MATH 122 NOTES: MODULES AND REPRESENTATION THEORY

ARUN DEBRAY
AUGUST 3, 2013

These notes were taken in Stanford's Math 122 class in Spring 2013, taught by Professor Gunnar Carlsson. I TEXed them using `vim`, and as such there may be typos; please send questions, comments, complaints, and corrections to `adebray@stanford.edu`.

CONTENTS

1. MODULES: 4/2/13

"I think we're the only non-physicists in this class."

Definition. Let k be a field. Then, a vector space over k is an abelian group V together with a map $\mu : k \times V \to V$, called scalar multiplication, such that, for any $k_1, k_2 \in k$ and $v_1, v_2, v \in V$,

a. $(k_1k_2)v = k_1(k_2v)$,
b. $(k_1 + k_2)v = k_1v + k_2v$,
c. $k_1(v_1 + v_2) = k_1v_1 + k_2v_2$, and
d. $1 \cdot v = v$.

Example 1.1. From multivariable calculus, we have $k = \mathbb{R}$ and $V = \mathbb{R}^n$, with $k(x_1, \ldots, x_n) = (kx_1, \ldots, kx_n)$. Similarly, one could set $k = \mathbb{C}$ and $V = \mathbb{C}^n$.

These seem like very simple examples, but up to isomorphism this is just about it. The structure of vector spaces is very restricted: if V is a vector space over k, then $V \cong k^n$, where n might be infinite.

Notice also the lack of multiplicative inverses in the above definition, so that it still makes sense for a ring with identity. Note that all rings will be taken to be commutative for today's lecture. Thus:

Definition. If A is a ring, an A-module is an abelian group M equipped with a map $A \times M \to M$ satisfying the conditions a to d above.

Example 1.2. a. Obviously, every vector space is a module over its field.
b. if $A = \mathbb{Z}$, $M = \mathbb{Z}^n$ is a $\mathbb{Z}$-module, where $m(m_1, \ldots, m_n) = (mm - 1, \ldots, mm_n)$.

Remark. More generally, A^n is always an A-module with $a(a_1, \ldots, a_n) = (aa_1, \ldots, aa_n)$.

c. Suppose $n \in \mathbb{N}$ and take $M = \mathbb{Z}/n\mathbb{Z}$. Then, M is a $\mathbb{Z}$-module with scalar multiplication given by $m[s] = [ms]$ (where $s \in \mathbb{Z}$ and the notation is $[s] = s \bmod n$).

It is important (albeit straightforward) to prove that this map is well-defined: suppose $s' = s + kn$, so that $m[s'] = [m(s+kn)] = [ms + mkn] = [ms]$ (since this mods out by n), so this is well-defined.

Notice that $\mathbb{Z}/n\mathbb{Z} \ncong \mathbb{Z}^m$ (since finite vs. infinite), so there are more interesting things going on than in the vector-spatial case.

d. Take a ring A and A-modules M and N. Then, their direct sum is $M \oplus N = \{(m,n) \mid m \in M, n \in N\}$ with $(m,n)+(m',n') = (m+m', n+n')$ and $a(m,n) = (am, an)$ (i.e. just coordinate-wise; this is not complicated). Since $A^n = \bigoplus_{i=1}^n A$ and A is an A-module over itself, this is another proof that A^n is an A-module. But now there are lots more modules, such as $\mathbb{Z}/3 \oplus \mathbb{Z}/7$ or $\mathbb{Z}/7 \oplus \mathbb{Z}/49$.

e. Let k be a field and $k[x]$ be its ring of polynomials. Consider k^2, which is a 2-dimensional vector space over k (and therefore a k-module), and it can be made into a $k[x]$-module: choose a 2×2 matrix A with entries in k. This gives a map $A : k^2 \to k^2$, with the elements of k^2 written as column vectors.

Define $\mu : k[x] \to x \times k^2$ to be $\mu(x,v) = x \cdot v = Av$. Then, μ can be extended in a unique way because of the axioms of the module: since $(kk')v = k(k'v)$, then $x^k v = A^k v$ for all $k \in \mathbb{Z}$. And by distributivity, $(k+k')v = kv + k'v$, so

$$\left(\sum_i k_i x^i\right) v = \sum_i k_i (x_i v) = \sum_i k_i A^i v,$$

which gives the overall formula. Thus, the choice of the matrix A gives a module structure of k^2 as a $k[x]$-module. This can be generalized to k^n, in which case A is an $n \times n$ matrix, in the straightforward manner.

f. Suppose A is any ring and $I \subseteq A$ is an ideal. Then, because $A \cdot I \subseteq I$, then I is a module over A, called a submodule of A. More generally:

Definition. If M is an A-module and $N < M$ (as groups) is closed under multiplication by A, then N is a module and referred to as a submodule of M.

Proposition 1.1. *Any abelian group G is a $\mathbb{Z}$-module in a unique way, and vice versa, so that there is a one-to-one correspondence of $\mathbb{Z}$-modules and abelian groups.*

Proof. Construct a map $\mathbb{Z} \times G \to G$ such that $1 \cdot g = g$ for all $g \in G$. Then, everything else is forced:

$$n \cdot g = \left(\sum_{i=1}^n 1\right) \cdot g = \prod_{i=1}^g = g^n,$$

with G written multiplicatively. Then, it's easy to check that this map prodvides a $\mathbb{Z}$-module structure. ⊠

$\mathbb{Z}$-modules are the same as abelian groups. This is important!

Turning to $k[x]$-modules, every $k[x]$-module V is a k-vector space, since k is a subring of $k[x]$. There is also a linear transformation $(x\cdot) : V \to V$, which is also called L_x.[1] Following the same argument as in the k^2 case above, the structure is forced by the choice of L_x. Thus, a $k[x]$-module is equivalent to a pair (V, L), where V is a k-vector space and $L : V \to V$ is a k-linear map.[2]

Definition. Let M and N be A-modules. Then, an A-module homomorphism from M to N is a homomorphism $f : M \to N$ of abelian groups that also satisfies the alinearity condition: $f(am) = af(m)$ for $m \in M$ and $a \in A$, so that the map respects scalar multiplication.

f is an isomorphism if it is bijective (equivalently, invertible; not that this forces f^{-1} to be A-linear); to say M and N are isomorphic is to say that M and N can be obtained from each other by relabelling the elements, so they're in some sense the same thing.

Definition. A module is finitely generated if there is a surjective homomorphism $\varphi : A^n \to M$ for some $n \in \mathbb{N}$.

This definition makes sense: if one takes the i^{th} standard basis vector $e_i \in A^n$, then every $m \in M$ can be written as $m = \sum_{i=1}^n a_i \varphi(e_i)$, so $\varphi(e_1), \ldots, \varphi(e_n)$ forms a generating set for M, and every element of M can be written as a linear combination of them.

Classifying modules up to isomorphism is a fundamental question, especially over a given ring or considering only finitely generated modules. This will occupy a significant portion of the class. Here are some results that will be shown:

Example 1.3. a. If $A = k$ is a field, then any finitely generated module over A is isomorphic to A^n for some n determined uniquely by the module, called the dimension of the vector space. This is a very clean, slick paramterization.

[1] Oh God it's a Lie derivative

[2] Here, k-linear means linear with respect to the field k; sometimes the notation k-linear is used for a multilinear map.

b. if $A = \mathbb{Z}$, this is the classification of finitely generated abelian groups: every finitely generated $\mathbb{Z}$-module is of the form

$$\mathbb{Z}^n \oplus \bigoplus_{i=1}^{k} \mathbb{Z}/p_i^{e_i},$$

where n is called the rank of the abelian group and the p_i are primes. There are several ways to write this, but n and the pairs (p_i, e_i) are determined buy the module, though the pairs can be reordered. This is a bit more complicated than vector spaces.

c. If M is a finitely generated $k[x]$-module, the structure will look very similar, because $k[x]$ and $\mathbb{Z}$ are both PIDs. Here,

$$M = k[x]^n \oplus \bigoplus_{i=1}^{k} k[x]/(f_i^{e_i}),$$

where the $f_i \in k[x]$ are irreducibles, and n and the set of pairs (f_i, e_i) are determined by the isomorphism class of the module.

Since a $k[x]$-module determines and is determined by a pair (V, L), then consider two modules $M \sim (V, L)$, and $M' \sim (V, L')$. Under what circumstances is $M \cong M'$?

If $M \cong M'$, then there is certainly a group isomorphism $f : M \to M'$. Then, f is an automorphism of V (as a k-vector space) which isn't necessarily the identity (hello Math 121!). But the fact that f is an isomorphism of $k[x]$-modules means that the following diagram commutes:

$$\begin{array}{ccc} V & \xrightarrow{L} & V \\ {\scriptstyle f}\downarrow & & \downarrow{\scriptstyle f} \\ V & \xrightarrow{L'} & V \end{array}$$

Thus, $f \circ L = L' \circ f$, so $f \circ L \circ f^{-1} = L'$. Thus, L and L' are conjugate. Getting more concrete, pick a basis for V, so L, L', and f are given by matrices M_L, $M_{L'}$, and M_f, respectively. Thus, $M_f M_L M_f^{-1} = M_{L'}$, so the modules M and M' are isomorphic iff the matrices representing their linear aps are conjugate. Now, it's a linear algebra problem: the isomorphism classification of $k[x]$-modules is the same as that of conjugacy classes of matrices over k. If $k = \mathbb{R}$ or $k = \mathbb{C}$, this is also an important problem in ordinary differential equations: $\mathbf{x}' = A\mathbf{x}$ is easier to solve if there are nice coordinates, which imvilves finding conjugates for A. Over $\mathbb{C}$ in particular, it will be possible to obtain a Jordan normal form.

Definition. Suppose $f : M \to N$ is a homomorphism of A-modules. Then, its kernel is $\operatorname{Ker}(f) = \{m \in M \mid f(m) = 0\}$.

$\operatorname{Ker}(f) \subseteq N$ is a submodule: it's closed under addition because f is a group homomorphism, and if $m \in \operatorname{Ker}(f)$, then $f(am) = af(m) = a \cdot 0 = 0$, so it's also closed under scalar multiplication.

2. Quotient Modules: 4/4/13

Suppose $f : M \to N$ is a homomoprhism of A-modules. In addition to the kernel, one has the submodule $\operatorname{Im}(f) = \{f(m) \mid m \in M\} \subseteq N$. Since f is a group homomoprhism, it is closed under addition, and $af(m) = f(am)$, which is in M, so this is closed under scalar multiplication as well.

Let $N \subseteq M$ be an A-submodule. Then, M/N, as abelian groups, can be given a module structure as follows: addition is defined as in abelian groups, and let $a(m+N) = am + N$. This is well-defined, because if $m + N = m' + N$, then $m' = m + n$ for some $n \in N$, so $a(m' + N) = a(m + n + N) = am + an + N = am + N = a(m + N)$, because $an \in N$ since N is a submodule.

Definition. If $f : M \to N$ is an A-module homomorphism, the cokernel of f is $N/\operatorname{Im}(f)$.

Definition. If M is an A-module and $m_1, \ldots, m_s \in M$, then let

$$L(m_1, \ldots, m_s) = \left\{ \sum_{i=1}^{s} a_i m + i \mid a_i \in M \right\}.$$

This is a submodule, which is fairly clear: addimg two of its elements or mutliplying by a scalar still gives a linear combination.

Example 2.1. Consider vector spaces over $\mathbb{Q}$: if $V = \mathbb{Q}^3$, the quotient $V/L(e_1, e_2)$ (where e_i is the i^{th} standard basis vector) will be isomorphic to $\mathbb{Q}$: define a homomorphism $\theta : \mathbb{Q} \to V/L$ given by $\theta(q) = \begin{pmatrix} 0 \\ 0 \\ q \end{pmatrix} + L$. This is fairly clearly a homomorphism of modules, and it can be shown to be an isomorphism:

- θ is injective, because if $\theta(q) = 0$, then $\theta(q) + L = L$, so $\theta(q) \in L$. If $\begin{pmatrix} 0 \\ 0 \\ q \end{pmatrix} \in L$, then $q = 0$. This is enough to imply that it's injective because it holds true for the underlying groups, and injectivity is just a ste-theoretic notion.
- θ is surjective, because

$$\begin{pmatrix} x \\ y \\ z \end{pmatrix} + L = \begin{pmatrix} 0 \\ 0 \\ z \end{pmatrix} = \theta(z).$$

Thus, θ is an isomorphism and $V/L \cong \mathbb{Q}$.

The takeaway is that quotienting is akin to zeroing out the basis vectors in the quotient set: $\mathbb{Q}^6/L(e_2, e_4, e_6) \cong \mathbb{Q}^3$, for another example. But it's not always that easy: take $V = \mathbb{Q}^4$ and $L = L\left(\begin{pmatrix} 1 \\ 1 \\ 0 \\ 0 \end{pmatrix}, \begin{pmatrix} 1 \\ 0 \\ 1 \\ 0 \end{pmatrix}, \begin{pmatrix} 0 \\ 1 \\ -1 \\ 0 \end{pmatrix}\right)$. There's an algorithm for finding the quotient module:

(1) Build a matrix whose columns are the vectors to be spanned.
(2) Then, one can perform arbitrary row and column operations to the matrix:

$$\begin{bmatrix} 1 & 1 & 0 \\ 1 & 0 & 1 \\ 0 & 1 & -1 \\ 0 & 0 & 0 \end{bmatrix} \sim \begin{bmatrix} 1 & 1 & 0 \\ 0 & -1 & 1 \\ 0 & 1 & -1 \\ 0 & 0 & 0 \end{bmatrix} \sim \begin{bmatrix} 1 & 1 & 0 \\ 0 & -1 & 1 \\ 0 & 0 & 0 \\ 0 & 0 & 0 \end{bmatrix} \sim \begin{bmatrix} 1 & 0 & 0 \\ 0 & 0 & 1 \\ 0 & 0 & 0 \\ 0 & 0 & 0 \end{bmatrix}.$$

Thus, here, $L = L(e_1, e_2)$, so $V/L \cong \mathbb{Q}^4$.

Proposition 2.1. *Suppose $L(m_1, \dots, m_s) \subseteq A^t$ is an A-sub-module, and:*

(1) Suppose α is an A-module automorphism of A^t. Then, $A^t/L(m_1, \dots, m_s) \cong A^t/L(\alpha(m_1), \dots, \alpha(m_s))$, and
(2) if M denotes the $t \times s$ matrix whose entries are a_{ij} is the i^{th} coordinate of m_j, then if α' is an automorphism of A^s, one obtains an isomorphism by right-multiplying by α'.

This proposition provides the theoretical justification for the row-reduction computation: M represents a homomorphism from $A^s \to A^t$, and the statement implies that $A^t/L(m_1, \dots, m_s) = \operatorname{coker}(M)$, because if $f : N \to M$ and α_N, α_M are automorphisms of N and M, respectively, then $\operatorname{coker}(f) \cong \operatorname{coker}(\alpha_M f \alpha_N)$.

Proof of Proposition 2.1.

$$\begin{array}{ccc} N & \xrightarrow{\alpha_N^{-1}} & N \\ {\scriptstyle f}\downarrow & & \downarrow{\scriptstyle \alpha_M f \alpha_N} \\ M & \xrightarrow{\alpha_M} & M \end{array}$$

□

By row and column operations, any matrix over a field can be transformed into $\begin{pmatrix} I & 0 \\ 0 & 0 \end{pmatrix}$, which is a linear-algebraic fact we already knew.

Stepping back into the more general PID case, consider $\mathbb{Z}^3/L$, where L is the span of $\begin{pmatrix} 1 \\ 1 \\ 3 \end{pmatrix}$ and $\begin{pmatrix} 1 \\ -1 \\ 5 \end{pmatrix}$. Then,

$$\begin{pmatrix} 1 & 1 \\ 1 & -1 \\ 3 & 5 \end{pmatrix} \sim \begin{pmatrix} 1 & 1 \\ 0 & -2 \\ 0 & 2 \end{pmatrix} \sim \begin{pmatrix} 1 & 1 \\ 0 & -2 \\ 0 & 0 \end{pmatrix} \sim \begin{pmatrix} 1 & 0 \\ 0 & -2 \\ 0 & 0 \end{pmatrix},$$

so $\mathbb{Z}/L \cong \mathbb{Z} \oplus \mathbb{Z}/2$, since dividing by 2 isn't possible. Notice how the theory of vector spacs and finitely generated modules over a PID relate to the lack of multiplicative inverses! The classification of modules over a PID relates to normal forms of matrices under row and column operations.

Theorem 2.2. *Any matrix over a principal ideal domain can be reduced to $\begin{pmatrix} D & 0 \\ 0 & 0 \end{pmatrix}$, where D is a diagonal matrix.*

This theorem will be proven later.

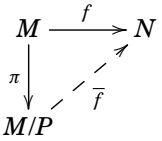
There are several key properties of homomorphisms:

Theorem 2.3 (Fundamental Isomorphism Theorems)**.** *Let $f : M \to N$ be a homomorphism. Then,*

a. $\operatorname{Ker}(f) \subseteq M$ *is a submodule, as is* $\operatorname{Im}(f) \subseteq N$*, and in particular* $M/\operatorname{Ker}(f) \cong \operatorname{Im}(f)$.

b. If A and B are submodules of some M, then $A+B = \{a+b \mid a \in A, b \in B\}$ and $A \cap B$ are submodules of M. Then, $(A+B)/B \cong A/A \cap B$.
c. If $A \subseteq B \subseteq M$ as submodules, then $M/A \supseteq B/A$, and $(M/A)/(B/A) \cong M/B$.
d. Submodules of M/N are in a one-to-one correspondence with submodules of M containing N.

Proof of part a. Suppose $f : M \to N$ is a homomorphism and $P \subseteq M$ is a submodule. Let $\pi : m \mapsto m+P$ be the projection homomorphism;[3] then, there is a homomorphism $\overline{f}$ such that the following diagram commutes:



An obvious necessary condition is for f to vanish on P, since $\pi(P) = 0$, but this turns out to also be a sufficient condition: suppose $f(P) = 0$. Then, define $\overline{f}(m+P) = \overline{f}(m) + P$. Again, this must be checked for well-definedness: if $m' + P = m + P$, then $m' = m + p$ for some $p \in P$, so $f(m') = f(m+p) = f(m) + f(p) = f(m) + 0$.

Thus, since $f(\mathrm{Ker}(f)) = 0$, then $\overline{f}(m + \mathrm{Ker}(f)) = f(m) + \mathrm{Ker}(f)$ (replacing P with $\mathrm{Ker}(f)$). Then, $\overline{f}$ is bijective:

- By definition, every element in $\mathrm{Im}(f)$ is of the form $x = f(m)$ for some $m \in M$. Thus, since the diagram commutes, then $x = \overline{f}(m + \mathrm{Ker}(f))$, so $\overline{f}$ is surjective.
- $\mathrm{Ker}(\overline{f}) = m + \mathrm{Ker}(f)$ such that $f(m) = 0$, so $m \in \mathrm{Ker}(f)$, so $\mathrm{Ker}(\overline{f}) = \mathrm{Ker}(f) = 0$ in $m/\mathrm{Ker}(f)$. Since the kernel is trivial, then $\overline{f}$ is injective.

Thus, $\overline{f}$ is an isomorphism. ⊠

The remaining parts will be proved in a future lecture. A typical example might include sending $\mathbb{Z}/8 \to \mathbb{Z}/8$ via multiplication by 2; then, the image is isomorphic to $\mathbb{Z}/4$ and the kernel to $\mathbb{Z}/2$, so one has that $\mathbb{Z}/8/\mathbb{Z}/2 \cong \mathbb{Z}/4$.

3. The Isomorphism Theorems: 4/9/13

"Wow. I just spent 70 minutes on three-quarters of an isomorphism theorem."

Today's lecture was given by Dr. Daniel Muellner (a postdoc), because Dr. Carlsson is out of town.

Recall that if $f : M \to N$ is an R-module homomorphism, then $\mathrm{Im}(f) \cong M/\mathrm{Ker}(f)$, as shown in Theorem 2.3, part a. Observe that there are two possible definitions of an R-module isomorphism:

(1) The standard set-theoretic definition requires that an isomorphism be a homomophism that is injective and surjective.
(2) A more algebraic definition requires f to have an inverse g such that $f \circ g = \mathrm{id}_N$ and $g \circ f = \mathrm{id}_M$.

The First Isomorphism Theorem equates these: if f is injective, then $\mathrm{Ker}(f)$ is trivial, and if it's surjective, then $\mathrm{Im}(f) = N$, so $M \cong N$.

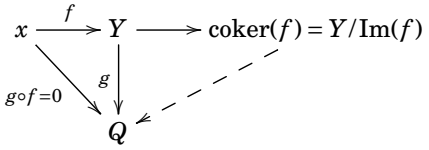
Example 3.1. For the Second Isomorphism Theorem (part b), let $M = \mathbb{Z}/60$, $A = 4\mathbb{Z}/60$ (i.e. the set of numbers divisible by 4 mod 60), and $B = 6\mathbb{Z}/60$. Then:

- $A + B = 2\mathbb{Z}/60$, since $\gcd(6,4) = 2$, and $(A+B)/B = (2\mathbb{Z}/60)/(6\mathbb{Z}/60) \cong (\mathbb{Z}/30)/(\mathbb{Z}/10) \cong \mathbb{Z}/3$.
- $A \cap B = 12\mathbb{Z}/60$, this time since $\mathrm{lcm}(6,4) = 2$, and $A/(A \cap B) = (4\mathbb{Z}/60)/(12\mathbb{Z}/60) \cong (\mathbb{Z}/15)/(\mathbb{Z}/5) \cong \mathbb{Z}/3$.

Proof of Theorem 2.3, part b. There is an inclusion of submodules $A \hookrightarrow A+B$ and quotient map $A+B \twoheadrightarrow (A+B)/A$, so their composition map, called f, must be surjective.

