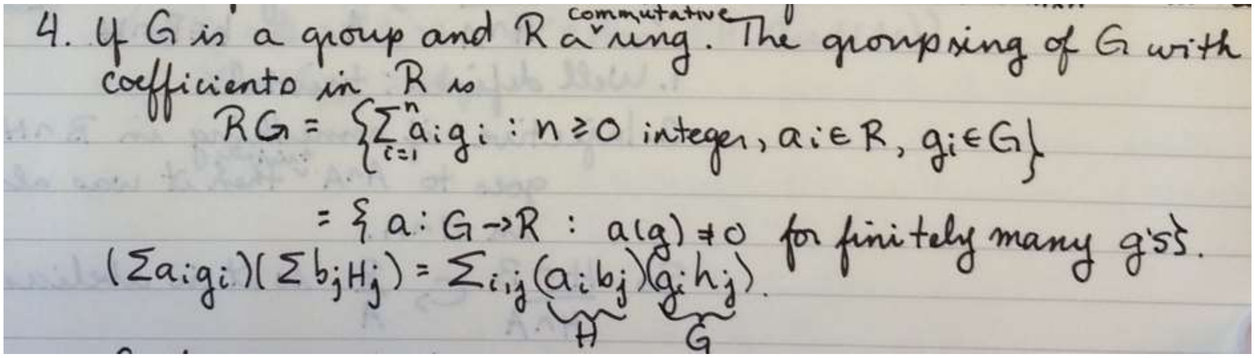
Text in purple = things that Prof. Dror Bar Natan said in class.

NOTE: None of the pictures are mine. Most of them are from Yvonne's notes that are posted on the class webpage.

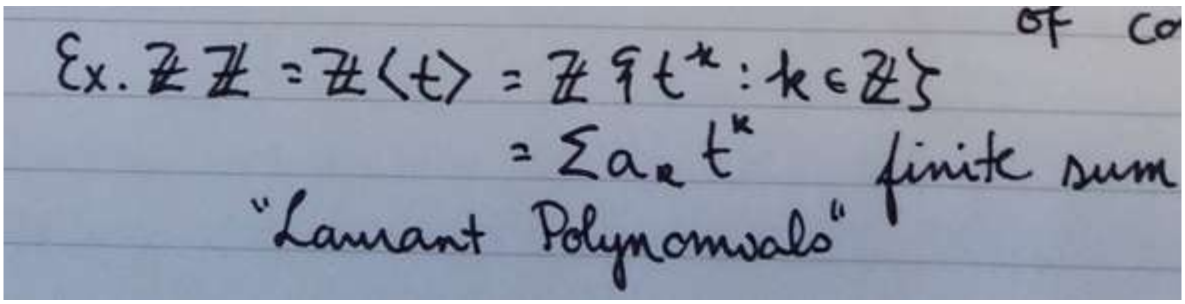
Thursday, October 23rd

Examples of rings



4. If G is a group and R a commutative ring. The groupring of G with coefficients in R is

$$RG = \left\{\sum_{i=1}^{n} a_i g_i : n \geq 0 \text{ integer}, a_i \in R, g_i \in G\right\}$$
$$= \{a : G \to R : a(g) \neq 0 \text{ for finitely many } g\text{'s}\}.$$
$$\left(\sum a_i g_i\right)\left(\sum b_j H_j\right) = \sum_{i,j} \underbrace{(a_i b_j)}_{H}\underbrace{(g_i h_j)}_{G}.$$

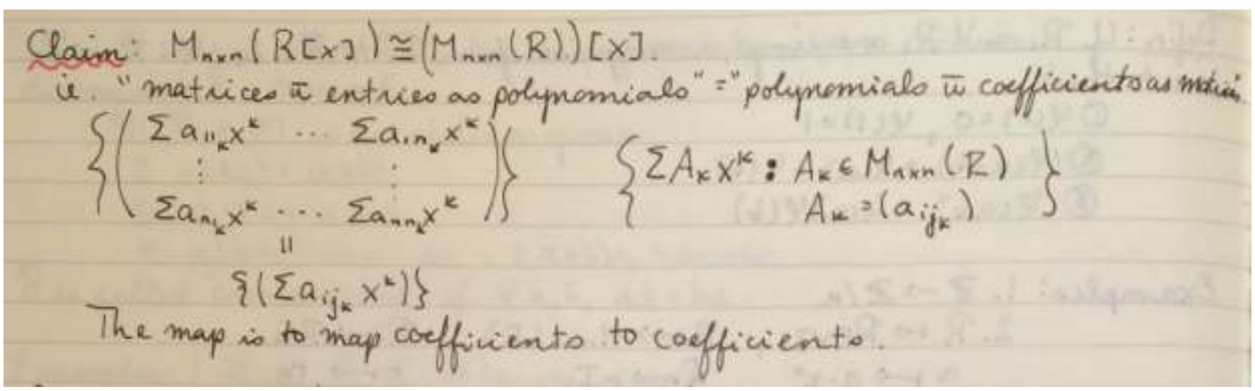


of co

$$\text{Ex. } \mathbb{Z}\mathbb{Z} = \mathbb{Z}\langle t\rangle = \mathbb{Z}\{t^k : k \in \mathbb{Z}\}$$
$$= \sum a_k t^k \quad \text{finite sum}$$

"Laurant Polynomials"

Monday, October 27th



Claim: $M_{n\times n}(R[x]) \cong (M_{n\times n}(R))[x]$.

i.e. "matrices w/ entries as polynomials" = "polynomials w/ coefficients as matrices"

$$\left\{\begin{pmatrix} \sum a_{11_k}x^k & \cdots & \sum a_{1n_k}x^k \\ \vdots & & \vdots \\ \sum a_{n1_k}x^k & \cdots & \sum a_{nn_k}x^k \end{pmatrix}\right\} \qquad \left\{\sum A_k x^k : A_k \in M_{n\times n}(R),\ A_k = (a_{ij_k})\right\}$$
$$\| $$
$$\{(\textstyle\sum a_{ij_k} x^k)\}$$

The map is to map coefficients to coefficients.

