(\mathbb{R}^3)\circlearrowright\mathbb{C}^n[x,y,z]$.

Theorem. *For each positive odd integer $2n+1$, $n = 0, 1, \ldots$, there is a unique irrep of* $\mathrm{SO}(\mathbb{R}^3)$ *of dimension $2n+1$ (up to isomorphism). Specifically, this irrep is* $\mathrm{Harm}^m(\mathbb{C}^3, \mathrm{SO}(\mathbb{R}^3))$. *These are all of the irreps of* $\mathrm{SO}(\mathbb{R}^3)$.

Proof. Recall from the first homework assignment that there is a double cover map $\pi : \mathrm{SU}_2 \to \mathrm{SO}(\mathbb{R}^3)$, which you obtained by thinking of SU_2 as $\mathrm{U}(\mathbb{H})$. The kernel of π is just $\{\pm 1\}$.

Given an irrep $\phi : \mathrm{SO}(\mathbb{R}^3) \to \mathrm{GL}(V)$, the composition $\phi \circ \pi$ is an irrep of SU_2 since ϕ is surjective, and the map $\phi \mapsto \phi \circ \pi$ clearly gives a bijection

$$\widehat{\mathrm{SO}(\mathbb{R}^3)} \overset{\pi^*}{\cong} \{\rho \in \widehat{\mathrm{SU}_2} \mid \rho(-1) = 1\}$$

between irreps ϕ of $\mathrm{SO}(\mathbb{R}^3)$ and irreps ρ of SU_2 that annihilate $\ker(\pi)$.

Any irrep of SU_2 is some $\mathbb{C}^m[u,v]$. Note that $-\mathrm{id}$ maps $u^a v^b$ to $(-1)^{a+b} u^a v^b$, so a representation descends to $\mathrm{SO}(\mathbb{R}^3)$ if and only if $m = a+b$ is even, i.e. $m = 2n$ for some m. Note that $\dim(\mathbb{C}^m[u,v]) = \dim(\mathbb{C}^{2n}[u,v]) = 2n+1$.

Now we need to identify this representation with the representation $\mathrm{Harm}^m(\mathbb{C}^3, \mathrm{SO}(\mathbb{R}^3))$. Recall that by a homework problem,

$$\mathbb{C}^n[x,y,z] \cong \mathcal{H}^n \oplus r^2 \mathcal{H}^{n-2} \oplus \cdots$$

where $r^2 = x^2 + y^2 + z^2$, and also that $\dim(\mathcal{H}^k) = 2k+1$. Note that $\mathcal{H}^k$ is an $\mathrm{SO}(\mathbb{R}^3)$-stable subspace of $\mathbb{C}^k[x,y,z]$.

There are two possibilities:

1. $\mathcal{H}^n$ is an irrep of dimension $2n+1$ (which is what we want), or
2. it isn't.

If it isn't, then each irreducible direct summand of $\mathcal{H}^n$ has dimension $< 2n+1$, and observing the decomposition of $\mathbb{C}^n[x,y,z]$ we wrote above, we see that statement 2 is equivalent to

2′. Each irreducible direct summand of $\mathbb{C}^n[x,y,z]$ has dimension $< 2n+1$.

Now, it will suffice to show that 2′ is impossible. Indeed, we claim that the $(2n+1)$-dimensional irrep of $\mathrm{SO}(\mathbb{R}^3)$ does occur in $\mathbb{C}^n[x,y,z]$.

Consider the map $\mathbb{R} \to \mathrm{SU}_2$ defined by $t \mapsto \left(\begin{smallmatrix} e^{it} & 0 \\ 0 & e^{-it} \end{smallmatrix}\right)$. Let's check what it does to monomials:

$$\begin{pmatrix} e^{it} & 0 \\ 0 & e^{-it} \end{pmatrix} : u^a v^b \mapsto e^{iat} e^{-ibt} u^a v^b = e^{i(a-b)t} u^a v^b.$$

Thus, the eigenvalues of this matrix on $\mathbb{C}^{2n}[u,v]$ are $\{e^{ikt} \mid -2n \le k \le 2n\}$, and in particular, the maximum possible k is $2n$.

Therefore, if we can show that $\pi\left(\begin{smallmatrix} e^{it} & 0 \\ 0 & e^{-it} \end{smallmatrix}\right)$ does have e^{2nit} as an eigenvalue when acting on $\mathbb{C}^n[x,y,z]$, we will be done, because no lower dimensional irrep could have produced it.

On the homework, you classified continuous homomorphisms $\mathbb{R} \to \mathrm{SO}_n$. Then we know that the composition $\rho : \mathbb{R} \to \mathrm{SU}_2 \xrightarrow{\pi} \mathrm{SO}(\mathbb{R}^3)$ must map t to e^{At} for some A, and moreover, we now know that we must have $A \in \mathrm{Lie}(\mathrm{SO}(\mathbb{R}^3))$, or in other words, $A \in \mathrm{M}_3(\mathbb{R})$ satisfies $A^t = -A$. Therefore, there exists an orthogonal basis x, y, z in which

$$A = \begin{pmatrix} 0 & a & 0 \\ -a & 0 & 0 \\ 0 & 0 & 0 \end{pmatrix}.$$

Note that

$$\begin{aligned} \{t \in \mathbb{R} \mid \rho(t) = 1\} &= \left\{ t \in \mathbb{R} \middle| \begin{pmatrix} e^{it} & 0 \\ 0 & e^{it} \end{pmatrix} = \pm 1 \right\} \\ &= \{t \in \pi\mathbb{Z}\} \end{aligned}$$

But on the other hand,

$$\begin{aligned} \{t \in \mathbb{R} \mid \rho(t) = 1\} &= \{t \mid e^{At} = 1\} \\ &= \{t \mid e^{\pm iat} = 1\} \\ &= \{at \in 2\pi\mathbb{Z}\} \end{aligned}$$

Therefore, $a = 2$, and the matrix e^{At} has eigenvalues e^{2it}, e^{-2it}, and 1. Acting on $\mathbb{C}^n[x, y, z]$, we can see that it has as e^{2nit} as an eigenvalue, because (for example) x^n is mapped to $(e^{2it}x)^n = e^{2nit}x^n$. Thus, we are done. $\square$