Then, $A \cap B \subseteq \mathrm{Ker}(f)$, because it is modded out bu B. Then, recall that the constructions of elements of $(A+B)/B$ as cosets or equivalence classes $a+b+B$ in the sense of an abelian group. Thus, $a+B = a+b+B$, so the isomorphism class $[a]$ of a is 0 in $(A+B)/B$ iff $a \in B$, so if $f(a) = 0$, then $a \in A$ and $a \in B$, so $\mathrm{Ker}(f) = A \cap B$. Then, by the First Isomorphism Theorem, the second is proved. ⊠

If $f : X \to Y$ is a homomorphism of modules, then there is a universal property of $\mathrm{coker}(f)$: if $g : Y \to Q$ is a homomorphism of modules such that $g \circ f = 0$, then there is a unique homomorphism $\mathrm{coker}(f) \to Q$ such that the following diagram commutes:

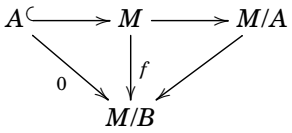


[3] That this is in fact a homomorphism is easy to verify.

Exercise 3.1. Prove the above universal property.

Universal properties such as that one are common in algebraic constructions.

Proof of Theorem 2.3, part c. Suppose $A \subseteq B \subseteq M$ as submodules, and consider $M \xrightarrow{f} M/B$. Since A is a submodule of B, then $A \subseteq \text{Ker}(f)$. Now, consider the diagram



where $A \to M/B = 0$ because $A \subseteq \text{Ker}(f)$. By the universal property, there exists a unique homomorphism $M/A \to M/B$. Since $B \supseteq A$, this must be surjective; in some sense, the equivalence classes of A are "stricter." Then, what s in the kernel? $[m] = 0$ in M/B iff $m \in B$, so $\text{Ker}(f)$ is everything in B, or $\{b + A \mid b \in B\} = B/A$. ⊠

The statement just proved is also referred to as the Third Isomorphism Theorem.

Example 3.2. Let F be a field with $\text{Char}(F) \neq 2$, and let $M = F[x,y]$, the module of polynomials in 2 variables over F. M is a ring over itself, but let $R = A = F[u]$, where $u \mapsto x+y$ gives M a structure as an R-module, and $A \subseteq M$ as a submodule via $A = \{\sum a_i (x+y)^i\}$. Let B be the set of symmetric polynomails in two variables (those such that $f(x,y) = f(y,x)$), which are generated by $\{x^a y^b + x^b y^a \mid a,b \geq 0, a \leq b\}$. Tread carefully here: there are lots of algebraic structures flying around, and many of these are structures over different things in the same way.

Since these polynomials can also be multiplied in a ring structure, they form an F-algebra generated by $\{x+y, xy\}$. This isn't completely obvious, since there's a theorem behind it, but it should seem at least plausible.[4] Thus, $B \subseteq M$ is a submodule, and $B = F[x+y, xy]$, which is interesting because it has degree 2.

After all of this setup, what are the quotient modules? M/B is the module of all anti-symmtric polynomials, or those in which $f(x,y) = -f(y,x)$, because every polynomial in two variables can be written uniquely as the sum of a symmetric and an anti-symmetric polynomial. A basis for this (as a vector space) is $\{x^a y^b - x^b y^a, a < b\}$. This is also an A-module, but not a ring, because the product of two antisymmetric polynomials is symmetric. (However, the product of a symmetric and an anti-symmetric polynomial is antisymmetric.)

Then $M/A = F[x,y]/F[x+y]$ as an A-module. Now, let $u = x+y$ and $v = x-y$ (which is why $\text{Char}(F) \neq 2$ is necessary, so that this is invertible). Thus, $M/A = F[x+y, x-y]/F[x+y] = F[u,v]/F[u]$. There's still some complexity here: this is a quotient of R-modules, but not vector spaces. Then, one can produce a (vector-spatial) basis: $u^k \mapsto 0$, but v is still a generator, as with all powers of v. uv is also nontrivial, as with $u^m v^n$ with $m,n > 1$. Thus, this module isn't finitely generated anymore.

There's one more module to go: $B/A = F[x+y, xy]/F[x,y]$ as an A-module, with a vector-spatial basis $(x+y)^m (xy)^n$, but $x+y \mapsto 0$ and $1 \mapsto 0$, so $m > 1$ is required, similarly to the previous case.

Once again, there is a chage of basis, so $B/A \cong F[u, (u^2 - v^2)/4]/F[u] \cong F[u, v^2]/F[u]$ (since $u^2 = 0$) as an $F[u]$-module. Thus, B/A is generated by v^2 and its powers. Similarly, $(M/A)/(B/A) = (v, v^2, v^3, \ldots)/L(v^2, v^4, \ldots)$, so it has an $F[u]$-module basis $\{v, v^3, v^5, \ldots\}$.

Finally, all of these can be considered as B-modules. M/B is generated by $\{v\}$ as a free B-module, so the symmetric and antisymmetric functions are isomorphic as modules, but not as rings.

Corollary 3.1. *As an $F[x+y]$-module, the antisymmetric polynomials in 2 variables x and y are generated by $x-y$.*

While the above example may be slightly confusing, it's at least more interesting than counting mod 60.

Recall the Fourth Isomorphism Theorem: that if $N \subseteq M$ as modules, then there is a one-to-one correspondence ϕ between submodules $S \subseteq M$ containing N and submodules of M/N given by $S \mapsto S/N$.[5] Unlike the other isomorphism theorems, this is an *a priori* statement about sets, but it has more structure: ϕ is an isomorphism of lattices; that is, $\phi(S+T) = \phi(S) + \phi(T)$ and $\phi(S \cap T) = \phi(S) \cap \phi(T)$ for all $N \subseteq S, T \subseteq M$. This isn't a hard theorem to prove; just take each part and kill it.

Example 3.3. Take $R = \mathbb{Z}[x]$ and $M = R$, so that M is an R-module over itself. Let $N = L(x^3 - 2x + 1) \subseteq M$ as modules (which might more normally be written $N = \text{span}(x^3 - 2x + 1)$). Then, $M/N \cong \text{span}(1, x, x^2)$, since $x^3 \mapsto 2x - 1$.

As an abelian group, this is isomorphic to $\mathbb{Z}^3$ as an abelian group (i.e. the free abelian group with 3 generators). As an R-module, it only has one generator, and can be given a module structure $x[x^2] = [x^3] = [2x-1]$. Then, the Fourth Isomorphism Theorem says that submodules of M/N correspond to submodules of $\mathbb{Z}[x]$ which contain $x^3 - 2x + 1$. These are $M = \mathbb{Z}[x]$, $L(x-1)$, and $L(x^3 + x - 1)$. What are the submodules of M/N? It's hard to tell without the theorem.

[4] A more thorough treatment of symmetric polynomials was given in Math 121.

[5] This obscures a slightly complex, but easy, proof that $S/N \subseteq M/N$ as modules.

This example skipped over a couple of weird details, but that would require delving into a bit of algebraic geometry.

It is important to distinguish between the sum $A+B$ for submodules $A,B\subseteq M$ with the more general direct sum: given any two R-modules X and Y, one can form $X\oplus Y=\{(x,y)\mid x\in X, y\in Y\}$, with addition and scalar multiplication componentwise: $r(x,y)=(rx,ry)$. $X\oplus Y$ is also an R-module. Sometimes, people say that $M=U\oplus V$ for $U,V\subseteq M$ as modules, but this requires $U\cap V=0$, or it won't work. If this does hold, then $U+V\cong U\oplus V$.

4. Universal Properties: 4/11/13

Universal properties give lots of useful ways to describe modules. The goal is to ask whether there exists a module that satisfies some property. Sometimes, this is sufficient to also imply uniqueness.

Definition. Let A be a commutative ring, M and N be A-modules, and X be some set. Then, suppose $\varphi_M: X\to M$ and $\varphi_N: X\to N$ are maps of sets. The universal property is that there exists a unique A-module homomorphism $f: M\to N$ such that the following diagram commutes:

$$\begin{array}{ccc} X & \xrightarrow{\varphi_M} & M \\ & \searrow^{\varphi_N} & \downarrow f \\ & & N \end{array}$$

(that is, $f\circ\varphi_M=\varphi_N$ as set maps). If M satisfies this condition, then M is said to be a free module on X.

Claim. Any two free modules on a set X are isomorphic.[6]

Proof. Suppose F and F' are both free modules on a set X:

$$\begin{array}{ccc} X & \xrightarrow{\varphi_F} & F \\ & \searrow^{\varphi_{F'}} & \uparrow g \downarrow f \\ & & F' \end{array}$$

By the universal property, there exists a unique $f: F\to F'$ such that $f\circ\varphi_F=\varphi_{F'}$, and since F' is also free, then there exists a unique map $g: F'\to F$ such that $g\circ\varphi_{F'}=\varphi_F$. Then,

$$\begin{array}{ccc} X & \xrightarrow{\varphi_F} & F \\ & \searrow^{\varphi_F} & \downarrow g\circ f \\ & & F \end{array}$$

$g\circ f\circ\varphi_F=g\circ\varphi_{F'}=\varphi_F$, so $g\circ f$ makes the diagram commute, but so does id_F. By the uniqueness clause, $g\circ f=\mathrm{id}_F$. The same logic in the other directon shows that $f\circ g=\mathrm{id}_{F'}$, so $F\cong F'$. ⊠

Claim. If $X=\{x\}$, then A is a free A-module on X, with $\varphi_A: X\to A$ given by $\varphi_A(x)=1$.

Proof. If M is any A-module, then $\varphi_M:\{x\}\to M$ is given by choosing some $m\in M$, such that $\varphi_M(x)=m$.

$$\begin{array}{ccc} \{x\} & \xrightarrow{\varphi_A} & A \\ & \searrow^{\varphi_M} & \downarrow f \\ & & M \end{array}$$

For the map $f: A\to M$, $f(1)=m$. This can be extended to $f(a)=am$ for any $a\in A$. This is forced, because $f(a)=f(a\cdot 1)=af(1)=am$. ⊠

For an arbitrary set X, let $F_X=\{f: X\to A$ such that $f(x)$ is nonzero for only finitely many $x\}$, or the set of finitely supported functions $X\to A$. Then, F_X is an A-module, and there exists a function $\varphi_{F_X}: X\to F_X$ such that $\varphi_{F_X}(x)=f_x$, where $f_x(x)=1$ and $f_x(x')=0$ when $x'\neq x$. If M is another A-module, then take $\theta(f)=\sum_{x\in X} f(x)\varphi_{F_M}(x)$. Since f has finite support, then this sum makes sense, and $\theta(f_x)=\varphi_M(x)$. Thus, θ makes the following diagram commute:

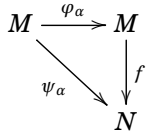
$$\begin{array}{ccc} X & \xrightarrow{\varphi_{F_X}} & F_X \\ & \searrow^{\varphi_M} & \downarrow \theta \\ & & M \end{array}$$

[6] Notice that existence hasn't been shown yet. We'll get to this shortly, but it's an important thing to keep in mind — legend has it that long ago at a Princeton thesis defense, someone has proved the uniqueness of some solution to a system of equations, but someone then pointed out it had no solutions...

Furthermore, it is unique: every $f \in F_X$ can be written as an A-linear combination of the f_x: $f = \sum_{x \in X} f(x) f_x$. Since f has finite support, this is a finite sum, so the value of θ is determined by its value on the elements f_x. Since $f_x \mapsto \varphi_M(x)$ is determined, then the whole function is. Thus, free modules in general exist, and are unique up to isomorphism.

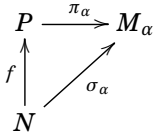
Section 10.3 of the textbook has lots of examples of universal constructuions:

(1) Suppose $\{M_\alpha\}_{\alpha \in A}$ is a family of modules. Then, define their sum to be a module M equipped with inclusion homomrphisms $M_\alpha \xrightarrow{\varphi_\alpha} M$. Then, the universal property is that if N is some other module with $M_\alpha \xrightarrow{\psi_\alpha} N$, then there should exist a unique $f : M \to N$ such that $f \circ \varphi_\alpha = \psi_\alpha$ for all $\alpha \in A$.



This universal property has a solution, which is contained within the direct product as sets, but in which only finitely many of the coordinates in any given element are nonzero.

(2) Taking $\{M_\alpha\}_{\alpha \in A}$ to again be a family of modules, their product is a module P such that there exist maps $\pi_\alpha : P \to M_\alpha$ for all α such that if N is another module with $N \xrightarrow{\sigma_\alpha} M_\alpha$ for all α, then the following diagram commutes:



(i.e. $\pi_\alpha \circ f = \sigma_\alpha$ for all α). This has the solution $\prod_{\alpha \in A} M_\alpha$, their direct product as sets.

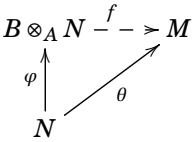
For example, the sum over $\mathbb{N}$ of copies of A is the set of finitely supported functions $\mathbb{N} \to A$, and the product is all function $\mathbb{N} \to A$.

There's another, more subtle one, leading to the notion of tensor product. In vector spaces, one has the tensor product of F^m and F^n, which is an mn-dimensional vector space $F^m \otimes F^n$ given by a basis in one-to-one correspondence with products of basis elements for F^m and F^n.

Let A be a ring and $A \to B$ be a ring homomorphism, and let M be a B-module. Any B-module becomes an A-module by restriction of scalars; $B \times M \to M$ can be restricted to $A \times M \to M$.

Then, turn it around: if N is an A-module, then can it be obtained by restriction of scalars from a B-module? In general, there's no reason for this to be so: if $A = \mathbb{Z}$, $B = \mathbb{Q}$, and $f : \mathbb{Z} \hookrightarrow \mathbb{Q}$ is given by inclusion, is $\mathbb{Z}$ obtained from restriction of $\mathbb{Q}$? In any $\mathbb{Q}$-module, every element is uniquely divisible by any number because multiplication by $1/n$ is allowed, but this causes issues with $\mathbb{Z}$. But there might be a best possible approximation, some sort of universal B-module that is a restriction of sorts.

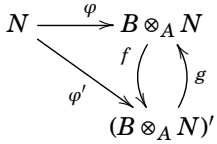
The universal property in quetion is if N is an A-module and M is a B-module taken as an A-module by restriction of scalars, then, there exists a B-module $B \otimes_A N$ such that if $\theta : M \to N$ is an A-module homomorphism, and $\varphi : N \to B \otimes_A N$ is a homomorphism of A-modules (viewing $B \otimes_A N$ as an A-module by restriction of scalars), then there exists a unique f such that this diagram commutes:



Here, f is a homomorphism of B-modules. Additionally, φ has the property that for any homomorphism $\psi : N \to M$, there is a unique homomorphism $f : B \otimes_A N \to M$ of B-modules such that $f \circ \varphi = \psi$.

This is a useful construction: if one takes the $\mathbb{Z}$-module $N = \mathbb{Z}^n \oplus \mathbb{Z}/n_1 \oplus \cdots \oplus \mathbb{Z}/n_k$, then it turns out that $\mathbb{Q} \otimes_{\mathbb{Z}} N = \mathbb{Q}^n$, so all of the torsion is wiped out once you go up to $\mathbb{Q}$.

Now, let's consider existence and uniqueness: suppose $B \otimes_A N$ and $(B \otimes_A N)'$ are both solutions to this universal problem. Then, they are both B-modules and have maps from N as A-modules:



Thus, there are (as in the free case) maps $f : B \otimes_A N \to (B \otimes_A N)'$ and $g : (B \otimes_A N)' \to B \otimes_A N$, and it can be shown that $f \circ g = g \circ f = \mathrm{id}$, so $B \otimes_A N \cong (B \otimes_A N)'$, which implies uniqueness.

Existence is a tougher nut to crack: take the free $\mathbb{Z}$-module (free abelian group) on all pairs (b,n) with $b \in B$, $n \in N$. This is a huge construction, since all of the elements of the product of B and N are just taken as a basis! This group, $F(B \times N)$, isn't the solution, but given any B-module M and homomorphism of A-modules $j : N \to M$, there exists a homomorphism $F(B \times N) \xrightarrow{\theta} M$ such that $\theta(b,n) = b \cdot j(n)$.

There are lots of properties we still need, so a subgroup which encodes the necessary information will be found. Specifically, take $K < F(B \times N)$, generated by elements of the form $(b_1 + b_2, n) - (b_1, n) - (b_2, n)$. Then, by distributivity, $\theta(K) = 0$. Thus, $F(B \times N)/K$ is still meaningful. The same thing works with elements of the form $(b, n_1 + n_2) - (b, n_1) - b(n_2)$ and $(ba, n) - (b, an)$, so throw these into K as well. These will all go to zero, so formally define K as the subgroup generated by all of them.

Claim. $F(B \times M)/K = F$ satisfies the existence question for $B \otimes_A N$.

Proof. Define $b'[(b,n)] = (b'b, n)$. This can be defined on a pre-coset level, but it's also necessary to check that F/K is a B-module:

(1) $(b_1 + b_2)(b,n) = b_1(b_1,n) + b_2(b_1 n)$.
(2) $((b_1 + b_2)b_1 n) = (b_1 b, n) + (b_2 b, n)$.

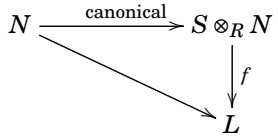
These two properties don't hold in $F(B \times N)$, but their differences were zeroed out as the quotient! The third condition guarantees that $n \mapsto (1,n)$ is a map of A-modules.

With regards to universality, f is already determined on elements of the form $(1,n)$ by the previous sentence, but everything in $F(B \times N)/K$ is generated as a B-module by the image of N, so f is uniquely determined if it exists. But for existence, we have only to check that the above homomorphism $f : F(B \times N) \to B \times N$ vanishes on K, which is immediate. ⊠

5. The Tensor Product: 4/16/13

Dr. Muellner gave today's lecture again.

Recall the universal property for the tensor product: if $R \subseteq S$ is a subring and N is a left R-module, there exists a map $N \to S \otimes_R N$, sending $u \mapsto 1 \otimes u$, such that if L is any other S-module, then there is a unique S-module map f such that the followng diagram commutes:



where $N \to L$ is a map of R-modules. This notation is heavily compressed, so review it to make sure it isn't too confusing. However, there is an immediate generalization: R isn't required to be a subring of S; there just needs to be a map between them.

Example 5.1.

- $R \otimes_R N \cong N$, by the trivial extension of scalars.
- If A is a finite abelian group, then $\mathbb{Q} \otimes_{\mathbb{Z}} A = 0$.

  Proof. If $n = |A|$, then $\mathbb{Q} \otimes_{\mathbb{Z}} A$ is generated by $\{p/q \otimes a\}_{p/q \in \mathbb{Q}, a \in A}$ with relations
  $$\frac{p}{q} \otimes a = \frac{pn}{qn} \otimes na = \frac{p}{qn} \otimes 0 = 0,$$
  so the module itself is zero. ⊠

There are lots of different flavors of tensor product, defined for left or right modules, connutative rings, vector spaces, R-algebras, and so on.

Definition. Let M be a right R-module and N be a left R-module. Then, the tensor product $M \otimes_R N$ is defined as the free abelian group on the set $M \times N$, or $\mathbb{Z}^{M \times N}$, quotiented out by the submodule generated by all elements of the form $(m_1 + m_2, n) - (m_1, n) - (m_2, n)$, $(m, n_1 + n_2) - (m, n_1) - (m, n_2)$, and $(mr, n) - (m, rn)$ for $m, m_1, m_2 \in M$ and $n, n_1, n_2 \in N$.

The free abelian group is huge and has no algebraic structure, so the quotient brings the useful properties back. Additionally, the notation $M \otimes_R N$ is helpful: it illustrates that in general, it is only possible to multiply by r on the right in M and on the left in N. If M is a ring and $R \subseteq M$ as a subring, then this returns to the previous case.

In this more general construction, $M \otimes_R N$ is an abelian group, but multiplication by R on either side isn't always defined.[7] In this group, the coset of (m,n) is denoted $m \otimes n$. By the free property, every element in $M \otimes_R N$ is a finite $\mathbb{Z}$-linear combination of these "simple tensors" $m \otimes n$.

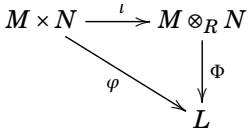
[7] One could try to define an R-module structure on $M \otimes_R N$ given by $r(m \otimes n) = mr \otimes rn$, but this only works if R is commutative.

Definition. Let M be a right R-module and N be a left R-module. If L is an abelian group, then a set map $M \times N \xrightarrow{\varphi} L$ is called R-balanced if:

- $\varphi(m_1 + m_2, n) = \varphi(m_1, n) + \varphi(m_2, n)$,
- $\varphi(m, n_1 + n_2) = \varphi(m, n_1) + \varphi(m, n_2)$, and
- $\varphi(mr, n) = \varphi(m, rn)$.

In some sense, this means that φ satisfies the tensor product properties. There is a canonical map (in that it doesn't require any choices) $\iota : M \times N \to \mathbb{Z}^{M \times N} \to M \otimes_R N$ that sends $(m,n) \mapsto 1 \cdot (m,n) \mapsto m \otimes n$. This is an R-balanced map because the conditions required are built into $M \otimes_R N$.

In the more general formulation of the tensor product, the universal property is that for any abelian group L and R-balanced map $M \times N \xrightarrow{\varphi} L$, there is a unique abelian group homomoprhism $\Phi : M \otimes_R N \to L$ such that $\varphi = \Phi \circ \iota$:



Corollary 5.1.

(1) Given Φ, the composition $\varphi = \Phi \circ \iota$ is R-balanced.

(2) Given an R-balanced map φ as above, there exists a unique group homomorphism Φ, so there is a one-to-one correspondence between R-balanced maps $M \times N \to L$ and group homomoprhisms $M \otimes_R N \to L$.

Proof. Part 1 is just given by checking structure, so here is the proof of Part 2:

Given some $\varphi : M \times N \to L$, defined $\tilde{\varphi} : \mathbb{Z}^{M \times N} \to L$ (using the universal property on free abelian groups) given by $(m,n) \mapsto \tilde{\varphi}(m,n)$. Since this is defined on the generators of $\mathbb{Z}^{M \times N}$, then it is well-defined. Additionally, since φ is R-balanced, then $\tilde{\varphi}$ maps all of the defining relations of the tensor product to zero: for example, $\tilde{\varphi}((mr,n) - (m,rn)) = \tilde{\varphi}(mr,n) - \tilde{\varphi}(m,rn) = 0$.