Caley-Hamilton Theorem

Cayley-Hamilton: "A matrix annihilates its characteristic polynomial"

Let $A \in M_{n\times n}(R)$ R is a commutative ring.

$$\underset{\sum a_k t^k}{\underset{\parallel}{R[t]}} \ni \chi_A(t) := \det(\underbrace{tI - A}_{\begin{pmatrix} t-a_{11} & -a_{12} & \cdots & -a_{1n} \\ -a_{21} & t-a_{22} & \cdots & -a_{2n} \\ \vdots & & & \vdots \\ -a_{n1} & -a_{n2} & \cdots & t-a_{nn} \end{pmatrix} \in M_{n\times n}(R[t])})$$

$$\det(a_{ij}) = \sum_{\sigma} (-1)^{\sigma} \prod_{i=1}^{n} a_{i\sigma j}$$

$a_{ij} \in S$

Claim: $\chi_A(A) = 0$ ie $\sum a_k A^k = \chi_A(A) = 0$.

Wrong Proof #1:

Diagonalize matrix A, so the entries on the diagonal are the eigenvalues. Since the characteristic polynomials annihilates eigenvalues, it follows.

This is not our proof since we haven't talked about diagonalization, and the ring can be any commutative ring, so we can't diagonalize, and we can't use eigenvalues and eigenvectors.

Wrong Proof #2:

Wrong Proof: $\chi_A(A) = \det(AI - A)$
$= \det(0) = 0.$

You're putting a matrix in a matrix.
The LHS is a matrix and the RHS a scalar so the evaluation makes no sense.
We also didn't use properties of determinant, so this would also be true for the characteristic polynomial defined by trace:

Basically, it's saying that if we could just sub in A into det (tI – A), then we could also sub in A into tr (tI – A), and then the calculation doesn't make sense.

Facts needed for the correct proof:

Definition of Adj A:

Aside: Adj A = "transpose of matrix of minors"
$$= \left((-1)^{i+j}\cdot A_{ji}\right)_{ij} \qquad A_{ji} = \det(A) \text{ removing row } j \text{ and column } i.$$

Fact about adj A:

$$A\cdot \operatorname{adj} A = \operatorname{adj} A \cdot A = \det(A)\cdot I. \text{ over any commutative } R.$$

You should have seen this proof in previous courses. The proof of this fact is entirely algebraic, and it doesn't use anything except for addition and multiplication. The entries of A adj A can be reinterpreted as the determinants of the original matrix minus the row of I and column of j and replaced by other things. It's entirely algebra, so it's true over any commutative ring R.

Correct proof:

Main idea of correct proof:

Sub in A into this equation:

$$\chi_A(t)\cdot I = \det(tI-A)I = \left(\sum B_i t^i\right)\cdot\left(tI - At^0\right)$$

Full correct proof:

$$\det(tI-A)\cdot I \overset{\text{in } M_{n\times n}(R[t])}{=} \operatorname{adj}(tI-A)(tI-A) \overset{\text{in } M_{n\times n}(R)[t]}{=} \left(\sum B_i t^i\right)(tI-A) \qquad (*)$$

The second equality there is from the isomorphism $M_{n\times n}(R[x]) \cong (M_{n\times n}(R))[x]$.

Recall that the evaluative map is defined by:

Aside: if S is commutative,
$$ev_u : S[x] \to S.$$
$$\sum a_i x^i \mapsto \sum a_i u^i$$

We would like to use the evaluation map and substitute the matrix A into (*). But the evaluation map is a ring homomorphism only if the A commute with the Bi’s. They’re matrixes, so even if the ring itself is commutative, we would still have to prove that the matrices commute.

We’ll prove this in the lemma (and R doesn’t have to be commutative):

Lemma: All the B_i's commute with A.

Proof of Lemma: $(tI - A)\,\mathrm{adj}(tI - A) = \mathrm{adj}(tI - A)(tI - A)$

$$\Rightarrow (tI - A)(\sum B_i t^i) = (\sum B_i t^i)(tI - A)$$

$$\Rightarrow A \sum B_i t^i = (\sum B_i t^i) A$$

$$\Rightarrow \forall i \; AB_i = B_i A.$$

The first line of the proof is because $A \cdot \mathrm{adj}\, A = \mathrm{adj}\, A \cdot A = \det(A) \cdot I$.

Using this lemma, we finish the proof of the Caley Hamilton theorem by evaluating (*) at A:

Hence under ev_A

$$\chi_A(\cancel{A}t) \cdot I = (\sum B_i t^i)(t \cdot I - A t^0)$$

$$\Rightarrow \chi_A(A) \cdot I = (\sum B_i A^i)(A I - A I)$$

$$= 0.$$

Thursday, October 30

Things covered:

4 isomorphism theorems for rings

Theorem: I is maximal if and only if R/I is a field.

Proof:

Maximal => Field:

Show that x + I (nonzero) has an inverse.

Consider <x> + I. 1 + I is in this ideal, since I is maximal, so [x][y] = [1].

Field => Maximal:

Monday, November 3rd

Things covered:

Thursday, November 6th

Things covered:

A ring R is **Noetherian** if every ascending sequence of ideals in it is eventually constant.

Proposition: A PID is Noetherian.

Proof: Consider I = U I_k. There exists n such that x \in I_n, so I = I_n.

Theorem: PID => UFD

Weak proof of theorem:

Build a strictly increasing chain (x1) \subset (x2) …

Take x1 nonunit, use axiom of choice to find maximal ideal M1 = (p1) containing (x1), so x1 = p1x2, and continue with x2. If it terminates (i.e., xn is a unit), then we're done. If not, since a PID is Noetherian, (xn) = (xn+1), so xn+1 = rxn = rpnxn+1 => rp = 1, so p is a unit. Contradiction.

Proposition: In a PID, <a,b> = <gcd (a,b)>.

Proof: <a,b> = <c> for some c, then use property of gcd to show <gcd (a,b)> \subset <c>.

Monday, November 10th

Direct Sums

The direct sum of two modules is easy:

Direct Sums: given two modules over the same ring M, N can construct new module

$M \oplus N = \{(m,n) : m \in M, n \in N\}$ s.t.

$(m_1, n_1) + (m_2, n_2) = (m_1 + m_2, n_1 + n_2)$

$a(m,n) = (am, an).$

(Don't mix these operations up with the tensor product! In particular, you can't add coordinates like this in a tensor product).