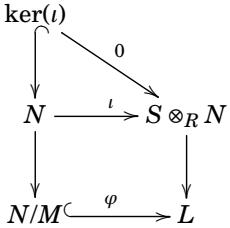
Thus, $\tilde{\varphi}$ induces a well-defined homomorphism on the quotient $\Phi : M \otimes_R N \to L$, and checking the commutativity of the diagram isn't so hard. Uniqueness is given because $M \otimes_R N$ is uniquely generated my $m \otimes n$ and linear extensions, and Φ is uniquely determined on the generators, so Φ is unique. ⊠

In the special case where M is a free module over R generated by $\{m_i\}_{i \in I}$ and $S \supseteq R$ as rings, then $S \otimes_R M$ is a free S-module, generated by $\{1 \otimes m_i\}_{i \in I}$. Thus, if they are finitely generated, then they have the same rank. Here, $M \subseteq S \otimes_R M$ as a submodule in some cases, but recall that if A is a finite abelian group then $\mathbb{Q} \otimes A = 0$.

Theorem 5.2. *Let $\iota : N \to S \otimes_R N$, $n \mapsto 1 \otimes n$ be the canonical map. Then, $N/\ker(\iota)$ is the unique largest quotient of N that can be embedded in any S-module.*

This can understood by choosing an example: finite abelian groups can't be embedded in $\mathbb{Q}$, and the free modules have $\ker(\iota) = 0$, so they can be embedded.

Proof of Theorem 5.2.



First, observe that $N/\ker(\iota)$ can be embedded into the S-module $S \otimes_R N$, since the non-injectiveness was modded out. Then, let $M \subseteq N$ be a submodule and $\varphi : N/M \hookrightarrow L$ be an injection of modules. Then, the universal property gives the above diagram, so $\ker(\iota) \subseteq M$, and therefore N/M is a quotient of $N/\ker(\iota)$. Thus, $N/\ker(\iota)$ is the unique largest quotient with the properties stated. ⊠

Corollary 5.3. *N can be embedded as an R-submodule of some S-module if $\ker(\iota) = 0$. (Otherwise, N would be larger than the unique largest quotient.)*

Definition. An (R,S)-bimodule M is a set M that is a left R-module and a right S-module such that $(rm)s = r(ms)$ for all $r \in R$, $s \in S$, and $m \in M$.

This definition is exactly what one would expect: it's a module in both senses, and the structures are compatible.

Example 5.2. $M \otimes_S N$ has a left R-module structure given by $r(m \otimes n) = (rm) \otimes n$. It's nontrivial to show that this is well-defined, however. There are lots of ways to get additional structure on the tensor product: for example, if M is a right R-module and N is an (R,S)-bimodule, then $M \otimes_R N$ is a right S-module in the obvious way. If R is commutative, then there is no difference between left and right R-modules, so $M \otimes_R N$ can be made into an R-module.

The moral of today's lesson is that, though universal products seem very abstract, the tensor product is a concrete object in which one can do calculations. For example, in $\mathbb{Z}/12 \otimes \mathbb{Z}/20$, $5 \otimes 2 = 1 \otimes 10 = 10 \otimes 1 = -2 \otimes 1$ and $7 \otimes 3 = (5 \cdot 11) \otimes 3 = 5 \otimes 30 + 5 \otimes 3 = 10 \otimes 15 - 7 \otimes 3$.

Lemma 5.4. $\mathbb{Z}/m \otimes \mathbb{Z}/n \cong \mathbb{Z}/\gcd(m,n)$.

For a proof of this, see the book.

6. More Tensor Products: 4/18/13

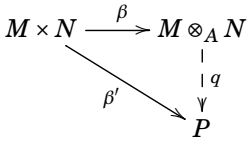
The statement "B is an A-algebra" means that there exists a ring homomorphism $A \to B$. Though noncommutative rings will be discussed later this quarter for representation theory, for now assume all rings are commutative. However, it will always be assumed that rings have a 1.

Consider the function $M \times N \to F(M \times N) \to M \otimes_A N$, where M and N are A-modules, and call the composite $\beta : (m,n) \mapsto m \otimes n$. Here are some of its properties:

- $\beta(m_1 + m_2, n) = \beta(m_1, n) + \beta(m_2, n)$.
- $\beta(m, n_1 + n_2) = \beta(m, n_1) + \beta(m, n_2)$.
- $\beta(am, n) = \beta(m, an) = a\beta(m, n)$.

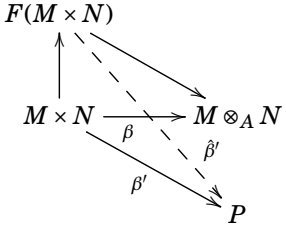
β is not a homomorphism, but if one variable is fixed, then it is a homomorphism with respect to the other. Thus, β is called A-bilinear, since it is linear with respect to each variable when the other is fixed.

Showing that $M \otimes_A N$ satisfies a universal property is useful because it allows one to prove things about it using just maps, rather than dealing explictly with the elements. For example, suppose P is an A-module and $\beta' : M \times N \to P$ is A-bilinear. Then, the universal condition is that there exists a unique homomorphism $q : M \otimes_A N \to P$ such that $q \circ \beta = \beta'$:



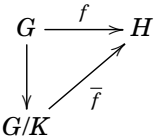
Notice that q can't be bilinear, since it's a function of one variable, but also that a linear map composed with a bilinear map is bilinear.

It can be shown that $M \otimes_A N = F(M \times N)/K$ satisfies this property:



Since β' is a set map $M \times N \to P$, then β' extends uniquely to an abelian group homomorphism $\hat{\beta}' : F(M \times N) \to P$ by the universal property of free abelian groups. Then, to prove the property, it will be necessary to show that $\hat{\beta}'$ vanishes on K, but this is simple: since β is A-bilinear, then $\hat{\beta}'$ vanishes on elements of type $(m_1 + m_2, n) - (m_1, n) - (m_2, n)$, etc. Thus, the required map $q : M \otimes_A B \to P$ exists.

This uses the fact that if $G \xrightarrow{f} H$ as abelian groups and $f|_K = 0$ for $K \leq G$, then there exists an $\overline{f} : G/K \to H$ such that the following diagram commutes:



Uniqueness of q follows as well: since every element in $F(M \times N)$ is of the form $\sum_{i=1}^{k}(m_i, n_i)$, then everything in $M \otimes_A N$ can be written as $\sum_i m_i \otimes n_i$. Thus,

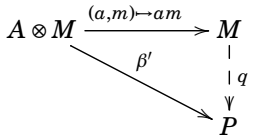
$$q\left(\sum_i m_i \otimes n_i\right) = \sum_i q(m_i \otimes n_i) = \sum_i \beta'(m_i, n_i),$$

so q is unique.

The tensor product is such a huge construction that it is worth seeing some examples.

Proposition 6.1. *If M is an A-module, then $A \otimes_A M \cong M$ as A-modules.*

Proof. The goal is to show that M is an appropriate choice in the following diagram:



Then, $\beta'(1, m_1 + m_2) = \beta'(1, m_1) + \beta'(1, m_2)$, so one obtains an abelian group homomorphism $M \to P$, since it specifies where 1 goes, and $\beta'(1, am) = a\beta'(1, m) = \beta'(a, m)$, so it becomes an A-module homomorphism, so $M \to A \times M$ given by $m \mapsto (1, m)$ makes everything work, and if $\theta : M \to A \times M \xrightarrow{\beta'} P$, then θ makes the diagram commute. ⊠

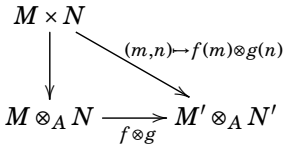
Proposition 6.2. *$M \otimes_A (N_1 \oplus N_2) \cong (M \otimes_A N_1) \oplus (M \otimes_A N_2)$, so that the tensor product distributues with direct sums. Similarly, $(M_1 \otimes_A M_2) \oplus N \cong (M_1 \otimes_A N) \oplus (M_2 \otimes_A N)$.*

Corollary 6.3. *Suppose M and N are free A-modules: $M = A^r$ and $N = A^s$ (e.g. vector spaces). Then, $A^r \otimes_A A^s \cong A^{rs}$.*

Proof. Proposition 6.2 can be generalized inductively to k-fold direct sums, so $A^r \otimes_A A^s \cong (A^r)^s = A^{rs}$. ⊠

Thus, for vector spaces, $\dim(V \otimes W) = \dim(V)\dim(W)$.

Remark (Functoriality of the tensor product)**.** Let M, N, M', N' be A-modules. Then, if $f : M \to M'$ and $g : N \to N'$ are A-module homomorphisms, then there exists an A-module homomorphism $f \otimes g : M \otimes_A N \to M' \otimes_A N'$ given by $f \otimes g(\sum m_i \otimes n_i) = \sum f(m_i) \otimes g(n_i)$. This is called functoriality because it respects transformations: $(m, n) \mapsto f(m) \otimes g(n)$ is clearly bilinear, so $f \otimes g$ makes the following diagram commute:



Proof of Proposition 6.2. There must be a map $(M \otimes_A N_1) \oplus (M \otimes_A N_2) \to M \otimes_A (N_1 \oplus N_2)$, because there are maps on the components $\mathrm{id} \otimes \iota_1 : M \otimes_A N_1 \to M \otimes_A (N_1 \oplus N_2)$ and $\mathrm{id} \otimes \iota_2 : M \otimes_A N_2 \to M \otimes_A (N_1 \oplus N_2)$ given by $n_1 \mapsto (n_1, 0)$ and $n_2 \mapsto (0, n_2)$. Then, the goal is to show that for any $\varphi : (M \otimes_A N_1) \oplus (M \otimes_A N_2) \to P$, for any A-module P, there exists a $\hat{\varphi} : M \otimes_A (N_1 \oplus N_2) \to P$ that commutes with (ι_1, ι_2).

Take the maps $\beta_1 : M \times N_1 \to P$ and $\beta_2 : M \times N_2 \to P$, which are A-bilinear. Then, there is a $\beta : M \times (N_1 \oplus N_2) \to P$ by $m\beta(m_1, (n_1, n_2)) = \beta_1(m, n_1) + \beta_2(m, n_2)$, and there's a correspondence going the other way: given β, one has $\beta_1(m, n_1) = \beta(m, (n_1, 0))$ and similarly for β_2. Since the data needed to make the homomorphisms is the same, then they are isomorphic. ⊠

Proposition 6.4. *The tensor product is associative up to isomorphism: if M, N, and P are A-modules, then $M \otimes_A (N \otimes_A P) \cong (M \otimes_A N) \otimes_A P$.*

Proof. Exercise in universal properties. Notice that the homomorphism is the same as a trilinear map out of $M \times N \times P$ (i.e. linear in each variable as the other two are fixed).

Exact sequences can sometimes be used to compute tensor products, but this will require more generality. Recall that a presentation of an A-module M is a homomorphism $f : A^n \to A^m$ such that $M \cong A^m \operatorname{Im}(f)$, and f is just represented by a matrix with entries in A, so this is a useful and common way to describe a module (since all modules have a presentation, even though not all of them are finitely generated). This allows something interesting to be said about modules: because of the distributivity property, $A^n \otimes_A N \cong \left(\bigoplus_{i=1}^n A\right) \otimes_A N \cong \bigoplus_{i=1}^n N$, so $M \otimes_A N$ can be described as the quotient of $A^m \otimes_A N$ by the image of $f \otimes \mathrm{id}_N$. This result is powerful, but its proof will be deferred.

Example 6.1. To compute $\mathbb{Z}/17 \otimes \mathbb{Z}/35$, because a presentation for $\mathbb{Z}/17$ is $\times 17 : \mathbb{Z} \to \mathbb{Z}$ (multiplying by 17), so $\mathbb{Z}/17 \otimes \mathbb{Z}/35$ is isomorphic to the quotient of $\times 17 : \mathbb{Z}/35 \to \mathbb{Z}/35$. Since 17 and 35 are coprime, then 17 is a unit in $\mathbb{Z}/35$, so $(\times 17)$ is surjective, and therefore $\mathbb{Z}/17 \otimes \mathbb{Z}/35 = 0$.

Example 6.2. Let $A = \mathbb{Q}[x]$ and take $A/(x^2 - 1)$ and $A/(x^3 - 3x + 2)$. These are A-algebras, but take them as modules for now. $A \to A$ given by multiplication by $x^2 - 1$ is a presentation of $A/(x^2 - 1)$, so take $A/(x^2 - 3x + 2) \to A/(x^2 - 3x + 2)$ can be given with the same map. Since $x^2 - 3x + 2 = (x - 1)(x - 2)$, then $(x^2 - 3x - 2) = (x - 1) \cap (x - 2)$ in A, and $A/(x^2 - 3x + 2) \cong \mathbb{Q} \oplus \mathbb{Q}$

given by $x \mapsto 1$ and $x \mapsto 2$, respectively (e.g. by the Chinese Remainder theorem). Thus, $x^2-1=(x-1)(x-2)$ is mapped to $(0,3)$, so there is something left, since 3 isn't a unit in $\mathbb{Z}$. Thus, $A/(x^2-1)\otimes A/(x^2-3x-2)\cong \mathbb{Q}[x]/(x-1)\cong \mathbb{Q}$.

Suppose M has a presentation $f: A^n \to A^m$, and let $\theta: A^m/\mathrm{Im}(f) \xrightarrow{\sim} M$ be the isomorphism. This can be packaged as a sequence $A^n \xrightarrow{f} A^m \xrightarrow{\theta\circ\pi} M$. The condition that this is a presentation is that $\mathrm{Im}(f)=\mathrm{Ker}(\theta\circ\pi)$, or that $\theta\circ\pi\circ f=0$.

Definition. A pair of composable homomorphisms $M \xrightarrow{f} N \xrightarrow{g} P$ is exact (at N) if $g\circ f=0$ and $\mathrm{Ker}(g)=\mathrm{Im}(f)$.

This is a very useful concept, and will resurface throughout the course. For example, if $M \xrightarrow{f} N \to 0$ is exact, then f is surjective (and vice versa), and $0 \to M \xrightarrow{f} N$ is exact iff f is injective. One can define longer exact sequences $M_n \to M_{n-1} \to \cdots \to M_1 \to M_0$, which is defined to be exact if each of the composites $M_{i+1} \to M_i \to M_{i-1}$ are. This can even be done for infinite sequences.

Exercise 6.1. Suppose $0 \to V \to W \to U \to 0$ is exact, where U, V, and W are finite-dimensional vector spaces. If $\dim(V)=m$ and $\dim(U)=n$, then what is $\dim(W)$?

7. Exact Sequences: 4/23/13

Definition. A short exact sequence is an exact sequence of the form $0 \to M \xrightarrow{f} N \xrightarrow{g} P \to 0$ (i.e. f is injective, g is surjective, and $\ker(g)=\mathrm{Im}(f)$).

Example 7.1.

a. If M and N are A-modules, then

$$0 \longrightarrow M \xrightarrow{m\mapsto(m,0)} M\oplus N \xrightarrow{(m,n)\mapsto n} N \longrightarrow 0$$

is exact. This is called a split sequence.

b. $0 \to \mathbb{Z}/p \to \mathbb{Z}/p^2 \to \mathbb{Z}/p \to 0$, where the maps are respectively $1 \mapsto p$ and reduction mod p. This sequence is not split, because if it were, then $\mathbb{Z}/p^2 \cong \mathbb{Z}/p\oplus\mathbb{Z}/p$, which is not the case.

A criterion for a split sequence is that if $0 \to M \to P \xrightarrow{\pi} N \to 0$ splits, then $P \cong M\oplus N$, so there exists a map $s: N \to P$ such that $\pi\circ s=\mathrm{id}_N$. Then, the map s is called a section. Notice that this cannot happen in part b of Example 7.1, because it would require 1 to be sent to an element of order p.

Proposition 7.1. *A short exact sequence*

$$0 \longrightarrow M \xrightarrow{i} P \xrightarrow{\pi} N \longrightarrow 0 \tag{1}$$

splits iff there exists a homomorphism $s: N \to P$ such that $\pi\circ s=\mathrm{id}_N$. In this case, s is called a section.

Digression (Morphisms of Sequences)**.** Given any two short exact sequences $0 \to M \to P \to N \to 0$ and $0 \to M' \to P' \to N' \to 0$, a map between them is a triple of morphisms $f: M \to M'$, $g: P \to P'$, and $h: N \to N'$ such that the following diagram commutes:

$$\begin{array}{ccccccccc} 0 & \longrightarrow & M & \xrightarrow{i} & P & \xrightarrow{\pi} & N & \longrightarrow & 0 \\ & & \downarrow{\scriptstyle f} & & \downarrow{\scriptstyle g} & & \downarrow{\scriptstyle h} & & \\ 0 & \longrightarrow & M' & \xrightarrow{i'} & P' & \xrightarrow{\pi'} & N' & \longrightarrow & 0 \end{array}$$

Specifically, it is required that $gi=i'f$ and $h\pi=\pi'g$. If f, g, and h can be inverted, then this is an isomorphism.

Definition. A short exact sequence $0 \to M \to P \to N \to 0$ is split if it is isomorphic to $0 \to M \to M\oplus N \to N \to 0$.

Proof of Proposition 7.1. If (1) is split, then it is isomorphic to $0 \to M \to M\oplus N \to N \to 0$, so the section is given by $s(n)=(0,n)$. Thus, suppose conversely that there exists a section $s: N \to P$. Along with $i: M \to P$, this is just the data needed to give a homomorphism of modules $\sigma=i+s: M\oplus N \to P$.

Then, the goal is to show that σ is an isomorphism. Take a $p \in P$ and consider $\pi(p) \in N$. Thus, $s\pi(p) \in P$, and $\pi(p-s\pi(p))=0$, since $\pi s=\mathrm{id}$. This means that $p-s\pi(p) \in \mathrm{Im}(i)$, or $p-s\pi(p)=i(m)$ for some $m \in M$, or $p=i(m)-s\pi(p)=\sigma(m,\pi(p))$. Thus, σ is surjective.

Now, suppose (m,n) is such that $\sigma(m,n)=0$ in P. Then, since $\pi\circ i=0$, then $\pi\sigma(,mn)=0$, but also $\pi\sigma(m,n)=\pi i(m)+\pi s(n)=n$. Thus, $n=0$, so everything is of the form $\sigma(m,0)=i(m)$. However, i is injective, so σ must be as well. Thus, σ is an isomorphism.

It remains to check that

$$\begin{array}{ccccccccc} 0 & \longrightarrow & M & \longrightarrow & M \oplus N & \longrightarrow & N & \longrightarrow & 0 \\ & & \downarrow{\scriptstyle \mathrm{id}} & & \downarrow{\scriptstyle \sigma} & & \downarrow{\scriptstyle \mathrm{id}} & & \\ 0 & \longrightarrow & M & \xrightarrow{i} & P & \xrightarrow{\pi} & N & \longrightarrow & 0 \end{array}$$

commutes, but this is not difficult. ⊠

For another example, let $\varphi : M \to N$ be any A-module homomorphism. Then, $0 \to \ker(\varphi) \to M \to \mathrm{Im}(\varphi) \to 0$ is a canonical exact sequence.

Finally, let F be a free module. Then, a short exact sequence $0 \to K \to F \to M \to 0$ is called a presentation of M: F encodes the generators, and K the relations (the homomorphism $K \to F$ provides information about how the generators interact).

Lemma 7.2 (Short Five Lemma)**.** *Suppose*

$$\begin{array}{ccccccccc} 0 & \longrightarrow & M & \xrightarrow{i} & P & \xrightarrow{\pi} & N & \longrightarrow & 0 \\ & & \downarrow{\scriptstyle f} & & \downarrow{\scriptstyle g} & & \downarrow{\scriptstyle h} & & \\ 0 & \longrightarrow & M' & \xrightarrow{i'} & P' & \xrightarrow{\pi'} & N' & \longrightarrow & 0 \end{array}$$

is a map of short exact sequences. Then,

a. *If f and h are injective, then g is injective.*
b. *If f and h are surjective, then g is surjective.*
c. *If f and h are isomorphisms, then so is g.*

Proof. It should be clear that c directly follows from the other two points. As for them:

a. Suppose $p \in P$ and $g(p) = 0$ in P'. Then, $h\pi(p) = \pi' g(p) = 0$, so $\pi(p) = 0$, since H is injective. Thus, $p = i(m)$ for some $m \in M$. But since $gi(m) = 0$ and i' and f are both injective, then $m = 0$, so $p = 0$.
b. Suppose $p' \in P'$. Then, take $\pi' p' = n'$. Since h is surjective, then there exists an $n \in N$ such that $h(n) = \pi'(p')$, and since π is surjective, then there exists a p such that $\pi p = n$. Thus, $h\pi(p) = \pi'(p') = \pi' g(p)$. Then, $\pi'(p' - g(p)) = 0$, so $p' - g(p) = i'(m')$ for some $m' \in M'$. Since f is surjective, there exists an $n \in M$ with $f(m) = m'$, so $i'f(m) = m' = gi(m)$. Therefore $p' = g(p) + g(im)$, so surjectivity follows. ⊠

This proof was an example of diagram chasing, sometimes called abstract nonsense. All of these results generalize to abelian categories (in which kernels and cokernels make sense), which are a generalization of modules.

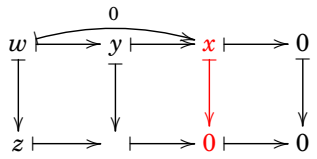
Lemma 7.3 (Five Lemma)**.** *Suppose*

$$\begin{array}{ccccccccccc} A & \xrightarrow{g_1} & B & \xrightarrow{g_2} & C & \xrightarrow{g_3} & D & \xrightarrow{g_4} & E \\ \downarrow{\scriptstyle f_A} & & \downarrow{\scriptstyle f_B} & & \downarrow{\scriptstyle f_C} & & \downarrow{\scriptstyle f_D} & & \downarrow{\scriptstyle f_E} \\ A' & \xrightarrow{g_1'} & B' & \xrightarrow{g_2'} & C' & \xrightarrow{g_3'} & D' & \xrightarrow{g_4'} & E' \end{array}$$

is exact everywhere and the diagram commutes. If f_A, f_B, f_D, and f_E are isomorphisms, then f_C is as well.

Proof. Injectivity will be shown here; surjectivity is similar and left as an exercise. Suppose $x \in C$ and $f_C(x) = 0$. Then, $g_3' f_C(x) = 0$, so by commutativity, $f_D g_3(x) = 0$, so $g_3(x) = 0$ because f_D is an isomorphism. Thus, x lives in B: there exists a $y \in B$ for which $x = g_2(y)$. Then, $f_C g_2(y) = 0$, and so $g_2' f_B(y) = 0$. Thus, $f_B(y) = g_1'(z)$ for some $z \in A'$, which means that $z = f_A(w)$ for some $w \in A$, because f_A is an isomorphism. Thus, $x = g_2 y = g_2 g_1 w = 0$, so f_C is injective. ⊠

Pictorially, here's a way to look at the proof of injectivity:



Exercise 7.1. Fill in the missing parts of the proof: show that f_C is surjective.

Commutative algebra (both algebraic geometry and algebraic topology) requires being fairly familiar with this stuff, so it's good to be acquainted with it.

Finally, one can classify short exact sequences up to equivalence.

Definition. Two short exact sequences of A-modules $0 \to M \to P \to N \to 0$ and $0 \to M \to P' \to N \to 0$ are equivalent if there is an isomorphism of sequences

$$\begin{array}{ccccccccc} 0 & \longrightarrow & M & \longrightarrow & P & \longrightarrow & N & \longrightarrow & 0 \\ & & \downarrow{\scriptstyle \mathrm{id}_M} & & \downarrow{\scriptstyle \varphi} & & \downarrow{\scriptstyle \mathrm{id}_N} & & \\ 0 & \longrightarrow & M & \longrightarrow & P' & \longrightarrow & N & \longrightarrow & 0 \end{array}$$

This is an equivalence relation, and the set of equivalence classes is called $\mathrm{Ext}^1(M,N)$, and is a very interesting object in homological algebra.

Example 7.2. If $A = \mathbb{Z}$ and $M,N = \mathbb{Z}/p$, let E be a short exact sequence of the form $0 \to \mathbb{Z}/p \xrightarrow{i} P \xrightarrow{\pi} \mathbb{Z}/p \to 0$. Then, construct a number $\xi(E) \in \mathbb{Z}/p$ as follows: choose an $x \in P$ such that $\pi(x) = 1$. Then, $px \in \mathbb{Z}/p$, so define $\xi(E) = px$. This happens to be well-defined: $x = 1 + kp$, so two choices of x differ by a multiple of p: if x, x' satisfy $\pi(x) = \pi'(x') = 1$, then $x - x' = pm$, so $px - px' = p^2 m = 0$. Thus, $[px]$ is a well-defined element in $\mathbb{Z}/p$.

Whenever $\xi(E) \neq 0$, then $P = \mathbb{Z}/p^2$. These sequences aren't all equivalent, though they are isomorphic. If $\xi(E) = 0$, then the sequence splits.

$\mathrm{Ext}^1(M,N)$ is functorial: morphisms $M \to M', N \to N'$ induce a morphism $\mathrm{Ext}^1(M,N) \to \mathrm{Ext}^1(M',N')$.

Example 7.3. If $M = \mathbb{Z}/3$ and $N = \mathbb{Z}/7$, then $0 \to \mathbb{Z}/3 \to P \xrightarrow{\pi} \mathbb{Z}/7 \to 0$. If x is an inverse image of 1, multiply it by 7 to get an element in $\mathbb{Z}/5$. But $15x \equiv x \bmod 7$ and $15x = 0 \in \mathbb{Z}/3$, so there are no nontrivial short exact sequences, and they all split.

Let X be a set and $F_A(X)$ be a free A-module on X. Suppose $\pi : M \to N$ is a surjective homomorphism of A-modules. Then, it turns out that it's possible to lift a homomorphism $F_A(X) \to N$ to one $F_A(X) \to M$. However, this doesn't extend to all modules:

$$\begin{array}{ccc} & & \mathbb{Z}/p^3 \\ & \nearrow & \downarrow \\ \mathbb{Z}/p^2 & \longrightarrow & \mathbb{Z}/p \end{array}$$

doesn't lift, because sending $p \to 0$ has unfortunate consequences. In general, this is pretty tricky, but an A-module P is called projective if for any A-modules M and N and map $P \to N$, the lift

$$\begin{array}{ccc} & & M \\ & \nearrow & \downarrow \\ P & \longrightarrow & N \end{array}$$

always exists.

Proposition 7.4. *A module P is projective iff it is a summand in a free module: $P \oplus P' = F$ for a free module F.*

Proof. There always exists a map $F \xrightarrow{\pi} P$ (for example, take $F = F(P)$), so in the diagram

$$\begin{array}{ccc} & & F \\ & {\scriptstyle i}\nearrow & \downarrow \\ P & \xrightarrow{\mathrm{id}} & P \end{array}$$

the lift always exists: $\pi \circ i = \mathrm{id}_P$, so the short exact sequence $0 \to \ker(\pi) \to F \to P \to 0$ is split exact, and thus $F \cong \ker(\pi) \oplus P$. ⊠

8. Projective and Injective Modules: 4/25/13

"As soon as I start talking, five seconds later people show up, so maybe I'll start."

Though projective modules were introduced in the previous lecture, they merit a formal definition:

Definition. An A-module is projective if for any surjective A-module homomorphism $M \xrightarrow{\pi} N$ and $f : P \to N$, there exists an $\hat{f} : P \to M$ such that the following diagram commutes:

$$\begin{array}{ccc} & & M \\ & {\scriptstyle \hat{f}}\nearrow & \downarrow{\scriptstyle \pi} \\ P & \xrightarrow{f} & N \end{array}$$

In some sense, the solid arrows are the given data, and f is lifted to $\hat{f}$.

It's easy to check that free modules are projective, as shown last lecture. We also saw that $\mathbb{Z}/n$ is not a projective $\mathbb{Z}$-module (though it is as a $\mathbb{Z}/n$-module, since it's free of rank 1). Additionally, we saw that projective modules are summands of free modules, as in Proposition 7.4.

Corollary 8.1. *If $K = \ker(\pi)$ in the proposition, then K is also projective.*

The summand result makes projective modules much easier to visualize. Let $F = P \oplus P'$, and let $e_p : F \to F$ be given by $e_p(p,p') = (p,0)$. This is an A-linear transformation, and e_p is idempotent: $e_p \circ e_p = e_p$. Thus, idempotent matrices lead to projective modules, which is useful for studying them, and is easier to understand than creating modules out of whole cloth.

Definition. Let k be a commutative ring and G be a group. Then, let $k[G]$ denote the ring of formal k-linear combinations of the elements of G: $\sum k_i g_i$, where addition is componentwise and multiplication is given by

$$\left(\sum k_i g_i\right)\left(\sum k'_j g'_j\right) = \sum_{i,j} (k_i k'_j)(g_i g'_j).$$

This is a (not necessarily commutative) ring, and has a k-module structure. If G is finite, then $k[G] \cong \prod_{g \in G} k$ as a k-module.

Any k-module M together with a group action α of G on M creates a $k[G]$-module structure on M. Such an action α is called a representation of G; G may be an abstract group, but the choice of an action is equivalent ot a choice of a group homomorphism $\alpha^* : G \to \mathrm{Aut}_A(M)$, where $\alpha^*(g)(m) = \alpha(g,m)$. If k is a field and M is finitely generated, then M is a k-vector space of dimension n, and $\mathrm{Aut}_k(k^n) = \mathrm{GL}_n(k)$, and is identified with the group of invertible $n \times n$ matrices with entries in k. Representation theory, the whole second half of this class, deals with this case.

Take $G = \mathbb{Z}/2\mathbb{Z}$ and $k = \mathbb{C}$. Then, $\mathbb{C}[G] = \mathbb{C}1 \times \mathbb{C}g$, where $(z+wg)(z'+w'g) = zz' + zw'g + z'wg + ww'g^2 = (zz'+ww') = (zw'+z'w)g$ (since $g^2 = 1$). This ring is a $\mathbb{C}$-vector space together with a matrix M such that $M^2 = 1$. These can be classified using the Jordan normal form, which says that over $\mathbb{C}$, every matrix is conjugate to one of the form $\begin{pmatrix} B_1 & & & \\ & B_2 & & \\ & & \ddots & \\ & & & B_n \end{pmatrix}$, where each B_i is a Jordan block (almost diagonal): $B_i = \begin{pmatrix} \lambda & 1 & & & \\ & \lambda & 1 & & \\ & & \ddots & \ddots & \\ & & & \lambda & 1 \\ & & & & \lambda \end{pmatrix}$.

Thus, the only Jordan blocks such that $B^2 = 1$ are $[1]$ and $[-1]$ (since the λ must square to 1 and upper triangular matrices form a multiplicative group). Thus, $\mathbb{C}^n \cong \mathbb{C}^n_+ \oplus \mathbb{C}^n_-$, where $\mathbb{C}^n_+ = \{\mathbf{v} \in \mathbb{C}^n \mid M\mathbf{v} = \mathbf{v}\}$, which is the trivial representation, and $\mathbb{C}^n_- = \{\mathbf{v} \in \mathbb{C}^n \mid M\mathbf{v} = -\mathbf{v}\}$, called the sign representation.

More abstractly, let $e = (1+T)/2$ and $f = (1-T)/2$, where T is the element of order 2 in G, so $e, f \in \mathbb{C}[G]$. Then, $e+f = (1+T+1-T)/2 = 1$, $e^2 = e$, and $f^2 = f$, so $\mathbb{C}[G] \cong \mathbb{C}[G]e \oplus \mathbb{C}[G]f$. Let $\varphi(a+bg) = ((a+bg)e, (a+bg)f)$. Since this is a commutative ring, this is a homomoprhism. Note that it has no kernel: if $((a+bg)e, (a+bg)f) = 0$, then $(a+bg)(e+f) = 0$, so $a+bg = 0$, and $(a+bg)e$ and $(a+bg)f$ generate distinct, one-dimensional subspaces of the images. Thus, by dimension φ is surjective, and thus an isomorphism.

The upshot is that $\mathbb{C}[G] \cong \mathbb{C} \oplus \mathbb{C}$. Since the former is free, then $\mathbb{C}[G]e$ and $\mathbb{C}[G]f$ are projective.

Definition. Suppose A is a ring and M, N are A-modules. Then, $\mathrm{Hom}_A(M,N)$ is the set of all A-module homomorphisms $M \to N$.

$\mathrm{Hom}_A(M,N)$ is in fact an abelian group under $(f+g)(m) = f(m) + g(m)$, defined pointwise, since it can be checked that $f+g \in \mathrm{Hom}_A(M,N)$, etc.

If $\theta : N \to N'$, then $\mathrm{Hom}_A(M,\theta) : \mathrm{Hom}_A(M,N) \to \mathrm{Hom}_A(M,N')$ is induced, and similarly $\varphi : M \to M'$ induces $\mathrm{Hom}(\varphi,N) : \mathrm{Hom}_A(M',N) \to \mathrm{Hom}_A(M,N)$. Take care to see that $\mathrm{Hom}_A(M,\theta)(f)(m) = \theta \circ f(m)$, but $\mathrm{Hom}(\varphi,N)(f)(m) = f \circ \varphi(m)$.

Now, throw in some exactness: if $0 \to N' \xrightarrow{i} N \xrightarrow{\pi} N'' \to 0$ is a short exact sequence of A-modules, then apply $\mathrm{Hom}_A(M,\_\_)$ to it to obtain

$$0 \longrightarrow \mathrm{Hom}_A(M,N') \xrightarrow{\alpha} \mathrm{Hom}_A(M,N) \xrightarrow{\beta} \mathrm{Hom}_A(M,N'') \longrightarrow 0. \tag{2}$$

Claim. α is injective.

Proof. If $\alpha(f) = 0$, then $i \circ f = 0$, so $i(f(m)) = 0$ implies $f(m) = 0$ (since i is injective). ⊠

Then, suppose $f \in \mathrm{Hom}_A(M,N)$ and $\beta(f) = 0$. Then, $\pi \circ f(m) = 0$ for all m, so $f(m) \in \mathrm{Im}(i)$ for all m, so $f = i \circ f^*$, where $f^* : M \to N$.

However, this sequence isn't always exact: with $0 \to \mathbb{Z} \to \mathbb{Z} \to \mathbb{Z}/p \to 0$, $\mathrm{Hom}(\mathbb{Z}/p, \mathbb{Z}) = 0$ (since $\mathbb{Z}$ has no elements of order p), but $\mathrm{Hom}(\mathbb{Z}/p, \mathbb{Z}/p) \cong \mathbb{Z}/p$, and there's no way to have $0 \twoheadrightarrow \mathbb{Z}/p$. Thus, the Hom functor is instead called left exact.

Similarly, if

$$0 \longrightarrow M' \longrightarrow M \longrightarrow M'' \longrightarrow 0 \tag{3}$$

is exact, then

$$0 \longrightarrow \mathrm{Hom}_A(M'',N) \longrightarrow \mathrm{Hom}_A(M,N) \longrightarrow \mathrm{Hom}_A(M',N) \longrightarrow 0 \tag{4}$$

is exact at the first two entries, but not the third.

If M is projective, then (2) is exact, because the homomorphism lifts. However, there's a related notion for (3).

Definition. An A-module N is called injective if for any short exact sequence of A-modules (3), the sequence (4) is exact.

These are considerably less intuitive than projective modules, but $\mathbb{Z}$, $\mathbb{Q}$, and $\mathbb{Q}/\mathbb{Z}$ are all injective $\mathbb{Z}$-modules.

Finally, given a short exact sequence of A-modules $0 \to N' \xrightarrow{i} N \xrightarrow{\pi} N'' \to 0$ and some other A-module M, is

$$0 \longrightarrow M \otimes_A N' \xrightarrow{\mathrm{id} \otimes i} M \otimes_A N \xrightarrow{\mathrm{id} \otimes_A \pi} M \otimes_A N'' \longrightarrow 0$$

exact? This will turn out to be right exact: at $M \otimes_A N''$, if $N \xrightarrow{\pi} M$, then every $n'' \in N''$ has $\pi(n) = n''$ for some n, so $m \otimes n \mapsto m \otimes n''$, and the map is surjective.

It's harder to show exactness at $M \otimes_A N$: if so, then one could take homomorphisms $M \otimes_A N' \to L$ or $M \otimes_A N \xrightarrow{f} L$ such that $f \circ (\mathrm{id}_M \otimes i) = 0$. These are homomorphisms from the cokernel, and it suffices to show that these two sets are the same. Every hmomorphism $\beta : M \times N'' \to L$ induces a $\beta^* : M \times N \to L$ which vanishes on $M \times i(N)$, but they're actually equivalent: if $\beta^* : M \times N \to L$ vanishes on $M \times i(N)$, then applying the bilinear conditions implies that this serves as a bilinear map $M \times N/i(M) \to L$.

Most interestingly, exactness fails at $M \otimes_A N'$. Consider $0 \to \mathbb{Z} \xrightarrow{*p} \mathbb{Z} \to \mathbb{Z}/p \to 0$, and apply $\mathbb{Z}/p \otimes \_\_$. Then, one obtains the sequence $0 \to \mathbb{Z}/p \xrightarrow{0} \mathbb{Z}/p \to \mathbb{Z}/p \otimes \mathbb{Z}/p \to 0$, since $p \equiv 0$ in $\mathbb{Z}/p$, so the map isn't injective, and exactness fails. This sort of functor is called right exact.

This result is useful in obtaining presentations of tensor products: suppose $0 \to K \to A^n \to M \to 0$ is a short exact sequence of A-modules. Then, one can understand $M \otimes_A N$: the sequence $K \otimes_A N \to A^n \otimes_A N = N^n \to M \otimes_A \to 0$ is exact. One might have instead that

$$\begin{array}{ccc} A^m & \twoheadrightarrow & K \\ \downarrow & & \downarrow \theta \\ A^n & \longrightarrow & A^n \\ \downarrow & & \downarrow \\ M & & M \end{array}$$

where $A^m \to A^n$ gives an $m \times n$ matrix. Thus, $A^m \otimes_A N \twoheadrightarrow K \otimes_A N$, so it suffices to consider $N^n/\mathrm{Im}(\theta \otimes \mathrm{id}_N)$. This isn't necessarily free, though it is over a PID, so it's a bit simpler.

9. Finitely Generated Modules Over a Euclidean Domain: 4/30/13

Recall that if A is a commutative ring and M is an A-module, then M is finitely generated if there is a surjective homomorphism $\varphi : F \twoheadrightarrow M$, where F is a free A-module on some finite set $B \subseteq F$. The elements $\{\varphi(b)\}_{b \in B}$ must be a generating set for M: every $m \in M$ is of the form $m = \sum_{b \in B} a_b \varphi(b)$ for some $a_b \in A$.

Recall also that a principal ideal ring is a ring R such that every ideal in R is of the form (r) for some $r \in R$. A principal ideal domain is a principal ideal ring which is also an integral domain (i.e. there are no zero divisors). A Euclidean domain is an integral domain A equipped with a Euclidean function $d : A \to \mathbb{N} \cup \{0\}$ such that $d(0) = 0$, $d(a) > 0$ if $a \neq 0$, and for every pair $a, \alpha \in A \setminus 0$ there exist $q, r \in A$ such that $a = q\alpha + r$, with $d(r) < d(\alpha)$.

For example, the absolute value function turns $\mathbb{Z}$ into a Euclidean domain, giving the usual division algorithm. If k is a field, then $k[x]$ is a Euclidean domain with the degree function.

Proposition 9.1. *Any Euclidean domain is a principal ideal domain.*

Proof. Let A be a Euclidean domain with Euclidean function d_A, and let $I \subseteq A$ be an ideal. Select an $i \in I$ which attains the minimum nonzero value of d_A on I. For any $j \in I$< apply the Euclidean algorithm to i and j: $j = qi + r$, where $d_A(r) < d_A(i)$, but $r = j - qi$, so $r \in I$ and r must have norm less than the minimum nonzero value on I, or $d_A(r) = 0$. Thus, $j = qi$, and $I = (i)$. ⊠

For simplicity and concreteness, one can take $A = \mathbb{Z}$.

Theorem 9.2 (Kronecker)**.** *Every finitely generated $\mathbb{Z}$-module M is isomorphic to a module of the form*

$$M \cong \mathbb{Z}^r \oplus \bigoplus_i \mathbb{Z}/p_i^{e_i}\mathbb{Z}, \tag{5}$$

and this decomposition is unique in that for any other such decompostion, r is the same, and the set $\{(p_i, e_i)\}$ is the same (i.e. the pairs can be reordered). Specifically, if $\Pi = \{(p,e) \mid p \text{ is prime}, e \in \mathbb{N}\}$, then (5) determines a function φ on Π that gives the number of occurrences of (p,e) among the (p_i, e_i), and this function φ is identical among every decomposition.

Proof. This proof will show existence; uniqueness is a simple afterthought and is left to the reader.

Let $\mathbb{Z}^r \overset{\varphi}{\twoheadrightarrow} M$ (which can be done because M is finitely generated). Thus, there is a short exact sequence $0 \to K = \ker(\varphi) \to \mathbb{Z}^r \to M \to 0$.

Claim. $K \cong \mathbb{Z}^s$ for some $s \le r$.

Proof. $\mathbb{Z}^r = \mathbb{Z}e_1 \oplus \mathbb{Z}e_2 \oplus \cdots \oplus \mathbb{Z}e_r$, where $e_1, \dots, e_r$ are the basis elements. Then, take

$$K \xhookrightarrow{i} \mathbb{Z}e_1 \oplus \cdots \oplus \mathbb{Z}e_r \xrightarrow{\pi} \mathbb{Z}e_r,$$

where π is given by projection onto $\mathbb{Z}e_r$: $\pi(e_j) = 0$ unless $j = r$, in which case $\pi(e_r) = e_r$. Then, $\mathrm{Im}(\pi \circ i) \subset \mathbb{Z}e_r \cong \mathbb{Z}$ is a submodule, so it's an ideal in $\mathbb{Z}$. Thus, it is principal as an ideal, so it is a cyclic module. In particular, every such ideal is isomorphic to $\mathbb{Z}$ as $\mathbb{Z}$-modules, and is thus free. Therefore,

$$0 \longrightarrow K \cap \mathbb{Z}e_1 \oplus \cdots \oplus \mathbb{Z}e_{r-1} \hookrightarrow K \xrightarrow{\pi \circ i} \mathrm{Im}(\pi \circ i) \cong \mathbb{Z} \longrightarrow 0$$

Then, since $\mathrm{Im}(\pi \circ i)$ is free, then it is projective, so the sequence splits, so $K \cong K \cap (\mathbb{Z}e_1 \oplus \cdots \oplus \mathbb{Z}e_{r-1}) \oplus \mathbb{Z}$.[8]

Inductively, suppose we can prove that any submodule of $\mathbb{Z}^r$ is isomorphic to $\mathbb{Z}^s$ for some $s \le r$ when $r < N$. Then, if $K \subseteq \mathbb{Z}e_1 \oplus \cdots \oplus \mathbb{Z}e_n$, then $k \cong K' \oplus \mathbb{Z}$ or $K \cong K'$, where $K' \subseteq \mathbb{Z}e_1 \oplus \cdots \oplus \mathbb{Z}e_{r-1}$, so $K \cong \mathbb{Z}^s$ for some $s \le N - 1$. Thus, $K \cong \mathbb{Z}^{s'}$ for some $s' \le N$. ⊠

Then, in conclusion, there exists a short exact sequence $0 \to \mathbb{Z}^s \xrightarrow{i} \mathbb{Z}^r \to M \to 0$ with $s \le r$. The homomorphism $\mathbb{Z}^s \to \mathbb{Z}^r$ can be written as a matrix over $\mathbb{Z}$: $\mathscr{I} = [n_{ij}]$, with $1 \le j \le s$, $1 \le i \le r$, and $\mathscr{I}$ given by $i(e_j) = \sum n_{ij} f_i$, where $e_1, \dots, e_s$ is a basis of $\mathbb{Z}^s$ and $f_1, \dots, f_r$ is a basis of $\mathbb{Z}^r$. ⊠

Recall that if $\alpha : \mathbb{Z}^s \to \mathbb{Z}^s$ and $\beta : \mathbb{Z}^r \to \mathbb{Z}^r$ are isomorphisms, then $\mathbb{Z}^r/\beta \circ \alpha(\mathbb{Z}^s) \cong \mathbb{Z}^r/i(\mathbb{Z}^s)$, so the goal is to find normal forms under conjugation by invertible matrices (in this case, the Smith normal form).