With an infinite number of modules, there are two definitions:

Definition 1:

$\bigoplus M_\alpha := (0 \ldots 0$ finitely many not zero$)$

maps

$$\begin{tikzcd} M \arrow[dr, "m \mapsto (m,0)"] \arrow[drr, bend left, "\alpha"] & & \\ & M \oplus N \arrow[r, "\exists! \gamma"] & P \\ N \arrow[ur, "n \mapsto (0,n)"'] \arrow[urr, bend right, "\beta"'] & & \end{tikzcd}$$

Given α, β $\exists! \gamma$ making the diagram commutative

$\gamma(m,n) = \gamma((m,0) + (0,n))$

$= \alpha(m) + \beta(n)$

is defn determines $M \oplus N$.

In category theory, this is a coproduct.

This definition works with finitely many coordinates not zero because gamma is defined by summing up the m_i's, so the sum is defined only with finitely many coordinates not zero.

Definition 2:

$\prod M_\alpha = ($arbitrary sequence$)$.

$$\begin{tikzcd} & & M \\ P \arrow[r, "\exists! \gamma"] \arrow[urr, bend left, "\alpha"] \arrow[drr, bend right, "\beta"'] & M \oplus N \arrow[ur, "\pi_1", "(m,n) \mapsto m"'] \arrow[dr, "\pi_2"', "(m,n) \mapsto n"] & \\ & & N \end{tikzcd}$$

similar to "def by coordinates"

$\gamma(P) = (\alpha(p), \beta(p))$

Homomorphisms of Direct Sums

For finite direct sums, it's obvious that:

$$\mathrm{Hom}\Big(\bigoplus_{j=1}^{n} N_j, \bigoplus_{i=1}^{m} M_i\Big) = \prod_{j=1}^{n} \mathrm{Hom}\big(N_j, \oplus M_i\big) = \prod_{j=1}^{n} \prod_{i=1}^{m} \mathrm{Hom}(N_j, M_i)$$

$$\sim \left\{ \underbrace{\begin{pmatrix} a_{11} & \cdots & a_{1n} \\ \vdots & a_{ij} & \vdots \\ a_{m1} & \cdots & a_{mn} \end{pmatrix}}_{n} \Big\} m : a_{ij} \in \mathrm{Hom}(N_j, M_i) \right\}$$

$$\begin{pmatrix} a_{11} & \cdots & a_{1n} \\ \vdots & & \vdots \\ a_{m1} & \cdots & a_{mn} \end{pmatrix} \begin{pmatrix} v_1 \\ \vdots \\ v_n \end{pmatrix} = \begin{pmatrix} a_{11}(v_1) + a_{12}(v_2) + \overset{n}{\cdots} + a_{1n}(v_n) \\ \vdots \end{pmatrix}$$

GCD/LCM lemma

Claim: If $\gcd(a,b) = 1$ then

$$\frac{R}{\langle ab \rangle} \cong \frac{R}{\langle a \rangle} \oplus \frac{R}{\langle b \rangle}$$

Proof 1:

$$\begin{pmatrix} 1 & 0 \\ 0 & ab \end{pmatrix} \sim \begin{pmatrix} a & 0 \\ 0 & b \end{pmatrix}$$

Proof 2:

In general,

Claim: (in a PID) if $g = sa + tb$ (guaranteed in a PID) then (#)

$$\frac{R}{\langle a \rangle} \oplus \frac{R}{\langle b \rangle} \cong \frac{R}{\langle g \rangle} \oplus \frac{R}{\langle \ell \rangle}$$

Proof by defining the isomorphisms explicitly using matrices:

$\langle a\rangle \quad \langle B\rangle \quad \langle ab\rangle$ module)

Proof: $\xrightarrow{\rho} \begin{pmatrix} s & t \\ -b/g & a/g \end{pmatrix}$ $\quad s: R/\langle a\rangle \to R/\langle g\rangle \quad t: R/\langle b\rangle \to R/\langle g\rangle$ $\quad -b/g: R/\langle a\rangle \to R/\langle \ell\rangle \quad a/g: R/\langle b\rangle \to R/\langle \ell\rangle$ } all well defined.

$\xleftarrow{\lambda} \begin{pmatrix} a/g & -t \\ b/g & s \end{pmatrix}$

$$\begin{pmatrix} a/g & -t \\ b/g & s \end{pmatrix}\begin{pmatrix} R/\langle g\rangle \\ R/\langle \ell\rangle \end{pmatrix} \to \begin{pmatrix} R/\langle a\rangle \\ R/\langle b\rangle \end{pmatrix}$$

Both maps are well defined The only thing left to check is that they are inverses of each other.

$$\begin{pmatrix} s & t \\ -b/g & a/g \end{pmatrix}\begin{pmatrix} a/g & -t \\ b/g & s \end{pmatrix} = \begin{pmatrix} \frac{sa+tb}{g} & 0 \\ 0 & \frac{bt+as}{g} \end{pmatrix} = \begin{pmatrix} 1 & 0 \\ 0 & 1 \end{pmatrix}$$

Fundamental Theorem for Finitely Generated Modules

Our goal is to prove:

$$M \text{ f.g } / \text{PID } R \Rightarrow M \cong R^k \oplus \bigoplus R/\langle p_i^{s_i}\rangle \quad p_i \text{ prime } s_i \in \mathbb{Z}_{>0}$$

Main idea of the proof:

Step 1: Show that M is associated with a matrix A. (Roughly speaking, A is associated with the “kernel of M”. We will define this specifically.)

Step 2: Show that if we use row operations on the matrix A to get another matrix A’, M will also be associated with the matrix A’.

Step 3: Show that we can map A to PAQ repeatedly to get to a matrix of this form: $\begin{pmatrix} a_1 & & & & & \\ & a_2 & & & & \\ & & \ddots & & & \\ & & & a_n & & \\ & & & & 0 & \\ & & & & & \ddots \\ & & & & & & 0 \end{pmatrix}$, where P and Q are invertible matrices.

Since M is associated with this matrix $\begin{pmatrix} a_1 & & & & & \\ & a_2 & & & & \\ & & \ddots & & & \\ & & & a_n & & \\ & & & & 0 & \\ & & & & & \ddots \\ & & & & & & 0 \end{pmatrix}$, $M \cong R^k \oplus \bigoplus R/\langle p_i^{s_i}\rangle$.

Details of the proof:

Step 1

Defining the obvious map for a finitely generated module, R^n -> M:

$\begin{pmatrix} a_1 \\ \vdots \\ a_n \end{pmatrix} \mapsto \sum a_i g_i \qquad M = \operatorname{im}\pi \cong R^n/\ker\pi.$

$R^n \overset{\pi}{\twoheadrightarrow} M \qquad \ker\pi = \langle r_x : x \in X\rangle$ → not claiming finite.

Let X be a generating set for ker pi, so that any element in ker pi can be written as rx for some r \in R and x \in X.

Defining another map from X -> R:

$\{a: X \to R;\ a(x) \neq 0 \text{ for finitely many } x\text{'s}\} = R^X \xrightarrow{A} R^n \underset{\pi}{\twoheadrightarrow} M.$

Explaining this map in details:

$R^X = \{a: X \to R;\ a(x) \neq 0 \text{ for finitely many } x\text{'s}\}$

We have a map A: R^X -> R^n by defining A(b) = $\sum_{x\in X} b(x)x.$, where b is in R^x. This sum is finite because b(x) \neq 0 for finitely many x's, and $\sum_{x\in X} b(x)x.$ is in R^n because b(x) is in R and x is in ker pi (which is in R^n), so $\sum_{x\in X} b(x)x.$ is a sum of elements in R^n.

$\operatorname{im} A = \ker \pi$ and $M := R^n/\operatorname{im} A.$

Since X is a generating set for ker pi, the image of A is ker pi.

M is isomorphic to R^n/im A:

By the first isomorphism theorem, pi is surjective, so R^n/ker pi = M. But ker pi = im A, so we also know that R^n/im A = M.

A can be interpreted as an $n \times X$ matrix

finite

finite rows, infinitely many columns.

$R^X = \langle e_x \rangle = \begin{pmatrix} 0 \\ 1 \\ 0 \\ x \\ 0 \\ \vdots \end{pmatrix}_x$

A can be interpreted as an n x X matrix because A maps R^|X| to R^n. An n x X matrix maps something that's |X| dimensional to something that's n dimensional. Furthermore, in each row, there are only finitely many non-zero entries, since anything in R^X only has finitely many non-zero entries (so if we take A(e_x) for each x, we would be summing up only finitely many non-zero entries).

Furthermore, every $n \times X$ matrix A defines a finitely generated module

The finitely generated module is just the image of the matrix A (i.e., the column space), then projected by the map pi.

Examples: $A = (1) \rightsquigarrow M = R^1/\operatorname{im} 1\cdot = \{0\}$.

$A = (a) \rightsquigarrow M = R^1/\operatorname{im} a\cdot = R/\langle a\rangle$

$A = (0) \rightsquigarrow M = R^1/\operatorname{im}(0) = R/\{0\} = R$.

4. $C = \left(\begin{array}{c|c} A & 0 \\ \hline 0 & B \end{array}\right)$ $M_C = M_A \oplus M_B$.

Thursday November 13

Every f.g module is M_A for some A.

M is f.g $\Rightarrow \phi : R^n \twoheadrightarrow M$!

$\Rightarrow M = R^n/\ker\varphi$

Take $X = \ker\varphi$.

$R^X \to R^n$: by $e_x \mapsto x$

Last time, we noted that A defines a finitely generated module, and this is the converse. Given a finitely generated module, take X = ker pi (where pi is the obvious projection map). Then define A: R^X -> R^n by mapping the basis elements of X to itself (since we took the generating set of ker pi X to be the whole set ker pi, it makes sense).

Step 2

$$\text{Claim: } \begin{tikzcd} R^X \arrow[r, "A"] \arrow[dr, phantom, "\circlearrowright"] & R^n \arrow[d, "P"] \\ \underset{\sim}{R}^X \arrow[u, "Q"] \arrow[r, "A'"'] & R^n \end{tikzcd}$$

$P \in M_{n\times n}(R)$ $Q \in M_{X\times X}(R)$

If P and Q are invertible, then $M_A = M_{A'}$

We would like to show that if we had such a commutative diagram, then the modules that are generated are equal.

Proof:
$$\begin{tikzcd} R^X \arrow[r, "A"] & R^n \arrow[r] \arrow[d, "P"] & R^n/\operatorname{im} A = M_A \arrow[d, dashed, shift left, "\rho"] \\ R^X \arrow[u, "Q"] \arrow[r, "A'"'] & R^n \arrow[r] & R^n/\operatorname{im} A' = M_{A'} \arrow[u, shift left, "\lambda"] \end{tikzcd}$$

ρ defined w̄ P and so well defined
λ defined w̄ P^{-1} and so well defined.

To show that $M_A \cong M_{A'}$.:

Define an isomorphism $\Phi : M_A \to M_{A'}$ by $\Phi([a]_{\operatorname{im} A}) = [P\alpha]_{\operatorname{im} A'}$., where \alpha \in R^n.

To show that this map is well-defined, we show that if $[\alpha]_{\operatorname{im} A} = 0$ then $[P\alpha]_{\operatorname{im} A'} = 0$. If $[\alpha]_{\operatorname{im} A} = 0$, then

. $\alpha \in \operatorname{im} A$ so $\alpha = A\beta$ for some $\beta \in R^X$. Let $\gamma = Q^{-1}\beta$, so that

$$P\alpha = PA\beta = PAQQ^{-1}\beta = PAQ\gamma = A'\gamma.$$

, so $[P\alpha]_{\operatorname{im} A'} = 0$.

Now, we would like to put the matrix A into this form A'= $\begin{pmatrix} a_1 & & & & & & \\ & a_2 & & & & & \\ & & \ddots & & & & \\ & & & a_s & & & \\ & & & & 0 & & \\ & & & & & \ddots & \\ & & & & & & 0 \end{pmatrix}$ by using $A \mapsto A' = PAQ$, where P \in $M_n(R)$ is invertible and $Q \in M_{|X|}(R)$. We can do this by using row/column operations on A, since row operations correspond to invertible matrices P and Q: Permutation matrices are invertible and swap rows and columns. The matrix $a_{ij}(b)$ which is identity plus b in the (i, j) position is invertible, and adds a multiple of b times a row/column to a row/column. Finally, we can take an identity matrix plus a row containing arbitrary things, which is still invertible. That is, $\sum_{\substack{i=1 \\ i \neq j}}^{|X|} a_{ij}(b_i)$ is invertible and will add a multiple of column j to column i for all i.