Here are some particular classes of invertible matrices:

- Permutation matrices, in which each row and column has exactly one nonzero element.
- Multiplication by ± 1 (the identity, except for a possible -1 somewhere along the diagonal).
- Matrices that are equal to the identity with the exception of one non-diagonal element.

Multiplication on the left or right by these matrices can be thought of as row or column operations, respectively. Specifically, rows can be permuted, as can columns, and can be multiplied by a scalar. Finally, a row can be multiplied by something and then added to another.

Using these matrices, what kind of normal form can be obtained?

Claim. Using only these row and column operations, any integer matrix ca be reduced to one of the form

$$\begin{bmatrix} n_1 & & & & & \\ & \ddots & & & & \\ & & n_k & & & \\ & & & 0 & & \\ & & & & \ddots & \\ & & & & & 0 \end{bmatrix}.$$

[8] Note that $\pi \circ i = 0$ is possible, in which case $K \subseteq \mathbb{Z}e_1 \oplus \cdots \oplus \mathbb{Z}e_{r-1}$, which is technically a different case.

This is a nce result: $e_j \to n_j e_j$, so $M \cong \mathbb{Z}/n_1 \oplus \cdots \oplus \mathbb{Z}/n_k \oplus \mathbb{Z}^r$, where r is the number of zeros along the diagonal. Specifically, $\bigoplus_{i=1}^{k+r} \mathbb{Z}/e_i/n_1e_1,\ldots,n_ke_k$ turns k of them into cyclic summands, and leaves the rest free.

Why does such a form exist? Algorithmically:

(1) Find each n_{ij} in the matrix with minimum nonzero absolute value, called n_{ij}^*.
(2) Use the division algorithm to subtract off multiples of the n_{ij} from that clumn and row. One of two things will happen:
   (a) If n_{ij}^* is the only nonzero entry in its row and column, then apply a permutation to put n_{ij}^* in location (i,i) and proceed to the next row and column (formally, perform the algorithm on the matrix made by removing row and column i).
   (b) Otherwise, there exists an entry v in either the i^{th} row or the j^{th} column such that $0 \le |v| \le n_{ij}^*$. In this case, go back to step 1 and repeat.

This gives us the existence part of Theorem 9.2: $M \cong \mathbb{Z}^r \oplus \mathbb{Z}/n_1 \oplus \cdots \oplus \mathbb{Z}/n_k$. Recall that by the Chinese Remainder theorem, if $n = p_1^{e_1} \cdots p_k^{e_k}$, then $\mathbb{Z}/n \cong \bigoplus_{i=1}^k \mathbb{Z}/p_i^{e_i}$, so $M \cong \mathbb{Z}^r \oplus \mathbb{Z}/p_1^{e_1} \oplus \cdots \oplus \mathbb{Z}/p_s^{e_s}$.

For uniqueness, it is possible to extract r and $(p_1,e_1),\ldots,(p_s,e_s)$ from M. First notice that r is independent of decomposition $\mathbb{Q} \otimes_{\mathbb{Z}} M \cong \mathbb{Z} \otimes_{\mathbb{Z}} (\mathbb{Z}^r \oplus \bigoplus \mathbb{Z}/p_i^{e_i}) \cong (\mathbb{Q} \otimes_{\mathbb{Z}} \mathbb{Z}^r) \oplus \bigoplus (\mathbb{Q} \otimes_{\mathbb{Z}} \mathbb{Z}/p_i^{e_i}) = \mathbb{Q} \otimes_{\mathbb{Z}} \mathbb{Z}^r = \mathbb{Q}^r$, so $r = \dim(\mathbb{Q} \otimes_{\mathbb{Z}} M)$ is the dimension of M as a $\mathbb{Q}$-vector space, which is thus invariant.

Then, $\bigoplus \mathbb{Z}/p_i^{e_i} \subseteq M$ is the torsion submodule $\mathrm{Tor}(M) = \{m \in M \mid nm = 0 \text{ for some } n \in A \setminus 0\}$. Let $G_p(n) = \{g \in M \mid p^n \cdot g = 0\}$. The sequence $G_p(1), G_p(2), \ldots$ indicates the number of summands, and is also invariant.

10. Finitely Generated Modules Over a PID: 5/2/13

Last lecture's proof was given in the case of $\mathbb{Z}$-modules, but it works for any finitely generated module over a Euclidean domain, which in particular could also be a ring of polynomials over a field. Then, the module is a sum of cyclic modules, some of which may be free, and others of which would be of the form $k[x]/(f(x))$.

However, there are PIDs that aren't Euclidean domains, such as $\mathbb{F}_p[x,y]/(y^2 - x^3 - x)$. These sorts of PIDs come up in algebraic geometry. The proof for the classification of modules over a PID is much more abstract than the previous proof, called the "invariant proof."

Definition. A module over a ring R is Noetherian if any increasing subsequence $M_0 \subseteq M_1 \subseteq M_2 \subseteq \cdots$ of submodules of M eventually stabilizes (i.e. there is an n such that $M_n = M_N$ for any $N \ge n$). A ring is Noetherian if it is Noetherian as a module over itself.

Proposition 10.1. *The following are equivalent:*

1. *M is Noetherian.*
2. *Any collection of submodules of M ordered by inclusion possesses a maximal element (i.e. a submodule not strictly contained in any of the others; there may be more than one).*
3. *Any submodule of M is finitely generated.*

Note that a finitely generated module may have submodules which aren't finitely generated. LEt $R = k[x_1, x_2, \ldots]$ be the ring of polynomials over a field in countably many variables, and $I = (x_1, x_2, \ldots)$. Then, I is not finitely generated, since there are no relations among the x_i, so R isn't Noetherian, even though it is finitely generated as an R-module.

Proof of Proposition 10.1.

$1 \implies 2$: Let Σ be a collection of submodules of M. Pick some $M_0 \in \Sigma$; if it's maximal, nothing more needs to be done. If not, then it's contained in some $M_1 \in \Sigma$, so the same game can be played. If none of them are maximal, one obtains an infinite sequence $M_0 \subset M_1 \subset M_2 \subset \cdots$, which is a contradiction, since M is Noetherian.

$2 \implies 3$: Let $N \subseteq M$ as submodules. Then, choose some $n_1 \in N$ and consider $(n_1) = Rn_1 \subseteq N$. If $Rn_1 = N$, then we win; if not, take some other $n_2 \in N$ and consider $Rn_1 + Rn_2$, and so on; if none of these is equal to all of N, then one has a sequence $Rn_1 \subset Rn_1 + Rn_2 \subset \cdots$ which doesn't stabilize, which means that the submodules of M have a chain without a maximal element.

$3 \implies 1$: Suppose M isn't Noetherian, so that there is a sequence $M_0 \subseteq M_1 \subseteq M_2 \subseteq \cdots$ that doesn't stabilize. Then, $M_\infty = \bigcup M_i \subset M$ is a submodule. If M_∞ were finitely generated by $\{m_1, \ldots, m_k\}$, each of the m_i would have to appear at some finite point in the chain, after which the sequence stabilizes. ⊠

Most rings that we think of are Noetherian: all polynomial rings in finitely many variables are Noetherian, for example.

Proposition 10.2. *Principal Ideal Domains are Noetherian as rings.*

Proof. Every ideal is finitely generated, since it is principal, so by Proposition 10.1, we're done. ⊠

Theorem 10.3 (Elementary Divisior Form)**.** *Suppose M is a finitely generated free R-module over a PID and $N \subseteq M$ is a submodule. Then, there exists a basis $y_1,\dots,y_n$ for M, and $r_1,\dots,r_m \in R$, such that $m \le n$, such that $r_1y_1,\dots,r_m,y_m$ is a basis for N. Moreover, we may assume that $r_1 \mid r_2 \mid r_3 \mid \cdots$ (i.e. $(r_1) \supseteq (r_2) \subseteq \cdots$).*

Notice that for vector spaces, $r_1,\dots,r_m = 1$. The above theorem has a different, equivalent formulation, giving two different parameterizations of the isomorphism types.

Theorem 10.4 (Rational Canonical Form)**.** *Let T be a finitely generated R-module (where R is again a PID) and take a presentation $M \xrightarrow{\varphi} T$, with $N = \ker(\varphi)$. Then,*

$$T \cong R^{n-m} \oplus \bigoplus_{i=1}^{m} R/(r_i),$$

for some $r_1 \mid \cdots \mid r_m \in R$.

Proof of Theorem 10.3. We have already proven that N is free of rank at most m, as seen in the proof of Theorem 9.2, since it didn't require the Euclidean property.

We will construct a $y \in M$ such that $y = r_1y_1$ for some r_1, y_1 and y_1 can be ectended to a basis for M.[9] This is akin to searching the matrix for the element of least nonzero absolute value.

For every $\varphi \in \mathrm{Hom}_R(M,N)$, $I_\varphi = \varphi(N)$ is a submodule (ideal) in R. Since R is Noetherian, then the collection of submodules I_φ must have a maximal element $I_\nu = (r_1)$. Thus, there exists a $y \in N$ such that $\nu(y) = r_1$.

Claim. $\varphi(y)$ is divisible by r_1 for any other $\varphi \in \mathrm{Hom}_R(M,N)$.

Proof. Given any $r, r' \in R$, $r\varphi + r'\nu \in \mathrm{Hom}_R(M,N)$. Then, $(r\varphi + r'\nu)(y) = r\varphi(y) + r'\nu(y) = r\varphi(y) + r'r_1$. If $\varphi(y) \notin (r_1)$ (i.e. it is not divisible), then $(\varphi(y), r_1) = I$ and $I \supsetneq (r_1)$. Thus, one can choose r, r' such that $r\varphi(y) + r'\nu(y)$ is a generatr for I; then, $\theta = r\varphi + r'\nu$ is a homomoprhism such that $\theta(N) = I$, contradicting the maximality of I_ν. ⊠

Since $M \cong R^n$, then the projections $\pi_i \in \mathrm{Hom}_R(M,N)$ ($\pi_i(\rho_1,\dots,\rho_r) = \rho_i$) and the $\pi_i(y)$ are all divisible by r_1, so all of the coordinates of y are divisible by r_1. Thus, y is too. Thus, there is a unique y' such that $y = r_1y'$. Notice that y' isn't necessarly in N, but that's not a problem. Then, $\nu(y) = r_1$, but $\nu(y') = 1$ (in some sense, "dividing" by r_1), which is useful:

Claim. $M \cong Ry' \oplus \ker(\nu)$.

Proof. $M \xrightarrow{\nu} R$ is surjective, because it hits 1. Thus, one has the short exact sequence $0 \to K \to M \xrightarrow{\nu} R \to 0$, where $K = \ker(\nu)$. Since M is free, then this sequence splits. ⊠

Claim. There exists a corresponding decomposition $N \cong Ry \oplus (\ker(\nu) \cap N)$.

Proof. $0 \to \ker(\nu) \cap N \to N \xrightarrow{\nu} Rr_1 \to 0$ is exact and N is free. ⊠

Thus, $r_1y' \in N$ and y' can be extended to a basis of M by choosing a basis of $\ker(\nu)$. But this is the same problem of a smaller rank: $\ker(\nu)$ is free of rank $n-1$, so apply induction to get the full decomposition. Thus, there are in fact bases $f_1,\dots,f_m$ of N and $e_1,\dots,e_n$ of N such that $f_jr_j = e_j$ for some r_j.

It remains to show that $r_1 \mid r_2$ (the rest follow from induction): r_1 was chosen so that π_1 is now identified with ν, the maximal homomorphism. In particular, since $\pi_2 \in \mathrm{Hom}_R(M,R)$, then $\pi_2(N) \subseteq \pi_1(N)$, so $(r_2) \subseteq (r_1)$, or $r_1 \mid r_2$. ⊠

Then, Theorem 10.4 falls out as a corollary: supposing the r_i are powers of p, this means the exponents are increasing, so it is the same as the other example. Increasing divisibility amounts to increasing the exponents.

This abstract theorem is useful for problems outside of commutative algebra. Let k be a field; then, two matrices M and M' over k are similar (or conjugate) if there exists an invertible matrix S such that $M = SMS^{-1}$. This is an equivalence relation, and one can parameterize the similarity classes of these matrices: for example, systems of linear differential equatins with constant coeffcients over $\mathbb{C}$ are given by

$$\begin{pmatrix} z_1'(t) \\ \vdots \\ z_n'(t) \end{pmatrix} = A \begin{pmatrix} z_1(t) \\ \vdots \\ z_n(t) \end{pmatrix},$$

and clearly differential equations are important. The solutions are given by $\mathbf{z}(t) = \mathbf{c}e^{At}$. This is unpleasant to compute, but if A is similar to a diagonal matrix D, or $A = S^{-1}DS$, then $\mathbf{z}'(t) = S^{-1}DS\mathbf{z}(t)$, or $S\mathbf{z}'(t) = D(S\mathbf{z}(t))$, so after a change of basis. the system has a diagonal matrix, giving a system $\mathbf{w}' = D\mathbf{w}$. This has a simpler solution $w_i = c_ie^{d_it}$, with $\mathbf{w} = S\mathbf{z}$. Additionally, knowing the entries of D is fairly useful to understand the qualitative properties of the system.

[9] Unlike in vector spaces, not every nonzero element can be part of a basis, because not everything is necessarily invertible.

But this is relate to what we have just proven: a matrix A is an automorphism φ_A on some vector space V_A. A and B are similar iff there is an automorphism $V_A \xrightarrow{f} V_B$ such that the following diagram commutes:

$$\begin{array}{ccc} V_A & \xrightarrow{f} & V_B \\ {\scriptstyle \varphi_A}\downarrow & & \downarrow{\scriptstyle \varphi_B} \\ V_A & \xrightarrow[f]{} & V_B \end{array}$$

Since V is also a module over $k[t]$, then the two matrices are similar iff these modules are isomorphic. Thus, this leads to the existence of some decompositions over algebraically closed fields.

11. The Jordan Normal Form: 5/7/13

Last time, we saw that if k is a field, then a $k[t]$-module is equivalent to a k-vector space V equipped with a k-linear endomorphism $f : V \to V$. Furthermore, if V is finite-dimensional, then f can be associated with an $n \times n$ matrix, where $n = \dim V$. The module attached to (V, B, M) (where B is the basis and M is the matrix) is isomorphic to $(V, B, \varphi M \varphi^{-1})$, where φ is auy invertible $n \times n$ matrix. Conversely, if M and M' five isomorphic modules, then they are cojugate (or similar), and the followng diagram commutes:

$$\begin{array}{ccc} V & \xrightarrow{f} & V \\ {\scriptstyle \varphi}\downarrow & & \downarrow{\scriptstyle \varphi} \\ W & \xrightarrow{g} & W \end{array}$$

What sets of modules are given by these finite-dimensional matrices? Consider $k = \mathbb{C}$, since $\mathbb{C}$ is algebraically closed. Finitely generated modules over $\mathbb{C}[z]$ are classified as $\mathbb{C}[z]^s \oplus \bigoplus_{i=1}^n \mathbb{C}[z]/(f_i^{e_i})$, where $f_1, \dots, f_n$ are irreducible polynomials, because $\mathbb{C}$ is a field, so $\mathbb{C}[z]$ is a Euclidean domain. Since we're trying to classify $m \times n$ matrices, it's possible to just throw out the free part and look at irreducible polynomials in $\mathbb{C}[z]$.

Proposition 11.1. *All irreducible polynomials over $\mathbb{C}$ are of the form $z - a$ for some $a \in \mathbb{C}$.*

Proof. Suppose $\deg(f) > 1$ for some $f \in \mathbb{C}[z]$. Then, there is a root z_0 of f. Then, $(z - z_0) \mid f(z)$, so $f(z) = q(z)(z - z_0) + r(z)$, where $\deg(r) < \deg(z - z_0) = 1$. Thus, r must be constant, so plug in at z_0: $0 = f(z_0) = q(z_0)(0) + r$, so $r = 0$. Thus, $f(z) = q(z)(z - z_0)$. ⊠

Thus, every module is of the form $\bigoplus_i \mathbb{C}[z]/(z - a_i)^{e_i}$, so every matrix can be broken up as a block sup: let $M(a, e)$ be the matrix corresponding to the module $\mathbb{C}[z]/(z - a)^e$; then, every matrix over $\mathbb{C}$ is similar to one with a block decomposition

$$\begin{bmatrix} M(a_1, e_1) & & \\ & \ddots & \\ & & M(a_n, e_n) \end{bmatrix}$$

Example 11.1.

- $\mathbb{C}[z]/(z - a) \cong \mathbb{C}$, with $z \cdot [1] = a$, corresponding to the 1×1 matrix $[a]$.
- $\mathbb{C}[z]/(z^2) \cong \mathbb{C}^2$, with a $\mathbb{C}$-basis $[1], [z]$. Then, $[1] \cdot [z] = [z]$ and $[z] \cdot [z] = 0$, so the matrix is $\begin{bmatrix} 0 & 0 \\ 1 & 0 \end{bmatrix}$.
- $\mathbb{C}[z^2]$ has the basis $1, z, z^2$, so the matrix is $\begin{bmatrix} 0 & 0 & 0 \\ 1 & 0 & 0 \\ 0 & 1 & 0 \end{bmatrix}$. Notice how the subdiagonal is built up.

In general, $\mathbb{C}[z]/(z^n)$ has the matrix that is entirely zeroes except for ones on the subdiagonal, written in the basis $\{1, z, z^2, \dots, z^{n-1}\}$.

Taking $\mathbb{C}[z]/((z - a)^2)$, the basis elements are 1 and $z - a$ (1 and z work, but aren't as preferred), so the matrix is $\begin{bmatrix} a & 0 \\ 1 & a \end{bmatrix}$, since multiplication does more interesting things: $z = a \cdot 1 + (z - a)$ and $z(z - a) = z^2 - a \cdot z = -a(z - a)$. In general, $\mathbb{C}[z]/((z - a)^n)$ corresponds to the matrix

$$\begin{bmatrix} a & & & \\ 1 & a & & \\ & \ddots & \ddots & \\ & & 1 & a \end{bmatrix}. \tag{6}$$

These blocks are a complete parameterization of the similarity classes of matries over $\mathbb{C}$, so any matrix over $\mathbb{C}$ is similar to one of the form $\begin{bmatrix} B_1 & & & \\ & B_2 & & \\ & & \ddots & \\ & & & B_n \end{bmatrix}$, where each B_i is a block matrix of the form given above.

This same classification applies to any algebraically closed field. In $\mathbb{R}$, though, things look different, since it isn't algebraically closed. Polynomials such as x^2+ax+b are irreducible if $a^2-4b<0$, and in fact these and linear polynomials are all of the prime polynomials. This can be seen by taking a monic $p \in \mathbb{R}[x]$ and viewing it as a polynomial over $\mathbb{C}$. Then, if $p = \prod_{i=1}^{n}(x-a_i)$ with $a_1,\dots,a_n \in \mathbb{C}$, then $p(x) = \overline{p(x)}$ because p is a real polynomial. Thus, if $x \in \mathbb{C}$ is a root, then so is $\overline{x}$.

Conversely, if $p \in \mathbb{C}[x]$ is such that $\overline{x}$ is a root whenever x is, then p is real-valued, since p can be written as

$$p(x) = \prod_{i=1}^{n}(x-a_i)(x-\overline{a_i}) = \prod_{i=1}^{n}(x^2-(a_i+\overline{a_i})x+a_i\overline{a_i}),$$

and $a_i+\overline{a_i}$ and $a_i\overline{a_i}$ are both real numbers (called the norm and trace, respectively). Notice that there could be single $x-a$ terms, with $a \in \mathbb{R}$, but the result still holds.

Thus, the Jordan blocks are either as in the complex case (6) with $a \in \mathbb{R}$, or they correspind to $\mathbb{R}[x]/(f^n)$, with f a degree-2 irreducible. For example, x^2+1 corresponds to the Jordan block $\begin{bmatrix} 0 & -1 \\ 1 & 0 \end{bmatrix}$, but over $\mathbb{C}$, this could be split into $\begin{bmatrix} i & 0 \\ 0 & -1 \end{bmatrix}$, and similarly, $\mathbb{R}[x]/((x^2+1)^2)$ has matrix

$$\begin{bmatrix} 0 & -1 & & \\ 1 & 0 & & \\ & & 0 & -1 \\ & & 1 & 0 \end{bmatrix}.$$

Thus, the description is relatively simple.

All right, how about a more arithmetically complicated field? In $\mathbb{F}_p$, the blocks of expoment 1 (i.e. $\mathbb{F}_p[x]/(f)$) will roughly correspond to some finite extension $\mathbb{F}_q$ of $\mathbb{F}_p$ (such that $q=p^n$). Let $\theta \in \mathbb{F}_q$; then, multiplication by θ is an $\mathbb{F}_p$-linear endomorphism of $\mathbb{F}_q$ as an $\mathbb{F}_p$-vector space, leading to a matrix. If θ_1,θ_2 are conjugate under $\mathrm{Gal}(\mathbb{F}_q/\mathbb{F}_p)$, then they will produce similar matrices. Also, not all θ will give irreducible blocks (e.g. if θ generates some $\mathbb{F}_r$ such that $\mathbb{F}_p \subsetneq \mathbb{F}_r \subsetneq \mathbb{F}_q$). Everything works so cleanly in $\mathbb{R}$ because there's only one finite field extension; $\mathbb{Q}$ is much hairier.

A related problem falls under the domain of representation theory.

Definition. Let G be a finite group and k be a field. Then, a k-linear representation of G is a homomorphism $G \xrightarrow{\rho} \mathrm{Aut}_k(V)$ for some k-vector space V.