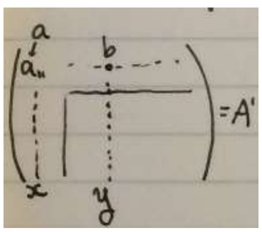
So putting A into this form $\begin{pmatrix} a_1 & & & & & & \\ & a_2 & & & & & \\ & & \ddots & & & & \\ & & & a_s & & & \\ & & & & 0 & & \\ & & & & & \ddots & \\ & & & & & & 0 \end{pmatrix}$ by using maps $A \mapsto A' = PAQ$ comes down to figuring out whether we could put it in that form by using row operations on A. Since we showed that if A' =

PAQ, $M_A = M_{A'}$, we have that M is “associated with” a matrix of this form, $\begin{pmatrix} a_1 & & & & & \\ & a_2 & & & & \\ & & \ddots & & & \\ & & & a_n & & \\ & & & & 0 & \\ & & & & & \ddots \\ & & & & & & 0 \end{pmatrix}$, and so we can find the structure of M.

Step 3

We need to show that given any matrix A, we can put it in this form $\begin{pmatrix} a_1 & & & & & \\ & a_2 & & & & \\ & & \ddots & & & \\ & & & a_n & & \\ & & & & 0 & \\ & & & & & \ddots \\ & & & & & & 0 \end{pmatrix}$.

Of all the matrices reachable from A, let A’ be one (not unique) that has a non-zero entry with a smallest D-H norm (i.e. # of divisors). WLOG, that entry is a_{11} (we can arrange this with permutations).



Claim: the rest of the first row/column is divisible by a11.

Set a = a11.

In a Euclidean domain, it is easier: If there is an entry in the first row/column that is not divisible by a11, b, then b = qa + r, so we can reduce c to r, which has a smaller number of divisors.

In a PID:

I can find a linear combination of a_{11} and c such that sa + tb = gcd (a,b). Let q = gcd (a,b).

We would like to find matrices P, Q, such that PAQ = [q …], and this would be a contradiction.

Then

$\begin{pmatrix} a & b \end{pmatrix} \begin{pmatrix} s & -\frac{b}{q} \\ t & \frac{a}{q} \end{pmatrix} = \begin{pmatrix} q & 0 \end{pmatrix}.$. Let Q’ = $\begin{pmatrix} s & -\frac{b}{q} \\ t & \frac{a}{q} \end{pmatrix}$, and let Q = $\left(\begin{array}{c|c} Q' & 0 \\ \hline 0 & I \end{array}\right)$ and let P be the identity matrix. Q is invertible, since det Q = 1.

Thus the claim is proved.

$$\Rightarrow \text{WLOG } A' = \begin{pmatrix} a_{11} & 0 \\ 0 & * \end{pmatrix}$$

Claim: Anything in $*$ divisible by a_{11}. If $\exists$ some d in $*$ not divisible by a_{11}, we use row operations to bring it to the first row/col and we do the same as above to find an element w/ less divisors.

Now we do row reduction to $*$, using induction to get a matrix where $a_{11} | a_{22} | a_{33} | a_{44} | \dots$

$$A''' = \begin{pmatrix} a_{11} & & & & \\ & a_{22} & & & \\ & & a_{33} & & \\ & & & \ddots & \\ & & & & 0 \end{pmatrix}$$

The process stops when rest of matrix equals 0.

$$\rightsquigarrow M_A \cong A / \begin{pmatrix} a_{11} & & & \\ & a_{22} & & \\ & & \ddots & \\ & & & 0 \end{pmatrix} = M_{(a_{11})} \oplus M_{(a_{22})} \oplus \dots \oplus \underbrace{M_{(0)} \oplus M_{(0)} \cdots}_{k \text{ times}}$$

$$= \frac{R}{\langle a_{11} \rangle} \oplus \frac{R}{\langle a_{22} \rangle} \oplus \dots \oplus R^k \quad (*)$$

Now remember that if $a = \prod p_i^{s_i}$ then $\frac{R}{\langle a \rangle} = \bigoplus \frac{R}{\langle p_i^{s_i} \rangle} \Rightarrow (*)$ becomes what we wanted

Thursday November 20

Jordan Canonical Form

Big picture of the JCF

This is a Corollary to the Fundamental Theorem of Finitely Generated Modules.

Part 1

Start with a matrix T with entries in F, so T is a linear transformation from Fn to Fn. Fn may be endowed with the structure of a F[x] module by identifying the action as xu = Tu. Since this module is finitely generated (by any basis of Fn), Fn is isomorphic, as a F[x] module, to $R^k \oplus \bigoplus R/(p_i^{s_i}),$, where R = F[x].

So now, we have T is a linear transformation from $R^k \oplus \bigoplus R/(p_i^{s_i}),$ to $R^k \oplus \bigoplus R/(p_i^{s_i}),$. Picking a basis element for each of the $R/(p_i^{s_i}),$, we can show that T is of the form $\begin{pmatrix} \boxed{\begin{matrix} \lambda_1 & 1 & \\ & \lambda_1 & 1 \\ & & \lambda_1 \end{matrix}} & & & & \\ & \boxed{\begin{matrix} \lambda_2 & 1 \\ & \lambda_2 \end{matrix}} & & & \\ & & \boxed{\lambda_3} & & \\ & & & \ddots & \\ & & & & \boxed{\begin{matrix} \lambda_n & 1 \\ & \lambda_n \end{matrix}} \end{pmatrix}$. in that basis.

Part 2

We prove that Fn is isomorphic to Rn/im (xI – T).

Part 3

The big goal of this section is that given a matrix T with entries in F, we would like to find the Jordan Canonical Form of T. From Part 1, we know that Fn is isomorphic to $R^k \oplus \bigoplus R/(p_i^{s_i}),$ as a F[x] module, but we need to figure out what this looks like explicitly (and once we do that, it'll be obvious what the JCF looks like from Part 1).