Definition. Two representations $G \xrightarrow{\rho_1} \mathrm{Aut}_k(V)$ and $G \xrightarrow{\rho_2} \mathrm{Aut}_k(W)$ are isomorphic if there is an isomorphism $\sigma : V \to W$ such that the following diagram commutes:

$$\begin{array}{ccc} V & \xrightarrow{\rho_1(g)} & V \\ {\scriptstyle\sigma}\downarrow & & \downarrow{\scriptstyle\sigma} \\ W & \xrightarrow{\rho_2(g)} & W \end{array}$$

This is like the previous problem, in particular because these matrices can be pulled back into modules over a ring. Here, a k-linear representation of G is a $k[G]$-module, where $k[G]$ is the group ring as discussed before: the ring of k-valued functions on G, with multiplication given by convolution: if $G \xrightarrow{f,g} k$, then

$$(f*g)(\gamma) = \sum_{\{\gamma_1,\gamma_2 | \gamma_1\gamma_2=\gamma\}} f(\gamma_1)g(\gamma_2).$$

Often, it's easier to see them as formal expressions.

A finitely generated module over $k[G]$ is a k-vector space along with a left action by G, which induces the map $G \to \mathrm{Aut}_k(V)$. Then, one can obtain a module in the same way. In some sense, representation theory is just the study of equivalence classes of $k[G]$-modules. The field k matters quite a lot, but the case $k=\mathbb{C}$ will be considered first: it is the simplest, since $\mathbb{C}$ is algebraically closed.

Suppose $G = \mathbb{Z}/n\mathbb{Z}$. Then, a representation of G can be given by where 1 goes, but that matrix must have order n, so a representation of G is an endomorphism $\mathscr{E}$ of a vector space such that $\mathscr{E}^n = \mathrm{id}$.

Claim. Over $\mathbb{C}$, if B is a Jordan block such that $B^n = I$, then $B = [\zeta]$, where ζ is an n^{th} root of unity.

Proof. All blocks of exponent greater than 1 (i.e. those corresponding to $\mathbb{C}[x]/(f^n)$, $n>1$) have infinite order:

$$\begin{bmatrix} a & 0 \\ 1 & a \end{bmatrix}\begin{bmatrix} a & 0 \\ 1 & a \end{bmatrix} = \begin{bmatrix} a^2 & 0 \\ 2a & a^2 \end{bmatrix},$$

and so on. Thus, there will always be a nonzero lower-left term. ⊠

Proposition 11.2. *For any $\zeta \in \mu_n$,*[10] *every representation V of $\mathbb{Z}/n\mathbb{Z} = \langle T\rangle$ decomposes as $V = \bigoplus_{i=0}^{n-1} V_{\zeta^i}$, and each V_{ζ^i} has the property that $T\mathbf{v} = \zeta^i \mathbf{v}$ for all $\mathbf{v} \in V_{\zeta^i}$.*

This is known as the eigenspace decomposition.

Since not all groups are cyclic, it's worth approaching this from a ring-theoretic point of view. Just for fun, let $G = \mathbb{Z}/3 = \{1, T, T^2\}$. The goal is to understand $\mathbb{C}[G]$. It has some interesting elements, scuh as $e_1 = (1+T+T^2)/3$. Then, $e_1^2 = e_1$ (which you can calculate yourself if you like), so it is an idempotent. Since $\mathbb{C}[G]$ is commutative, it is specifically a central idempotent. If ζ is a primitive cube root of unity, then $e_2 = (1+\zeta T+\zeta^2 T^2)/3$ satisfies $e_2^2 = e_2$ as well. There's a third such idempotent element, $e_3 = (1+\zeta^2 T+\zeta T^2)/3$. Moreover, $e_1+e_2+e_3 = 1$. Thus, one can take the submodules (or ideals) $\mathbb{C}[G]e_i$: $\mathbb{C}[G] = \mathbb{C}[G]\cdot e_1 \oplus \mathbb{C}[G]\cdot e_2 \oplus \mathbb{C}[G]\cdot e_3$ as rings. Each of the $\mathbb{C}[G]\cdot e_i \cong \mathbb{C}$ as rings, so $\mathbb{C}[G] \cong \mathbb{C}^3$.

The module classification of $A \times B$ given the module classifications of A and B is relatively easy, which is important, because the group ring decomposes into matrix rings over $\mathbb{C}$ for *any* finite group. Choosing the idempotents is a bit more complicated, but it still happens.

12. Maschke's Theorem: 5/9/13

First, we will discuss some examples of representations of a finite group G over a field k.

- The most interesting representation is the trivial representation, in which G acts on k as the identity.
- There's also the regular representation, in which $k[G]$ is a vector space and G acts by left multiplication. For example, $\mathbb{Z}/4\mathbb{Z}$ acts by $(x_1,x_2,x_3,x_4) \mapsto (x_2,x_3,x_4,x_1)$. This representation has dimension $\#G$.

  The reduced regular representation acts on $\mathscr{E}_G = k\cdot\sum_{g\in G} g \subseteq k[G]$. $\mathscr{E}_G$ is an invariant subspace, because the trace $T_G = \sum_{g\in G} g$ satisfies $gT_G = T_G$, because the terms are just rearranged. One can also consider the set of vectors $\overline{T}_G$ in $k[G]$ such that $\sum x_g g = 0$, which is another invariant subspace. For $\mathbb{Z}/4\mathbb{Z}$, this is generated by $(1,-1,0,0),(0,1,-1,0),(0,0,1,-1)$. If k has characteristic zero or prime to $\#G$, then the regular representation decomposes as $k[G] \cong \mathscr{E}_G \oplus \overline{T}_G$.

  For example, if $k = \mathbb{F}_2$ and $G = \mathbb{Z}/2 = \{1, T\}$, then $\mathscr{E}_G$ is generated by $\{0, 1+T\}$ and $\overline{T}_G$ by $\{0, 1+T\}$. The direct sum doesn't happen here.
- Another representation is given by the symmetric group Σ_n acting on $\{1,\dots,n\}$. Form a vector space with basis $\{e_1,\dots,e_n\}$ such that $\sigma(e_i) = e_{\sigma(i)}$. This is called the permutation representation of Σ_n. More generally, if G acts on a set X, one can take a k-vector space $k[X]$ with X as a basis and $g(\sum_{x\in X} a_x x) = \sum a_x gx$. Each of these has a reduced form as well: the subset of all sums whose coefficients sum to zero.
- Let $\rho : G \to \mathrm{Aut}_k(V)$ be a representation (so that V is a k-vector space) and $f : H \to G$ be a homomorphism. Then, one has $\rho \circ f$, which is a representation of H over k. The regular representation of G over k can be thought of as the permutation representation $\Sigma_{|G|}$ along the homomorphism $G \to \Sigma_{|G|}$ in which elements of G act as permutations of G by left multiplication.
- A homomorphism $\chi : G \to k^*$ (the group of units) can be regarded as a one-dimensional representation. This factors through the maximal abelian subgroup of G: let $[G,G]$ be the subgroup generated by all commutators $g_1g_2g_1^{-1}g_2^{-1}$, so that $[G,G] \trianglelefteq G$ and $G/[G,G]$ is abelian (the maximal abelian quotient, in fact). Then, every one of these characters χ factors over $G/[G,G]$; to be precise, if $\pi : G \to G/[G,G]$ is the quotient homomoprhism, then a map $\chi : G \to k^*$ induces a Frattini quotient $\overline{\chi}$ such that the following diagram commutes:

$$\begin{array}{ccc} G & \xrightarrow{\pi} & G/[G,G] \\ & \searrow^{\chi} & \downarrow{\scriptstyle \overline{\chi}} \\ & & k^* \end{array}$$

- $\mathbb{C}$ is a real two-dimensional vector space of dimension 2 with basis $\{1, i\}$. Let μ_n be the set of n^{th} roots of unity in $\mathbb{C}^*$. This is a finite group which acts $\mathbb{R}$-linearly[11] and is represented on the 2-dimensional real vector space.

  These are given by the generators $\cos(2\pi/n) + i\sin(2\pi/n)$. Then, when multiplied by the basis elements, one gets $\mu = \begin{bmatrix} \cos(2\pi/n) & -\sin(2\pi/n) \\ \sin(2\pi/n) & \cos(2\pi/n) \end{bmatrix}$, a two-dimensional, real representation of μ_n.

[10] Here, μ_n is the group of n^{th} roots of unity in $\mathbb{C}$.

[11] Actually, it acts $\mathbb{C}$-linearly as well, but that's not important right now.

One can also consider the complex conjugate, which is $\mathbb{R}$-linear but not $\mathbb{C}$-linear. This action has matrix $\begin{bmatrix}1 & 0\\ 0 & -1\end{bmatrix}$, because $\overline{1} = 1$ and $\overline{i} = -i$. Combining them, one has

$$\begin{bmatrix}1 & 0\\ 0 & -1\end{bmatrix}\begin{bmatrix}\cos(2\pi/n) & -\sin(2\pi/n)\\ \sin(2\pi/n) & \cos(2\pi/n)\end{bmatrix}\begin{bmatrix}1 & 0\\ 0 & -1\end{bmatrix} = \begin{bmatrix}\cos(2\pi/n) & \sin(2\pi/n)\\ \sin(2\pi/n) & \cos(2\pi/n)\end{bmatrix} = \mu^{-1}.$$

Complex conjugation produces an automorphism of the group, but doesn't commute with it. Let $\alpha : \mathbb{Z}/2 \to \mathrm{Aut}(\mathbb{Z}/n)$ with $\alpha(T)(\mu) = -\mu$, which means that this is a representation of $\mathbb{Z}/2 \ltimes_\alpha \mathbb{Z}/n = D_{2n}$. Notice additionally that it is faithful.

- The quaternions are a four-dimensional non-commutative algebra over $\mathbb{R}$: $\mathbb{R}[i,j]/(i^2 = j^2 = 1, ij = -ji)$, so it has an $\mathbb{R}$-basis $\{1, i, j, ij\}$. This is in fact a non-commutative field or division algebra, because every nonzero element is invertible (which is not hard to double-check). Take the subgroup generated by i and j: $\{\pm 1, \pm i, \pm j, \pm ij\}$. This group is presented as $\langle i, j \mid i^2 = j^2, i^4 = 1, ij = j^3 i\rangle$. This is a nonabelian, nondihedral group (since all of its abelian subgroups are cyclic) called Q_8 (since there are higher-order analogues). Thus, $\mathbb{H}$ offers a four-dimensional real representation of Q_8.

The following theorem is the big result in classifying representations:

Theorem 12.1 (Maschke)**.** *Suppose V is a k-linear representation of G and suppose $U \subseteq V$ is an invariant subspace (i.e. $gU = u$ for every $g \in G$, or U is a subrepresentation), and suppose* $\mathrm{Char}(k) = 0$ *or is prime to the order of G. Then, there eists an invariant complement W to U (i.e. $V \cong U \oplus W$, and W is invariant under G).*

Notice how untrue this is for modules: the $\mathbb{Z}$-module $\mathbb{Z}$ has $2\mathbb{Z} \subset \mathbb{Z}$ as a submodule, but there is no complement to $2\mathbb{Z}$ in $\mathbb{Z}$. Additionally, the condition on the characteristic is necessary: let $k = \overline{\mathbb{F}}_2$ (the algebraic closure) and $G = \mathbb{Z}/2$. Then, there are two possible Jordan blocks, the trivial one I_2, and $\begin{bmatrix}1 & 1\\ 0 & 1\end{bmatrix}$, which squares to the identity. If $T \to (e, f)$, then $\mathrm{Span}(e)$ has no complement.

Proof of Theorem 12.1. Ignoring the action by G, select a complement W^* to U that isn't necessarily invariant. This can be done because U and V are vector spaces. Thus, $V \cong U \oplus W^*$, which gives a map $\pi : V \to V$ such that $\pi(u, w^*) = (u, 0)$. The map can be thought of as $\pi : V \to U$, and is surjective onto U.

π is not G-invariant, because if it were, then $\ker(\pi) = W^*$ and we would be done. Thus, it needs to be modified with an averaging process. For every $g \in G$, there is a k-linear map from V to itself given by $g^{-1}\pi g$, and $\mathrm{Im}(g^{-1}\pi g \subseteq U$ because πg has its image in U and U is invariant under G. Now, they can all be avaraged, which is where the characteristic condition becomes necessary: let

$$\Pi = \frac{1}{|G|}\sum_{g\in G} g^{-1}\pi g.$$

This is still a projection $V \to U$, but it still must be shown that it is G-invariant, i.e. that $\Pi|_U = \mathrm{id}$ and $\Pi(gv) = g\Pi(v)$ for any $v \in V$.

Notice that $gu \in U$ for any $u \in U$, so $\Pi(gu) = gu$. Thus, $\Pi(u) = u$ for any $u \in U$:

$$\Pi(u) = \frac{1}{n}\sum_{g\in G} g^{-1}\pi g u = \frac{1}{n}\sum g^{-1} g u = \frac{1}{n}\sum u = \frac{n}{n}u = u.$$

Thus, Π is a projection. Then, for any $h \in G$ and $v \in V$,

$$\Pi(hv) = \frac{1}{n}\sum_{g\in G} g^{-1}\pi g h v = \frac{1}{n}\sum_{g\in G} h g^{-1} h g v = h\Pi(v),$$

since this is a simple reordering of the terms. ⊠

Definition. A module or representation that has no submodules or subrepresentations other than $\{0\}$ and itself is called simple.

Corollary 12.2. *Every finite-dimensional representation V of a finite group G over k such that* $\mathrm{Char}(k)$ *is zero or relatively prime to $|G|$ has a decomposition $V = \bigoplus_{i=1}^n V_i$, where each V_i is a simple representation.*

Proof. If V is simple, then we're done. If not, then it has a submodule, so $V = V_1 \oplus V_2$ with $V_1, V_2 \neq \{0\}$. Now, repeat for each of V_1 and V_2, and by finiteness of dimension, this must eventually terminate. ⊠

Corollary 12.3. *$k[G] \cong \bigoplus_{i=1}^n k[G]_i$ as modules, for simple modules $k[G]_1, \ldots, k[G]_n$.*

For example, we have seen $\mathbb{C}[\mathbb{Z}/2] = \mathbb{C}^+ \oplus \mathbb{C}^- = \mathbb{C}[\mathbb{Z}/2]\cdot(1+T)/2 \oplus \mathbb{C}[\mathbb{Z}/2]\cdot(1-T)/2$, but this result about cyclic groups now holds for any finite group. Rings with this property are called semisimple, and have some nice properties.

13. Schur's Lemma and $k[G]$-modules: 5/14/13

Last time, we proved Maschke's Theorem (Theorem 12.1) for a group ring $k[G]$, where G is a finite group and $\mathrm{Char}(k)$ is prime to $\#G$. Then, if M is a $k[G]$-module, then any submodule $N \subseteq M$ has a complement N' such that $M \cong N \oplus N'$. This means that $k[G]$ satisfies the descending chain condition on ideals, so any finitely generated $k[G]$-module admits a decomposition into simple modules.

The following lemma is small, but very useful.

Lemma 13.1 (Schur)**.**

(1) Suppose P and Q are nonisomorphic simple modules over a ring R. Then, $\mathrm{Hom}_R(P,Q) = 0$.

(2) Consider the ring $\mathrm{End}_R(P) = \mathrm{Hom}_R(P,P)$*, where addition is pointwise and multiplication is given by composition. Then,* $\mathrm{End}_R(P)$ *is a division ring.*[12]

Proof. Let $\varphi : P \to Q$ be a homomorphism of R-modules. Then, $\mathrm{Im}(\varphi) \subseteq Q$ is a submodule, as is $\ker(\varphi) \subseteq P$. Since Q is simple, then $\mathrm{Im}(\varphi) = 0$ or $\mathrm{Im}(\varphi) = Q$. In the former case we're done, so suppose $\mathrm{Im}(\varphi) = Q$, so that φ is surjective. If $\ker(\varphi) = P$, then again $\varphi = 0$ and we're done, and if $\ker(\varphi) = 0$, then φ is injective, and thus $P \cong Q$.

If $\varphi \in \mathrm{Hom}_R(P,P)$ and $\varphi \neq 0$, then $\mathrm{Im}(\varphi) = P$, because P is simple, and $\ker(\varphi) = 0$ (since it can't be P, and must be one or the other). Thus, φ is an isomorphism, and in particular is multiplicatively invertible. Thus, $\mathrm{End}_R(P)$ is a skew field. ⊠

Now, take $k[G] = R$ and decompose it into simple submodules $R = \bigoplus_i R_i$, where the R_i are simple left R-modules. Then, Maschke's and Schur's results provide the information necessary to classify R.

Lemma 13.2. *If R is taken as a left R-module over itself, then $R \cong \mathrm{End}_R(R)$ as rings.*

Proof. Let $f : R \to R$ be a left R-module homomorphism. Then, $f(1)$ determines f, because $f(r) = rf(1)$ for any $r \in R$, and moreover, any r can be chosen as $f(1)$: if $\varphi_{\overline{r}}(r) = \overline{r}r$, then this defines a homomorphism from R to itself. Then, $(\varphi_{r'} \circ \varphi_r)(1) = \varphi_{r'}(r) = rr'$, so this is an isomorphism, but it reverses the order of multiplication. Thus, the isomorphism is given by $r \mapsto \varphi_r$. ⊠

Remark. $k[G] \cong k[G]^{\mathrm{op}}$ (i.e. $k[G]$ with order of multiplication reversed: $ab \leftrightarrow ba$), because $g \mapsto g^{-1}$ defines an automorphism respecting the structure. For a commutative ring (G is abelian), of course, they are identical. Thus, $k[G] = \mathrm{End}_{k[G]}(k[G])$.

Suppose $R = k[G] = \bigoplus_i E_i$ and $R = \bigoplus_j \bigoplus_{k=0}^{S_j} E_{j,k}$ (i.e. $\bigoplus_j W_j$, where $W_j = \bigoplus_{i=0}^{S_j} E_{j,k}$), so that j parameterizes the isomorphism classes of the simple modules occurring, such that $E_{j,k} \cong E_{j,k'}$. Thus, $\mathrm{Hom}_R(E_{j,k}, E_{j,k'}) = 0$ if $j \neq j'$, so all endomorphisms must preserve the summands W_j, so $\mathrm{End}_R(k[G]) = \prod \mathrm{End}_R(W_j)$.[13] This is a pretty big result; most rings don't split up like this.

Consider the specific endomorphism $\varepsilon_j \in \mathrm{End}_R(R)$ given by $\varepsilon_j|_{W_j} = \mathrm{id}$ and $\varepsilon_j|_{W_{j'}} = 0$ if $j \neq j'$. Notice that ε_j is idempotent (intuitively, it acts as a projection), and $\varepsilon_j \varepsilon_{j'} = \varepsilon_j$ if $j = j'$ and is zero otherwise. Thus, the ε_j all commute. Additionally, $\sum_j \varepsilon_j = 1$, since each ε_j is the identity somewhere, and they collectively do this everywhere. These calculations imply things in $k[G]$, known as the idempotent property: for each isomorphism type of simple modules, one obtains a central idempotaent, and each ε_j commutes with each ring element. Thus, in $k[G]$, call these idempotents e_j, so that $R \cong \bigoplus Re_i$, or $R = \prod \mathrm{End}_R(W_j)$.

These idempotents are now useful for understanding R-modules: let M be an R-module, and consider the submodules $e_i M$. Since the e_i are cnetral, then left action preserves this decomposition: $M \cong \bigoplus e_i M$ by $m \mapsto \sum e_i m$. The inclusions into the direct sum provide a map in the reverse direction. Since the e_i sum to 1, then the composite $M \to \bigoplus e_i M \to M$ is the identity, and each part is an isomorphism. This is pretty nice. The summand corresponding to e_i in M is called the e_i-isotypic component.

Digging deeper, what does $\mathrm{End}_R(W_i)$ actually look like? $W_i \cong \bigoplus_{j=1}^{s_j} E_j$, where E_j is a single cyclic module in the isomorphism class defined by W_i. Thus, since Hom and $\oplus$ commute, then

$$\begin{aligned}\mathrm{Hom}_R(W_i, W_i) &= \mathrm{Hom}_R\left(\bigoplus_{j=1}^{s_j} E_j, \bigoplus_{j=1}^{s_j} E_j\right) \\ &= \bigoplus_{j'} \mathrm{Hom}_R\left(\bigoplus_j E_j, E_j'\right) = \bigoplus_j \bigoplus_{j'} \mathrm{Hom}_R(E_j, E_{j'}).\end{aligned}$$

[12] A division ring, or skew field, is a (noncommutative) ring in which every nonzero element is invertible.

[13] This is a direct product, since finiteness isn't a concern.

Since the E_j are simple and isomorphic, then they can be viewed as modules over $\mathrm{End}_R(E_j)$ and $\mathrm{End}_R(E_{j'})$ (one from the left, and one from the right), so $\mathrm{Hom}_R(E_j, E_{j'})$ is a single copy of the division ring $D = \mathrm{End}_R(E_j) \cong \mathrm{End}_R(E_{j'})$. Thus,

$$\mathrm{End}_R(W_j) \cong \prod_{j,j'=1}^{s_j} D.$$

In some sense, the homomorphisms are parameterized by an array of elements in the division ring! This is how one goes from homomorphisms to matrices: additively, this is isomorphic to $M_s(D)$. In fact,

Theorem 13.3 (Wedderburn)**.** *This correspondence is also multiplicative:* $\mathrm{End}_R(W_j) \cong M_s(D)$*. Thus,* $k[G] \cong \prod R_i$*, where* R_i *is a matrix ring over a division algebra* D_i*:* $R_i \cong M_{s_i}(D_i)$*.*

Now, for a brief digression on matrix rings. Consider a 3-dimensional matrix ring $M_3(R)$. Let M_i be the set of matrices with nonzero entries only in the i^{th} column, such as

$$M_2 = \left\{ \begin{bmatrix} 0 & a_{12} & 0 \\ 0 & a_{22} & 0 \\ 0 & a_{32} & 0 \end{bmatrix} \mid a_{12}, a_{22}, a_{32} \in R \right\}.$$

Left-multiplication preserves these M_i, so each M_i is a left submodule of $M_3(R)$, equal to $M_3(R) \cdot e_i$ (where e_i is the matrix with a 1 in entry a_{ii} and zero elsewhere). Thus, $e_1 + e_2 + e_3 = I_3$ and $e_i e_j = 0$ if $i \neq j$, and is e_i if $i = J$. However, $M_3(R)$ does *not* break up as a product ring, because the idempotents aren't central in $M_3(R)$. That said, $Me_i \cong Me_j$ through the conugation

$$e_2 = \begin{pmatrix} 0 & 0 & 0 \\ 0 & 1 & 0 \\ 0 & 0 & 0 \end{pmatrix} = \begin{pmatrix} 0 & 1 & 0 \\ 1 & 0 & 0 \\ 0 & 0 & 1 \end{pmatrix} \begin{pmatrix} 1 & 0 & 0 \\ 0 & 0 & 0 \\ 0 & 0 & 0 \end{pmatrix} \begin{pmatrix} 0 & 1 & 0 \\ 1 & 0 & 0 \\ 0 & 0 & 1 \end{pmatrix} = \sigma e_1 \sigma^{-1},$$

and the essentially similar ones for the other conjugations. These induce isomorphisms $Me_i \to Me_j$. The division algebras over such a ring form a group called the Brauer group, and have a subgroup called the Schur subgroup.

Over $\mathbb{C}$, all of this is easier because it is algebraically closed. Suppose D is a finite-dimensional divison algebra over $\mathbb{C}$: $\mathbb{C} \subseteq Z(D) \subseteq D$. Then, $D = \mathbb{C}$: if not, then choose a $\delta \in D \setminus \mathbb{C}$. This satisfies some sort of algebraic equation in $\mathbb{C}$, since $|D : \mathbb{C}|$ is finite, so the sequence $1, \delta, \delta^2, \ldots, \delta^n, \ldots$ is eventually linearly dependent. Thus, $\sum_{i=1}^n a_i \delta_i = 0$ for some nonzero $a_i \in \mathbb{C}$.

But this is just a polynomial in δ, so it splits into a product because $\mathbb{C}$ is algebraically closed: $0 = \prod(\delta - \rho_i)$ for some roots ρ_i. Thus, either $\delta - \rho_i$ has no inverse, in which case $\delta = \rho_i \in \mathbb{C}$, or D isn't a division algebra.

Thus, $\mathbb{C}[G]$ always splits as a product of matrix rings $M_{n_i}(\mathbb{C})$, so the isomorphism type of this algebra is specified by the orders n_i. How should these be parameterized? Recall the definition of the trace of a matrix over a commutative ring.

Proposition 13.4. *Let* M *and* N *be* $n \times n$ *matrices over* A*. Then,* $\mathrm{Tr}(MN) = \mathrm{Tr}(NM)$*. In particular, if* S *is invertible, then* $\mathrm{Tr}(M) = \mathrm{Tr}(SMS^{-1})$*.*

Proof.

$$\mathrm{Tr}(MN) = \sum_j \sum_i m_{ji} n_{ij} = \sum_i \sum_j n_{ij} m_{ji} = \mathrm{Tr}(NM). \qquad \boxtimes$$

This means that the trace is a function on the similarity classes of matrices.

Thus, for a representation of G on V, by choosing a basis for V there is a matrix M_g for every $g \in G$ that acts on the basis. $\mathrm{Tr}(M_g)$ will turn out to be isomorhism-invariant, because if a different basis were chosen, the matrix would be similar anyways. Thus, one obtains a complex-valued class function on these conjugacy classes. This is an example of a character.

14. Characters: 5/16/13

Recall some facts we proved: $\mathbb{C}[G] \cong \prod_i M_{n_i}(\mathbb{C})$ – in general, the group ring decomposes as a direct product of finite-dimensional division algebras over the field, but $\mathbb{C}$ is the only finite-dimensional division algebra over itself. The more general formula is $k[G] \cong \prod_i M_{n_i}(D)$. Over $\mathbb{R}$, for example, one may have the quaternions.

Additionally, the matrix ring decomposes as $M_n(\mathbb{C}) = \bigoplus_{i=1}^n M_n(\mathbb{C}) e_i$. If $\mathbb{C}[G] = \prod_{i=1}^s M_{n_i}(\mathbb{C})$, then the dimension and multiplicity of the irreducible module over $M_{n_i}(\mathbb{C})$ is n_i. Thus, $|G| = \dim_{\mathbb{C}} \mathbb{C}[G] = \sum_i n_i^2$. This is an interesting and useful fact.

Next, one might ask how many summands there are. First, recall that the center of $\mathbb{C}[G]$, denoted $Z(\mathbb{C}[G])$, is the subring (which is not necessarily an ideal) of elements $x \in \mathbb{C}[G]$ such that $xa = ax$ for all $a \in \mathbb{C}[G]$.

Lemma 14.1. $Z(M_n(\mathbb{C})) = \mathbb{C} \cdot I_n$ *(i.e. it consists only of matrices* λI *such that* $\lambda \in \mathbb{C}$*).*

Proof. Let e_{ii} be the matrix with a 1 in row and column i and zeroes everywhere else, so that it is an idempotent matrix. What matrices commute with all of the e_{ii}? If $A = [a_{ij}]$, then $e_{ii}A$ has zeroes everywhere but the i^{th} row, and A_{ii} has zeroes everywhere except the i^{th} column. Thus, it is necessary for $a_{ij} = 0$ whenever $i \neq j$ if A is in the center.

Then, it is necessary for $a_{ii} = a_{jj}$ for any i, j. Consider the permutation matrix τ which swaps rows i and j. Then, in order for $A = \tau A \tau^{-1}$, it is necessary for $a_{ii} = a_{jj}$, since conjugation by τ swaps them.

Finally, it is easy to check that this is a sufficient condition for being in the center. ⊠

The center of a product is $Z(\prod_i A_i) = \prod_i Z(A_i)$, which is easy to check. Thus, $Z(\mathbb{C}[G]) = \prod_{i=1}^{s} Z(M_{n_i}(\mathbb{C})) = \prod_{i=1}^{s} \mathbb{C}$, and thus s is the number of isomorphism types of irreducible representations. But treating $\mathbb{C}[G]$ strictly as a group ring, suppose g and g' are conjugate, so that $g' = \gamma g \gamma^{-1}$, and suppose that $x = \sum_g \alpha_g g \in Z(\mathbb{C}[G])$. Then, $\gamma x \gamma^{-1} = x$ for all $\gamma \in G$. Choose the γ from before and apply it componentwise:

$$\gamma x \gamma^{-1} = \gamma \left(\sum \alpha_g g \right) \gamma^{-1} = \sum \alpha_g \gamma g \gamma^{-1} = \sum \alpha_g g,$$

so $\alpha_{\gamma g \gamma^{-1}} = \alpha_g$. This means that the coefficients of conjugate elements have to be the same. Thus, α_g depends only on the conjugacy classe of g if $\sum \alpha_g g \in Z(\mathbb{C}[G])$. Take some conjugacy class $C = \{g_1, \dots, g_t\} \in G$, which is a set that is acted on transitively by G. Thus, there is an $s_C = \sum_{g_i \in C} g_i$. Then, $s_C \in Z(\mathbb{C}[G])$, because C is invariant under conjugation.

Thus, if the conjugacy classes are $C_1, \dots, C_s$, then $Z(\mathbb{C}[G]) = \sum \mathbb{C} s_{C_i}$, because the coefficients have to be constant, so these are the only conjugate-invariant expressions. Thus, $\dim(Z(\mathbb{C}[G])) = s$, which is the number of conjugacy classes of G, but this is also equal to the number of distinct isomorphism types of representations in G.

Example 14.1. Take the symmetric group on three letters Σ_3. The conjugacy classes are e, (1 2), and (1 2 3), so there are three irreducible representations. There are 2 one-dimensional representations: the trivial representation $\sigma \mapsto 1$ and the sign representation $\Sigma_3 \to \mathbb{C}^*$ given by $\sigma \to \text{sign}(\sigma) = \pm 1$. Thus, $\mathbb{C}[\Sigma_3] = \mathbb{C} + \mathbb{C} + M_2(\mathbb{C})$ because $|\Sigma_3| = 6$, so the orders have to work. The third representation is the one given by D_6, as seen before.

In Σ_4, there's e, (1 2), (1 2)(3 4), (1 2 3), and (1 2 3 4). There are five conjugacy classes and therefore five irreducible representations.

The whole theory of representations over Σ_n is well understood and fairly pretty. It relates to partition types of the underlying set.

Recall that for any representation ρ of the group G over a field k, the character of ρ, denoted $\chi_\rho : G \to k$, is the function where $\chi_\rho(g)$ is the trace of the action of G in some basis. We saw that this was independent of basis, because χ_ρ is a class function (i.e. it is constant on conjugacy classes). In some sense, these are complex-valued functions on G.

Notice that $\chi_\rho(e) = \dim(\rho)$, because $\rho(e) = I_n$, where $n = \dim(\rho)$. On the regular representation of G, where G acts on $\mathbb{C}[G]$ by left action, take G as a basis for $\mathbb{C}[G]$, so that every element of G is a permutation matrix. Thus, the trace is always zero unless $g = e$: if g has a diagonal element, then $gh = h$ for that diagonal. Thus, for the regular representation, $\chi(g) = 0$ unless $g = e$, for which $\chi(e) = |G|$. Within ρ_G, there is the invariant subspace ε_G spanned by $\sum_{g \in G} g$. Every element of g acts on it by the identity, and $\rho_g = \varepsilon_g \oplus \overline{\rho}_G$ (the latter is the reduced regular representation). Notice that the character of the direct sum does the straightforward thing: $\chi_{\rho \oplus \rho'} = \chi_\rho + \chi_{\rho'}$. This is because within $\rho \oplus \rho'$, $g \mapsto \begin{bmatrix} \rho(g) & 0 \\ 0 & \rho'(g) \end{bmatrix}$, so $\text{Tr}(\rho(g))) + \text{Tr}(\rho'(g)) = \text{Tr}(\rho \oplus \rho'(g))$. With the components of the regular representation as above, note that $\chi_{\varepsilon_G} = 1$, since everything is mapped to the identity. Thus, $\chi_{\overline{\rho}_G}(g) = -1$ for $g \neq e$ and $\chi_{\overline{\rho}_G}(e) = \#G - 1$.

These functions end up capturing the isomorphism types exactly.

Claim. If ρ, ρ' are representations of G and $\chi_\rho = \chi_{\rho'}$, then $\rho \cong \rho'$.

Proof. First, extend the characters in G to linear function(al)s $\mathbb{C}[G] \to \mathbb{C}$, with $\chi\left(\sum \alpha_g g\right) = \sum \alpha_g \chi(g)$. Since the characters are class functions, then the vector space of class functions on G (or equivalently $\mathbb{C}[G]$) has dimenson equal to the number of conjugacy classes of G. Let $\{z_i\}$ be the set of central idempotents corresponding to the irreducible components of representations of $\mathbb{C}[G]$; since they're elements of $\mathbb{C}[G]$, then the characters can be called on them.

If χ_i is the character afforded by the irreducible representation $\rho_i = z_i \mathbb{C}[G]$, then what is $\chi_i(z_j)$? $\chi_i(g) = \chi_{\rho_i}(z_i g)$, so $\chi_i(z_j) = \chi_i(z_j z_i)$, and thus $z_i z_j = 0$ if $i \neq j$, so $\chi_i(z_j) = 0$ when $i \neq j$. $\chi_i(z_i g) = \chi_i(1) = \dim(\rho_i)$. Thus, the χ_i are linearly independent, and as a $\mathbb{C}$-vector space span the space of all class functions.

Thus, it follows that $\chi_\rho = \chi_{\rho'} \implies \rho = \rho'$: each representation ρ can be written as the direct sum of copies of irreducibles for each i. If n_i is the multiplicity of ρ_i in the sum, then $\chi_{\oplus n_i \rho_i} = \sum n_i \chi_i$, but since the χ_i are linearly independent, then this vector is uniquely determined. ⊠

15. Orthogonality of Characters: 5/21/13

"I wouldn't have asked the question if the answer weren't yes, so yes."

We now have a couple of ways of looking at representations, such as the central idempotents e_i, so that $e_i \cdot \mathbb{C}[G]$ is a primitive ideal of the group ring, isomorphic to a matrix ring. There is also the notion of the character χ attached to the

representation. χ is a class function on the group (i.e. invariant under conjugation): if $M(g)$ is the matrix of $g \in G$ in this representation in some basis, then $\chi(g) = \mathrm{Tr}(M(g))$. This seems very different from the central idempotent story, but there is a way to write the idempotents in terms of characters.

χ can be thought of as a $\mathbb{C}$-linear functional on the group ring by extending it: $\chi : \mathbb{C}[G] \to \mathbb{C}$. If χ_i is the character for e_i, then $\chi_i(e_j) = 0$ whenever $i \neq j$. Write $e_i = \sum_{g \in G} \alpha_g g$. Then, the goal is to write the α_g in terms of the χ_i.

Let χ_{reg} denote the regular character, or the character of the regular representation. Then, $\chi_{\mathrm{reg}}(g) = 0$ if $g \neq e$ and is $|G|$ if $g = e$. Thus, $\chi_{\mathrm{reg}}(e_i g^{-1}) = |G|\alpha_g$, since the non-identity coefficients are zeroed out. However, we also have that $\chi_{\mathrm{reg}} = \sum_i \chi_i(1)\chi_i$, where $\chi_1, \dots, \chi_n$ are the characters associated to the irreducible representations $e_1, \dots, e_n$. If $m_i = \dim e_i$, then $n_i = \dim_{\mathbb{C}} e_i \cdot \mathbb{C}[G] = m_i^2$, and since $1 \mapsto I$, then $\chi_i(1)$ is the dimension of the irreducible representation. Thus, $M_{m_i}(\mathbb{C}) = e_i\mathbb{C}[G]$ is equal to m_i copies of an irreducible representation of dimension m_i. Thus,

$$|G|\alpha_g = \chi_{\mathrm{reg}}(e_i g^{-1}) = \sum_j \chi_j(1)\chi_j(e_i g^{-1}) = \chi_i(1)\chi_i(e_i g^{-1}) = \chi_i(1)\chi_i(g^{-1}).$$

Thus, $\alpha_g = \chi_i(1)\chi_i(g^{-1})/|G|$, and

$$e_i = \frac{\chi_i(1)}{|G|} \sum_g \chi_i(g^{-1}) g.$$

It is possible to construct an inner product on the space of class functions in which the irreducible representations form an orthonormal basis (since we know the dimensions are the same).

Recall that a Hermitian inner product on a $\mathbb{C}$-vector space V is a function $\langle , \rangle : V \times V \to \mathbb{C}$ such that $\langle v_1 + v_2, v_3 \rangle = \langle v_1, v_3 \rangle + \langle v_2, v_3 \rangle$, $\langle zv, w \rangle = \langle v, zw \rangle$, $\langle v, w \rangle = \overline{\langle w, v \rangle}$, and $\langle v, v \rangle > 0$ if $v \neq 0$. An example for $V = \mathbb{C}^n$ is $\langle (z_1, \dots, z_n), (w_1, \dots, w_n) \rangle = \sum z_i \overline{w}_i$.

An orthonormal basis $\{b_1, \dots, b_n\}$ for such a space is a basis such that $\langle b_i, b_j \rangle = \delta_{ij}$. Importantly, an orthonormal basis gives the "Fourier expansion" for any $v \in V$: $v = \sum_{i=1}^n \langle v, b_i \rangle b_i$. This is because the b_i are a basis, so $v = \sum z_i b_i$, but

$$\langle v, b_i \rangle = \left\langle \sum_j z_j b_j, b_i \right\rangle = \sum_j z_j \langle b_j, b_i \rangle = \sum_j z_j \delta_{ij} = z_i.$$

This will provide information about the characters that makes computation much easier.

if $f, f' : G \to \mathbb{C}$ are class functions, then define

$$\langle f, f' \rangle = \frac{1}{|G|} \sum_{g \in G} f(g)\overline{f'(g)}.$$

That this is an inner product is mostly obvious, but for an example, positive-definiteness follows from $\langle f, f \rangle = \frac{1}{|G|} \sum_{g \in G} f(g)\overline{f(g)}$, but $z\overline{z} > 0$ for any $z \in \mathbb{C}$, so it works. Thus, this is a Hermitian inner product on the space of class functions, which is often called $\mathscr{C}(G)$.

Claim. The χ_i form an orthonormal basis for this space.

Proof. In $\mathbb{C}[G]$,

$$\begin{aligned} \delta_{ij} e_i = e_i \cdot e_j &= \frac{\chi_i(1)}{|G|} \sum_g \chi_i(g^{-1}) g \cdot \frac{\chi_j(1)}{|G|} \sum_h \chi_j(h^{-1}) h \\ &= \frac{\chi_i(1)\chi_j(1)}{|G|^2} \sum_{g,h \in G} \chi_i(g^1)\chi_j(h^{-1}) gh. \end{aligned}$$

Let $x = h$ and $y = gh$, so that $g^{-1} = xy^{-1}$:

$$= \frac{\chi_i(1)\chi_j(1)}{|G|^2} \sum_y \left(\sum_x \chi(xy^{-1})\chi_j(x^1) \right) y.$$

Using the formula given for e_i, this is also equal to

$$= \delta_{ij} \frac{\chi_i(1)}{|G|} \chi_i(g^{-1}).$$

Since this formula holds for all $g \in G$, g and g^{-1} can be switched to make the notation easier to deal with. Additionally, we can let $g = 1$.

$$\delta_{ij} \left(\frac{\chi_i(g)}{\chi_i(1)} \right) = \frac{1}{|G|} \sum_x \chi_i(xy)\chi_j(x^{-1}). \implies \delta_{ij} \frac{\chi_i(1)}{\chi_j(1)} = \frac{1}{|G|} \sum_x \chi_i(x)\chi_j(x^{-1}).$$

Thus, $1 = (1/|G|)\sum_x \chi_i(x)\chi_i(x^{-1})$ and, when $i \neq j$, $0 = (1/|G|)\sum_x \chi_i(x)\chi_j(x^{-1})$.

For any group character whatsoever, $\chi(g^{-1}) = \overline{\chi(g)}$: this can be shown on cyclic groups, since in general it's determined by the cyclic subgroups of G (in some sense, the trace is local). If $G = \mathbb{Z}/n$, then every representation is of the form $\rho(g) = \begin{bmatrix} \mu_1 & & \\ & \ddots & \\ & & \mu_n \end{bmatrix}$, with the μ_i n^{th} roots of unity. Thus, $\mu = \cos(2\pi\ell/n) + i\sin(2\pi\ell/n)$, so $\overline{\mu} = \cos(2\pi\ell/n) - i\sin(2\pi\ell/n)$. Thus, $\mu\overline{\mu} = \cos^2(2\pi\ell/n) + \sin^2(2\pi\ell/n) = 1$, so $\overline{\mu} = \mu^{-1}$. Thus, $\rho(g^{-1}) = \overline{\rho(g)}$, and thus $\chi(g^{-1}) = \overline{\chi(g)}$. Thus, the above formula simplifies to

$$\delta_{ij} = \frac{1}{|G|}\sum_x \chi_i(x)\overline{\chi_j(x)},$$

so they do indeed form an orthonormal basis. ⊠

Corollary 15.1. *Thus, a representation is irreducible iff its character χ satisfies $\langle \chi, \chi \rangle = 1$.*

This is a useful way to quickly check whether a representation is irreducible.

Example 15.1. Consider the Σ_3 case, as seen before in Example 14.1. Using the above result, it is possible to derive some of the information there in another way. There are two one-dimensional representations, the trivial representation ε and the sign representation σ, given by the sign homomorphism $\Sigma_3 \to \mathbb{Z}/2$. Let $r \in \Sigma_3$ be a 3-cycle and f be a 2-cycle, so that $\Sigma_3 = \{1, r, r^2, f, fr, f^2r\}$, and the conjugacy classes are $\{1\}$, $\{r, r^2\}$, and $\{f, fr, f^2r\}$. Then, it is possible to construct a character table, as in Table 1. There's yet one more representation, and its character can be calculated: here, a, b, and c are unknowns.

TABLE 1. The incomplete character table of Σ_3.

	ε	σ	ρ
1	1	1	a
r	1	1	b
r^2	1	1	b
f	1	-1	c
fr	1	-1	c
f^2r	1	-1	c

Notice $\langle \chi_\varepsilon, \chi_e \rangle = 1$, and similarly for χ_σ. Additionally, $\langle \chi_\varepsilon, \chi_\sigma \rangle = 0$. Then, by orthogonality, $a + 2b + 3c = 0$, and $a + 2b - 3c = 0$, so $2a + 4b = 0$, and thus $c = 0$. Then, $a = 2$, since this is a two-dimensional representation, and thus $b = -1$. Notice that $\langle \chi_\rho, \chi_\rho \rangle = (1/6)(4 + 1 + 1) = 1$.

TABLE 2. The filled-in column of Table 1, giving ρ on Σ_3.

	ρ
1	2
r	-1
r^2	-1
f	0
fr	0
f^2r	0

This example worked nicely, but it will work on yet more things in conjunction with constructing representations, in particular by induction. Since a representation of G is just a left $\mathbb{C}[G]$-module, suppose $K \leq G$, so that $\mathbb{C}[K] \subseteq \mathbb{C}[G]$ as rings. If one has a representation of K, which is just a $\mathbb{C}[K]$-module M, then one might wish to extend M to a left $\mathbb{C}[G]$-module $i_K^G(\varepsilon) = \mathbb{C}[G] \otimes_{\mathbb{C}[K]} M$. The associated representation is called the representation induced from K on the representation M. In a certain class of groups, all representations can be written in this form.