Main steps of this (apparently, this was done in the year 2010):

1. Starting with a matrix T, figure out the corresponding matrix A \in M(F[x]) from the Structure Theorem by computation (In details: from the structure theorem, every finitely generated module is associated to a matrix A – think of A as the kernel. Fn is a finitely generated F[x]-module, with the action of x as xu = Tu, so we would like to find the matrix A \in M(F[x]) associated to this finitely generated F[x]-module).

Example: $T = \begin{pmatrix} 3/2 & 1/2 \\ 1/2 & 3/2 \end{pmatrix}.$ would become $A = \begin{pmatrix} \frac{3}{2} - t & \frac{1}{2} \\ \frac{1}{2} & \frac{3}{2} - t \end{pmatrix} = T - tI$.

2. Row and column reduce this matrix A, so we (sort of) get a diagonal matrix.

Example: Row reducing $A = \begin{pmatrix} \frac{3}{2} - t & \frac{1}{2} \\ \frac{1}{2} & \frac{3}{2} - t \end{pmatrix} = T - tI$ becomes $\to \begin{pmatrix} 1 & 0 \\ 0 & t^2 - 3t + 2 \end{pmatrix}$.

3. Figure out the module this matrix is associated to (from the Structure Theorem). The JCF would be obvious.

Example: $\to \begin{pmatrix} 1 & 0 \\ 0 & t^2 - 3t + 2 \end{pmatrix}$ becomes $V \cong F[t]/\langle (t-1)(t-2) \rangle \cong F[t]/\langle t-1 \rangle \oplus F[t]/\langle t-2 \rangle.$, so $[T] = \begin{pmatrix} 1 & 0 \\ 0 & 2 \end{pmatrix}$.

4. To actually figure out the basis, we would have to write down the isomorphism (from the Structure theorem) explicitly, and trace through the row operations.

Part 4

As an aside, if P and Q are invertible in this diagram, then we can cover the map c.

$$\begin{tikzcd}
R^n \arrow[r, "xI-A", "M"'] & R^n \arrow[r, "\pi_A"'] \arrow[d, "P"] & F^n \arrow[d, "c"] \\
R^n \arrow[u, "Q"] \arrow[r, "xI-B", "N"'] & R^n \arrow[r, "\pi_B"'] & F^n
\end{tikzcd}$$

This shows explicitly that in particular for step 2 in Part 3, row-reducing doesn't affect Fn, using the symbols from Part 2 (that is, without just quoting that it works from the proof of the Structure theorem).

So in step 2, row reduction may not always work, but the goal is to find invertible matrices, P, Q, so we get it in the right form.

The details of the JCF

Part 1

V is a finite dimensional vector space T: V->V linear.
$\Updownarrow$ Algebraically closed field
a finitely generated module over F[x] finitely dimensional
as a vector space.
xu <=> Tu.

$$V = M \cong R^k \oplus \bigoplus \frac{R}{\langle p_i^{s_i}\rangle} \cong \bigoplus \frac{R}{\langle (x-\lambda_i)^{s_i}\rangle}$$

$\frac{R}{\langle (x-\lambda)^s\rangle}$: basis.

$$\underbrace{1}_{e_0},\ \underbrace{(x-\lambda)}_{e_1},\ (x-\lambda)^2, \dots, \underbrace{(x-\lambda)^{s-1}}_{e_{s-1}} \xrightarrow{x-\lambda} 0$$

$T-\lambda: e_i \mapsto e_{i+1},\ e_{s-1} \mapsto 0.$

$T: e_i \mapsto e_{i+1} + \lambda e_i$

$$[T]_{e_0 \dots e_{s-1}} = \begin{pmatrix} \lambda & 0 & & \\ 1 & \lambda & & \\ & 1 & \ddots & \\ & & 1 & \lambda \end{pmatrix}$$

columns of matrix are images of basis vectors

In words:

Any finitely generated module is of this form: $R^k \oplus \bigoplus \frac{R}{\langle p_i^{s_i}\rangle} \cong \bigoplus \frac{R}{\langle (x-\lambda_i)^{s_i}\rangle}$. We can put each of the $\frac{R}{\langle (x-\lambda)^s\rangle}$ into blocks of $\begin{pmatrix} \lambda & 0 & & \\ 1 & \lambda & & \\ & 1 & \ddots & \\ & & 1 & \lambda \end{pmatrix}$ by setting $1, (x-\lambda), (x-\lambda)^2, \dots, (x-\lambda)^{s-1} \to 0$ to be the basis.

This is because we are identifying the action of x as $xu \Leftrightarrow Tu$, $T-\lambda: e_i \mapsto e_{i+1},\ e_{s-1} \mapsto 0$, so $T: e_i \mapsto e_{i+1} + \lambda e_i$.

Part 2

To show that Fn is isomorphic to Rn/im (xI – T), consider $R^n \cong R^{x^n} \xrightarrow[xI-A]{M} R^n \xrightarrow{\pi} F^n$, $M_{n\times n}(F)$, where pi is defined by $e_i \mapsto e_i$ and $x^k \mapsto A^k e_i$.

We will show that $\langle r_i \rangle_{i=1}^n = \ker \pi$, for $r_i = xe_i - Ae_i$, so then by the first isomorphism theorem, Fn \cong Rn/ker pi \cong Rn/im (xI – T).

To show that $r_i = xe_i - Ae_i \in \ker \pi$: Proof: $\pi(r_i) = Ae_i - Ae_i = 0$.

To show the other inclusion:

Consider this sequence $F^n \xrightarrow[\pi]{\beta} \frac{R^n}{\langle r_i \rangle_{i=1}^n} \xrightarrow{\alpha} \frac{R^n}{\ker \pi} \xrightarrow{\cong} F^n \quad (*)$. This is the identity map, since

Let's take some $e_i \in F^n$ and see where it goes.
$e_i \to e_i$ (modulo some relations) $\to e_i$ (modulo some relation) $\to e_i$.

\alpha is well-defined, from the first inclusion.

We must show that \alpha is injective to show the inclusion, and this is true if and only if \beta is surjective.

To show that \beta is surjective:

I need to show that every element of $R^n/\langle r_i \rangle_{i=1}^n$ is in the image of β
i.e. need to show every $x^k e_i$ can be written, mod r_i, as a combination of e_j's.