For example, take $\mathbb{Z}/3 = \langle (1\ 2\ 3) \rangle < \Sigma_3$. The trivial representation $\mathbb{Z}/3 \xrightarrow{\mathscr{E}} \mathbb{C}^*$ is induced into $\mathbb{C}[\Sigma_3] \otimes_{\mathbb{C}[\mathbb{Z}/3]} \mathscr{E}$. To understand this, it's useful to build a presentation of $\mathscr{E}$ as a $\mathbb{C}[\mathbb{Z}/3]$-module as $\mathscr{E} \leftarrow \mathbb{C}[\mathbb{Z}/3] \xleftarrow{1 \longmapsto (1\ 2\ 3)} \mathbb{C}[\mathbb{Z}/3]$. Thus, $\mathbb{C}[\Sigma_3] \xleftarrow{1 \longmapsto (1\ 2\ 3)} \mathbb{C}[\Sigma_3])$, yielding $\mathbb{C}[\Sigma_3/(\mathbb{Z}/3)] = \mathbb{C}[1, (1\ 2)]$.

Suppose instead of $\mathscr{E}$ we have $(1\ 2\ 3) \mapsto \mu$, where μ is some primitive 3^{rd} root of unity. Then, we get $\mathbb{C}[\mathbb{Z}/3] \xleftarrow{\mu \longmapsto (1\ 2\ 3)} \mathbb{C}[\mathbb{Z}/3]$ and correspondingly $\mathbb{C}[\Sigma_3] \xleftarrow{\mu \longmapsto (1\ 2\ 3)} \mathbb{C}[\Sigma_3]$. The dimension is the same, but the action is different, yet familiar. Next time, we will discuss the characters of such induced representations.

16. Character Tables: 5/23/13

Suppose that $H \leq G$ and one has a $k[H]$-module M that is a representation. Recall that the induced representation of G over k is $k[G] \otimes_{k[H]} M = i_h^G(M)$. Notice the group action is multiplication from the left, as $k[G]$ is a $k[G]$-bimodule, so $\_\_ \otimes_{k[H]} M$ is applied using the restriction of the right action along the inclusion $k[H] \subseteq k[G]$, so the G-action on $i_H^G(M)$ is considered using the left action of $k[G]$ on itelf.

Since G is a k-basis for $k[G]$, then $k[G]$ is free over k.

Claim. $k[G]$ is also a free $k[H]$-module.

Proof. Since $H \leq G$, then G can be partitioned into left cosets gH. Pick one representative γ_i from each coset, so there are $|G/H| = |G|/|H|$ of them. For each γ_i, the right $k[H]$-module generated by γ_i is free of rank 1, so $k[G] = \bigoplus k[G]_i$ as right $k[H]$-modules. But tensors of direct sums are easy to compute: $k[G] \otimes_{k[H]} M \cong \bigoplus k[G]_i \otimes_{k[H]} M \cong \bigoplus_i M$, so as a k-vector space, $i_H^G(M) \cong \bigoplus_{|G|/|H|} M$. ⊠

The left G-action permutes the summands $k[G]_i$, since $k[G]_i$ is the span of a coset $\gamma_i H$.

For a simpler case, suppose $H \trianglelefteq G$. Then, it stabilizes every coset $\gamma_i H$, so H-action leaves the decomposition $i_H^G(M) = \bigoplus M_i$ unchanged. Within a factor $M_i = \gamma_i \otimes M$, $h \cdot \gamma_i \otimes M = \gamma_i \otimes \gamma_i^{-1} h \gamma_i M$, so the action of G on the summand is the conjugate action.

Example 16.1. Let $G = \Sigma_3$ and $H = \mathbb{Z}/3 < \Sigma_3$. Write $\mathbb{Z}/2 = \{1, \sigma\}$. An H-representative is $f(T) = \zeta$, with $\zeta = e^{2\pi i/3}$. Thus, i_H^G is two-dimensional, as $i_H^G(\rho) = 1 \otimes \mathbb{C} \oplus \sigma \otimes \mathbb{C}$, but here, conjugation in $\mathbb{Z}/3$ inverts elements, so the matrix for the action of $\mathbb{Z}/3$ on $i_H^G(\rho)$ is $\begin{bmatrix} \zeta & 0 \\ 0 & \overline{\zeta} \end{bmatrix}$. The action of any of (1 2), (1 2)(1 2 3), or (1 2)(1 3 2) permute $1 \otimes \mathbb{C}$ and $\sigma \otimes \mathbb{C}$, so it has a matrix $\begin{bmatrix} 0 & B \\ A & 0 \end{bmatrix}$, so the trace is zero, and $\chi_{i_H^G(\rho)}((1\ 2)) = 0$ (and similarly for the other two). Thus, the character table must be the same one given in Table 2. What's significant here is that this representation can be constructed from simpler ones; next lecture, a formula for constructing the characters of induced representations will be shown.

Notice that $H \trianglelefteq G$ was assumed, which mean the left action of H on G/H is trivial. More generally, if $x \in gH \in G/H$, the stabilizer G_x is a little more complicated.

17. Induction of Characters: 5/28/13

Let ρ be a (complex) representation of H, where $H \leq G$. Then, recall that χ_ρ is a class function on H, and the induced representation $i_H^G(\rho)$ is given by taking ρ as a $\mathbb{C}[G]$-module, giving $i_H^G(\rho) = \mathbb{C}[G] \otimes_{\mathbb{C}[H]} \rho$. It turns out that its character can be computed by a formula:

$$\chi_{i_H^G(\rho)}(s) = \frac{1}{|H|} \sum_{\substack{t \in G \\ t^{-1}st \in H}} \chi_\rho(t^{-1}st). \tag{7}$$

Example 17.1. For example, if $H = \{e\}$, then ρ is just a k-dimensional vector space, and $i_H^G(\mathbb{C}^k) = \mathbb{C}[G]^k$, which is just k copies of the regular representation. This is because $i_H^G(V \oplus W) = i_H^G(V) \oplus i_H^G(W)$ because direct sums and tensor products distribute. Then,

$$\chi_{\mathbb{C}[G]}(s) = \begin{cases} |G|, & s = e \\ 0, & \text{otherwise.} \end{cases}$$

The induced character is taken over all $tst^{-1} = e$, so that $t = e$, but this just means $\chi_{i_{\{e\}}^G}(s)$ is equal to $\chi_{\mathbb{C}[G]}$ above.

Example 17.2. For another example, if $H = G$, then $i_G^G(\rho) = \rho$, and

$$\begin{aligned} \chi_{i_G^G(\rho)}(s) &= \frac{1}{|G|} \sum_{\substack{t \in G \\ t^{-1}st \in G}} \chi_\rho(t^{-1}st) \\ &= \frac{1}{|G|} \sum_{t \in G} \chi_\rho(s), \end{aligned}$$

because $t \in G$ iff $t^{-1}st \in G$, and χ_ρ is a class function. This simplifies to

$$= \frac{1}{|G|} |G| \chi_\rho(s) = \chi_\rho(s).$$

That result makes sense.

A proof sketch for (7) will be given. In the left action of H on the cosets G/H, the stabilizers $G_{gH} = gC_H g^{-1} = gHg^{-1}$. Then,

$$i_H^G(\rho) = \bigoplus_{x \in G/H} \rho = \bigoplus_{x \in G/H} V_x,$$

where the $V_x \subseteq i_H^G(\rho)$ and $\sum V_x = i_H^G(\rho)$. The elements of G permute these summands V_x, so $gV_x = V_{gx}$.

Suppose some $g \in G$ weren't contained in any conjugate $\gamma H \gamma^{-1}$ of H, so that it doesn't fix any of the V_x, instead permuting them all. Thus, its matrix has zeros along the diagonal, so its trace is zero, so it doesn't affect the value of the character. Thus, we only care about $g \in tHt^{-1}$ with $t \in G$.

Conversely, if $g \in tHt^{-1}$ for some $t \in G$, then its matrix does have some nonzero entry or entries along the diagonal. Then, in H,

$$\mathrm{Tr}(g) = \sum_{\substack{t \in G \\ g \in tHt^{-1}}} \mathrm{Tr}(t^{-1}gt).$$

The rest of the argument is counting and bookkeeping, but the key idea is to take the diagonal elements in the matrix of a given G. The $1/|H|$ term occurs because each term is overcounted: if $t^{-1}st \in H$, then $(th)^{-1}s(th) \in H$ as well for any $h \in H$, and gives the same contribution.

Example 17.3. Once again consider $\Sigma_3 \geq \mathbb{Z}/3$. Let ρ is the $\mathbb{C}$-representation with character $\chi_\rho(1\ 2\ 3) = \zeta$, where $\zeta^2 = \overline{\zeta}$, such as $\zeta = 1/2 + i\sqrt{3}/2$. Then, using (7), if $\sigma \in \Sigma_n$ is a transposition, then it isn't conjugate to anything in $\mathbb{Z}/3$, so $\chi_{i_{\mathbb{Z}/3}^{\Sigma_3}(\rho)}(\sigma) = 0$. Otherwise, $\sigma \in \mathbb{Z}/3$, so $\chi(\sigma) = (1/3)\sum \chi_\rho(\tau^{-1}\sigma\tau)$. There are six choices of τ, three of which send ζ to $(1\ 2\ 3)$, and the other three of which send $\zeta \mapsto (1\ 3\ 2)$. Thus, the value becomes $\zeta + \zeta^{-1}$.

In general, this sort of computation can be done by a computer, since the formula is reasonably straightforward to implement.

There's a very interesting and useful property called Frobenius reciprocity: suppose $H \leq G$, and V is a complex[14] representation of G, and W is a complex representation of H. Then, does V occur in a summand of $i_H^G(W)$ for some W? This question involves understanding larger representations in terms of smaller ones. If V is irreducible, this is equivalent to asking whether there exists a nontrivial homomorphism $i_H^G(W) \to V$. The object of study is thus $\mathrm{Hom}_{\mathbb{C}[G]}(i_H^G(W), V) = \mathrm{Hom}_{\mathbb{C}[G]}(\mathbb{C}[G] \otimes_{\mathbb{C}[H]} W, V) \cong \mathrm{Hom}_{\mathbb{C}[H]}(W, V|_H)$, by the universal property of the tensor product, and the restriction $V|_H$ taken as a representation. This connection is known as Frobenius reciprocity.

Suppose ρ and η are representations over k of a group G. Then, $\rho \otimes_k \eta$ is a k-vector space, but it is also a module over $k[G \times G] = k[G] \otimes_k k[G]$, with action $(g_1, g_2) \cdot (v \otimes w) = g_1 v \otimes g_2 w$, or $(g_1 \otimes g_2)(v \otimes w) = (g_1 v \otimes g_2 w)$. Thus, the diagonal map $\Delta : g \mapsto (g, g)$ gives a homomorphism $k[G] \xrightarrow{k[\Delta]} k[G \times G] \cong k[G] \otimes k[G]$. Using restriction of scalars along $k[\Delta]$, one can thus obtain a G-representation $\rho \otimes \eta$. Thus, representations can in some sense be multiplied.

On characters, this is just the pointwise product $\chi_{\rho_1 \otimes \rho_2} = \chi_{\rho_1} \cdot \chi_{\rho_2}$, because $\mathrm{Tr}(M \otimes N) = \mathrm{Tr}(M)\mathrm{Tr}(N)$ for matrices M and N, as in the following example:

$$\begin{array}{c} \\ e_1 \\ e_2 \end{array} \begin{array}{c} \begin{array}{cc} e_1 & e_2 \end{array} \\ \begin{pmatrix} a & b \\ c & d \end{pmatrix} \end{array} \otimes \begin{array}{c} \\ f_1 \\ f_2 \end{array} \begin{array}{c} \begin{array}{cc} f_1 & f_2 \end{array} \\ \begin{pmatrix} e & f \\ g & h \end{pmatrix} \end{array} = \begin{array}{c} \\ e_1 \otimes f_1 \\ e_1 \otimes f_2 \\ e_2 \otimes f_1 \\ e_2 \otimes f_2 \end{array} \begin{array}{c} \begin{array}{cccc} e_1 \otimes f_1 & e_1 \otimes f_2 & e_2 \otimes f_1 & e_2 \otimes f_2 \end{array} \\ \begin{pmatrix} ax & & & \\ & aw & & \\ & & dx & \\ & & & dw \end{pmatrix} \end{array}$$

so the trace is a product. (The rest of the rightmost matrix is stuff that isn't important to the final calculation and has been omitted.) Thus, the characters almost form a ring, except for the absence of additive inverses. This can be fixed by considering virtual characters, which are just negatives of regular characters. This is perfectly valid, since they're complex-valued class functions, so one obtains an abelian group and therefore a ring. This character ring is denoted $R[G]$.

Example 17.4. If $G = \mathbb{Z}/2$, there are the characters ε and σ, corresponding to the trivial and sign representations, with character table as in Table 3.

TABLE 3. Character table for $\mathbb{Z}/2$.

	1	T
ε	1	1
σ	1	-1

[14] There is a version of this that holds in other fields, though.

As always, the trivial representation is the identity. Then, since $\sigma^2(1) = 1$ and $\sigma^2(-1) = 1$, then $\sigma^2 = \varepsilon$. In this case, $R[G] \cong \mathbb{C}[G]$.

Σ_3 is a little more interesting. The ring $R[\Sigma_3]$ has generators and relations $\sigma^2 = \varepsilon$ and $\rho^2 = \rho + \varepsilon + \sigma$, with the representations as in Table 1, and with the calculation shown in Table 4.

TABLE 4. Showing that $\chi_\varepsilon + \chi_\sigma + \chi_\rho = \chi_\rho^2$.

	χ_ε	χ_σ	χ_ρ	χ_ρ^2
1	1	1	2	4
(1 2 3)	1	1	−1	1
(1 3 2)	1	1	−1	1
(1 2)	1	−1	0	0
(1 3)	1	−1	0	0
(2 3)	1	−1	0	0

As in the above example, when $H \leq G$, induction gives a homomorphism $i_H^G : R[H] \to R[G]$.

Suppose one has a family of subgroups $\mathscr{F}$ of G that covers G (i.e. every $g \in G$ lies in some $H \in \mathscr{F}$). For example, one might have the cyclic subgroups of G. Then, there is a homomorphism

$$\bigoplus_{H \in \mathscr{F}} R[H] \xrightarrow{\sum i_G^H} R[G].$$

The idea here is that the representations of elements of $\mathscr{F}$ are better understood than those of G, and this homomorphism is useful. However, it isn't necessarily surjective. However, there is the following result:

Theorem 17.1 (Artin)**.** *The induced homomorphism*

$$\bigoplus_{H \in \mathscr{F}} R[H] \otimes_{\mathbb{Z}} \mathbb{Q} \to R[G] \otimes_{\mathbb{Z}} \mathbb{Q}$$

is surjective.

There is also a much, much harder theorem that is slightly more general.

18. Different Directions in Representation Theory: 5/30/13

Recall that we have the representation (character) ring $R[G]$, additively generated by the irreducible characters, and with multiplication given by the tensor product. If $H \to G$ is a group homomorphism, then one has the pullback map $R[G] \to R[H]$ given by restriction of representations, which is a ring homomoprhism. The induction map $i_H^G : R[H] \to R[G]$ is a group homomorphism, but not necessarily a ring homomorphism.

If $\mathscr{F}$ is a family of subgroups of G, as in the previous lecture, it's useful to understand the image of $\bigoplus_{H \in \mathscr{F}} R[H] \to G$ to understand more complicated representations in terms of simpler ones. Recall also Frobenius reciprocity, which says many things, including in particular $\langle V, i_H^G W \rangle = \langle V|_H, W \rangle$, where W is a representation of H, and V is a representation of $G \geq H$, the restriction is as representations, and the inner product is as class functions. Now, the proof of Theorem 17.1 can be formulated.

Proof of Theorem 17.1. Let $\theta = \sum i_H^G \otimes \mathrm{id}_{\mathbb{Q}}$ and suppose $x \in R[G] \otimes \mathbb{Q}$, but $x \notin \mathrm{Im}(\theta)$. In an inner product space, one has projections, so write $x = x^\perp + x^\pi$, where $x^\perp$ is perpendicular to $\mathrm{Im}(\theta)$ and $x^\pi \in \mathrm{Im}(\theta)$.[15] Since $x \notin \mathrm{Im}(\theta)$, then $x^\perp \neq 0$. In particular, for all $H \in \mathscr{F}$ and $W \in R[H]$, $\langle x^\perp, i_H^G(W) \rangle = 0$, but by Frobenius reciprocity, $\langle x^\perp|_H, W \rangle = 0$ for any representation W of H.

Thus, $x^\perp|_H = 0$, since it dots to zero with every element of the inner product space, and this is true for all $H \in \mathscr{F}$, so for any $g \in H$ and $H \in \mathscr{F}$, the value of the virtual character $x^\perp$ is zero. Thus, $x^\perp|_{\langle g \rangle} = 0$ for all $g \in G$, because $\mathscr{F}$ covers G, and therefore $x^\perp = 0$. ⊠

The tensoring with $\mathbb{Q}$ doesn't seem to have explicitly happened, but it was necessary in order to write $x = x^\perp + x^\pi$, since one must be able to divide by things. There is a much harder theorem by R. brauer that doesn't require $\otimes\mathbb{Q}$, and gives surjectivity with a larger family of subgroups.

Definition. A group G is regular if it can be written as $G \cong C \times H$, where C is a cyclic group and H is a p-group for some p.

[15] One way to do this is to choose an orthonormal basis and work in it.

Theorem 18.1 (R. Brauer)**.** *The map*

$$\bigoplus_{\substack{H\leq G\\ H \text{ regular}}} R[H] \xrightarrow{\sum i_H^G} R[G]$$

is surjective.

Thus, a representation of any group can be described in terms of its regular subgroups, though this still encodes some complexity, because regular subgroups aren't all that simple. But there's another pretty theorem.

Theorem 18.2 (Blickfeldt[16])**.** *Let G be a p-group. Then, for any irreducible representation ρ of G, there is a subgroup H of G and a one-dimensional representation σ of H sich that $i_H^G(\sigma) = \rho$.*

This is a really precise statement, and has pretty nice consequences from the definition of induction: every irreducible representation, and therefore every representation, of a p-group is monomial (that is, given by monomial matrices, which are those with one nonzero element in every row and column), and the entries are all p^{th} roots of unity. Thus, these representations look somewhat like permutation representations.

There's a whole direction called modular representation theory[17] which discusses the representation theory of finite groups over finite fields. When $|G|$ is prime to $\text{Char}(F)$ Wedderburn's theorem still holds, which is fine, but it becomes more complicated otherwise (e.g. the $\mathbb{F}_2$-representation theory of Σ_3),

But there's yet another extnesion that goes beyond finite groups. What do representations of $\mathbb{Z}$ look like? This is determined by choosing where 1 goes, so an n-dimensional representation of $\mathbb{Z}$ is the same as a choice of a conjugacy class of invertible matrices. Over $\mathbb{C}$, we have seen this is the Jordan normal form, but there are notions of topology and continuity on these representations: $\mathbb{C}^*$ determines one-dimensional representations of $\mathbb{Z}$, but it has geometric and topological structure, so the set of representations becomes a space, called a moduli space or representation variety. Since it's no longer a finite list, the answers aren't as conclusive. One could even have deformations of representations, whereas the discreteness of the finite case makes it rigid.

One specific direction which is particularly useful in physics is to take compactness as a replacement for finiteness: one considers compact topological groups, or specifically compact Lie groups, which have a manifold structure, such as S^2, $\text{O}(n)$, $\text{SO}(n)$, $\text{U}(n)$, $\text{SU}(n)$, and so on. For these, Maschke's theorem roughly holds, because of compactness. Thus, for a finite-dimensional representation of a compact Lie group, there exists a unique direct-sum decomposition into irreducible representations, though there are infinitely many such irreducible representations.

Example 18.1. Consider the circle group S^1 or $\text{SO}(2)$. One can send ζ to itself in $\text{U}(1)$, which is a one-dimensional complex representation. Call this representation ρ. There's also the n^{th} power map given by wrapping S^1 around itself n times, giving a representation $S^1 \xrightarrow{\times n} S^1 \xrightarrow{\rho} \text{U}(1)$, or the n^{th} tensor power $\rho^{\otimes n}$, given by sending $\zeta \mapsto \zeta^n$, or compose with complex conjugation on S^1. For each integer, there is one of these representations.

Once again, there is a representation ring that is built in the same way. Then, it turns out that $R[S^1] = \mathbb{Z}[\mathbb{Z}]$, or the group ring of $(\mathbb{Z}, +)$ over itself as a ring, which is equal to the ring of Laurent polynomials $\mathbb{Z}[t^{\pm 1}]$. This has much more obvious importance than for finite groups, because if one takes functions on a circle, such as $L^2(S^1)$, which is an infinite-dimensional $\mathbb{C}$-vector space, they are acted on by S^1 as $(\zeta f)(z) = f(\zeta z)$. This can be rewritten as $L^2(S^1) = \prod_{-\infty}^{\infty} \rho^n$, which is just the Fourier decomposition! Thus, the notion of Fourier series and bases for function spaces can be generalized, so that one wants to pick bases arising from the symmetries of the object.

Example 18.2. $\text{SO}(3)$ acts on the 2-sphere S^2, so some natural representations can be considered. Take the polynomials in x, y, z, but only consider the harmonic functions.[18] The action of $\text{SO}(3)$ commutes with the Laplacian Δ, so it preserves harmonic polynomials. This gives an irreducible representation of $\text{SO}(3)$ with a basis of harmonic functions on S^2, or spherical harmonics, which turn out to be very useful. This does generalize to S^n.

Notice that the presence of symmetry leads to useful bases for functions. The representation rings of all compact, connected Lie groups are known, because such Lie groups can be classified: for example, the representation ring of $\text{SO}(3)$ is a polynomial ring in one variable: $R[\text{SO}(3)] = \mathbb{Z}[u]$, given by taking the action on $\mathbb{R}^3$ and tensoring it up to $\mathbb{C}$. The representation rings of Lie groups tend to be polynomial rings, sometimes with the Laurent twist.

This is an active field of research, even with more general groups such as $\text{GL}(n)$. For a text on this material, consult Bröcker and tom Dieck, *Representations of Compact Lie Groups*.

[16] Blickfeldt was at Stanford in the 1920s and 1930s.

[17] Some of which popped up on the exam.

[18] A function f defined to be harmonic if $\Delta f = \dfrac{\partial^2 f}{\partial x^2} + \dfrac{\partial^2 f}{\partial y^2} + \dfrac{\partial^2 f}{\partial z^2} = 0$.