Indeed $x^k e_i = x^{k-1}(x e_i)$ $\qquad r_i = x e_i - A e_i$
$= x^{k-1}(A e_i)$ $\qquad \Rightarrow r_i + A e_i = x e_i$
$= A \underbrace{x^{k-1} e_i}$ $\qquad \Rightarrow$ mod r_i, $x e_i = A e_i$.
now can inductively repeat process
$= A A^{k-1} e_i$
$= A^k e_i$ (just a column vector)
$\Rightarrow x^k e_i = A^k e_i \in \operatorname{im} \beta$.

Part 4

$$\begin{tikzcd}
R^n \arrow[r, "xI - A", "M"'] & R^n \arrow[r, "\pi_A"'] \arrow[d, "P"] & F^n \arrow[d, "c"] \\
R^n \arrow[u, "Q"] \arrow[r, "xI - B", "N"'] & R^n \arrow[r, "\pi_B"'] & F^n
\end{tikzcd}$$

Having this diagram, with P,Q invertible, we would like to recover c:

where $c : F^n \to F^n$ is defined as $ce_i = \pi_B(Pe_i)$. However, applying π_B is highly non-trivial. Note that $\pi_B(x^k u) = B^k u$ and write $P = \sum_k x^k P_k$ where $P_k \in M_n(F)$. Then

$$\begin{aligned} ce_i &= \pi_B(Pe_i) \\ &= \pi\left(\sum_k x^k P_k e_i\right) \\ &= \sum_k B^k P_k e_i \end{aligned}$$

and so $C = \sum_k B^k P_k$.

GCD Trick

The "GCD" Trick

If $q = \gcd(a, b) = s\,a + t\,b$, the equality $\begin{pmatrix} s & t \\ -b/q & a/q \end{pmatrix} \begin{pmatrix} a \\ b \end{pmatrix} = \begin{pmatrix} q \\ 0 \end{pmatrix}$ allows us to replace pairs of entries in the same column by their greatest common divisor (and a zero!), using invertible row operations. A similar trick works for rows.

Factoring Diagonal Entries

Factoring Diagonal Entries

If $1 = \gcd(a, b) = s\,a + t\,b$, the equality $\begin{pmatrix} s\,a & 1 \\ -t\,b & 1 \end{pmatrix} \begin{pmatrix} 1 & 0 \\ 0 & a\,b \end{pmatrix} \begin{pmatrix} a & -b \\ t & s \end{pmatrix} = \begin{pmatrix} a & 0 \\ 0 & b \end{pmatrix}$ is an invertible row-column-operations proof of the isomorphism $\frac{R}{\langle a \rangle} \oplus \frac{R}{\langle b \rangle} \simeq \frac{R}{\langle ab \rangle}$.

The Jordan Trick

We would like to show:

$$\begin{pmatrix} 1 & & & \\ & 1 & & \\ & & \ddots & \\ & & & p^s \end{pmatrix} \sim \begin{pmatrix} p & & & & \\ 1 & p & & & \\ & 1 & p & & \\ & & 1 & p & \\ & & & 1 & p \end{pmatrix}$$

We know that

$$\frac{R}{\langle p^s\rangle} = \frac{\langle y\rangle}{p^s y = 0} \qquad y_0 = y \quad y_1 = -py, \; y_2 = p^2 y \quad y_3 = -p^3 y, \ldots \; y_{s-1} = \pm p^{s-1} y$$

$$\cong \frac{\langle y_0 \ldots y_{s-1}\rangle}{\left.\begin{matrix} p y_i + y_{i+1} = 0 \\ p y_{s-1} = 0 \end{matrix}\right\}} \text{ modulo both of these relations}$$

$\begin{pmatrix} 1 & & & & 0 \\ & 1 & & & \\ & & 1 & & \\ & & & \ddots & \\ 0 & & & & p^s \end{pmatrix}$ corresponds to $\dfrac{R}{\langle p^s\rangle}$ and

$\begin{pmatrix} p & 0 & & & \vdots \\ 1 & p & & \vdots & \vdots \\ 0 & 1 & & \vdots & \\ \vdots & 0 & \cdots & p & 0 \\ \vdots & \vdots & & 1 & p \end{pmatrix}$ corresponds to $\dfrac{\langle y_0 \ldots y_{s-1}\rangle}{p y_i + y_{i+1} = 0\}}$, (think structure theorem, kernel).

Explicitly,

$$\begin{pmatrix} p^{k-1} & -1 \\ 1 & 0 \end{pmatrix}\begin{pmatrix} 1 & 0 \\ 0 & p^k \end{pmatrix}\begin{pmatrix} 1 & p \\ 0 & 1 \end{pmatrix} = \begin{pmatrix} p^{k-1} & 0 \\ 0 & p \end{pmatrix}$$

Then repeat for the bigger version…

Monday November 24

Tensor Products

We wish to put a group structure on modules. Let's try using direct sums…

"First we say something completely wrong:
(R-mod, $\oplus$) is an "abelian group."

1. $M_1 \oplus M_2 = M_2 \oplus M_1$
2. $(M_1 \oplus M_2) \oplus M_3 = M_1 \oplus (M_2 \oplus M_3)$
0. 0 (module w/ single element zero)
   $0 \oplus M = M$.

It doesn't work, since there are no inverses.

1. No inverses!
2. The above equalities are really isomorphisms.

Nevertheless,

We will show ($\underbrace{R\text{-mod}}_{\text{coll'n}}$, $\oplus$, $\otimes$) is a "ring" in a similar sense since all rules in a ring apply up to iso except. inverses.

Definition of tensor product:

Tensor Product $M \otimes N$ of two Modules: (Def'n of a tensor product, not the tensor product)
$M \otimes N$ is a module along with a bilinear map $\tau : M \times N \to M \otimes N$ such that

$$\begin{tikzcd} M \times N \arrow[r, "\tau", "\text{bilinear}"'] \arrow[dr, "\rho"', "\text{bilinear}"] & M \otimes N \arrow[d, dashed, "\exists!\ \text{linear map}", "\alpha"'] \\ & P \end{tikzcd}$$

Given any module P and bilinear $\rho : M \times N \to P$,
$\exists!$ $\alpha : M \otimes N \to P$ s.t. $\rho = \alpha \circ \tau$.

A better way of thinking of tensor products:

Theorem: $M \otimes N$ exists ie there is such a module and it is unique up to an isomorphism.

Proof: Let $M \otimes N = \langle m \otimes n : m \in M, n \in N \rangle / \text{relations}$.

$$M \otimes N = \left\{ \sum_{i=1}^{k} a_i m_i \otimes n_i : a_i \in R, m_i \in M, n_i \in N \right\} / \text{rel.}$$

$$M \times N \xrightarrow[(m,n) \mapsto m \otimes n]{\tau} M \otimes N$$

Now we need to know what the relations are

The relations are the obvious ones:

$$\begin{aligned}
&v, v_1, v_2 \in V; w, w_1, w_2 \in W; c \in K;\\
&(v_1, w) + (v_2, w) \sim (v_1 + v_2, w)\\
&(v, w_1) + (v, w_2) \sim (v, w_1 + w_2)\\
&c(v, w) \sim (cv, w) \sim (v, cw)
\end{aligned}$$

(from Wikipedia)

To make the mapping bilinear we mod out the relations that define a bilinear relation.

So $M \otimes N$ is an R-module an τ is obviously bilinear.

Suppose $\rho : M \times N \to P$ bilinear is given. We need to find a linear α s.t. $\rho = \alpha \circ \tau$.

$$\alpha\left(\sum a_i m_i \otimes n_i \right) = \sum a_i \rho(m_i, n_i).$$

Claim: α is well defined. To check well defined we need to see if all of our relations are mapped to 0.

$$\begin{aligned}
&\alpha((m_1 + m_2) \otimes n - m_1 \otimes n - m_2 \otimes n)\\
&= \rho((m_1 + m_2), n) - \rho(m_1, n) - \rho(m_2, n)\\
&= 0, \text{ since } \rho \text{ is bilinear.}
\end{aligned}$$

The same holds for all of the other relations.

That was existence.

To show uniqueness:

Main idea: Use the universal property on both of them, and then use the uniqueness of the universal property.

Theorem: $M \otimes N$ is unique up to isomorphism.
Proof: Suppose $(M \otimes N, z)$ and $(M \bar{\otimes} N, \bar{z})$ both satisfy the universal property. Then using the universal property for $M \otimes N$

$$\begin{tikzcd} M \times N \arrow[r, "z"] \arrow[dr, "\bar{z}"'] & M \otimes N \\ & M \bar{\otimes} N \arrow[u, dashed, "\exists \alpha"'] \end{tikzcd} \qquad \exists \alpha : M \bar{\otimes} N \to M \bar{\otimes} N$$

Then using the universal property for $M \bar{\otimes} N$

$$\begin{tikzcd} M \times N \arrow[r, "\bar{z}"] \arrow[dr, "z"'] & M \bar{\otimes} N \arrow[d, dashed, "\exists \bar{\alpha}."] \\ & M \otimes N \end{tikzcd} \qquad \exists \bar{\alpha}\ M \bar{\otimes} N \to M \otimes N.$$

Now use the universal property for $M \otimes N$ as follows:

$$\begin{tikzcd} M \otimes N \arrow[r, "z"] \arrow[dr, "z"'] & M \otimes N \arrow[d, dashed, "\mathrm{Id.}\ \&\ \bar{\alpha} \circ \alpha."] \\ & M \otimes N \end{tikzcd}$$

both id & $\bar{\alpha} \circ \alpha$ are maps that satisfy our diagram.
But we have uniqueness in the universal property so $I = \bar{\alpha} \circ \alpha$.
We do the same to find $\alpha \circ \bar{\alpha} = I$.

$$\begin{tikzcd} M \times N \arrow[r, "z"] \arrow[dr, "\bar{z}"] \arrow[ddr, "z"'] & M \otimes N \arrow[d, dashed, "\bar{\alpha}"'] \arrow[dd, dashed, bend left, "I = \bar{\alpha} \circ \alpha"] \\ & M \bar{\otimes} N \arrow[d] \\ & M \otimes N \end{tikzcd}$$

Dimension of tensor products:

Example: Suppose V, W are vectors spaces over a field F with bases $(u_i)_{i=1}^{n}$ of V and $(w_j)_{j=1}^{m}$ of W.
Claim: $V \otimes W$ is a vector space of dim $n \cdot m$. with bases $(u_i \otimes w_j)_{i,j=1}^{n,m}$ ~~where i~~

Proof: Pick the obvious basis $(u_i \otimes w_j)$.

Show the basis spans:

Proof: Given $u \in V$, $w \in W$, we need to show $u \otimes w$ is a linear combination of $(u_i \otimes w_j)_{i,j=1}^{n,m}$

$u \otimes w = (\sum \alpha_i u_i) \otimes (\sum \beta_j w_j)$

$= \sum \alpha_i \beta_j u_i \otimes w_j$ due to the relations.

Show linear independence:

Now we need to do linear independence. Let $\{\phi_i\}, \{\psi_j\}$ be the dual bases of $\{v_i\}$ and $\{w_j\}$ in V^* and W^*, respectively.

Claim 3.13. If $\phi \in V^*$ and $\psi \in W^*$ then $\phi \otimes \psi : V \bigotimes_F W \to F$ given by $\phi \otimes \psi(\sum a_\alpha v_\alpha \otimes w_\alpha) = \sum a_\alpha \phi(v_\alpha)\psi(w_\alpha)$ is well-defined.

The above claim is easy to verify, and just involves checking that the relations quotiented out by in constructing $V \bigotimes_F W$ are preserved. It is clear that $\phi \otimes \psi$ is linear.

Now assume that $\sum a_{i,j} v_i \otimes w_j = 0$. Apply $\phi_{i'} \otimes \psi_{j'}$ to both sides. We get $\sum a_{i,j}\delta_{i,i'}\delta_{j,j'} = 0$, so $a_{i',j'} = 0$ and we got linear independence. □

Thursday November 27

Examples of tensor products:

Almost $\mathcal{F}(X) \otimes \mathcal{F}(Y) \cong \mathcal{F}(X \times Y)$ where $\mathcal{F}(X) = \{\phi : X \to F\}$ (module: Vector Space

This is true if X and Y are finite ($\mathcal{F}(X)$ δ-fns on points of X, $\mathcal{F}(Y)$ δ-fns on points of Y, so is so to δ-fns on points of $X \times Y$ where δ-fn is indicator fns on points of X & Y)

$\exists$ a map $\mu : \mathcal{F}(X) \otimes \mathcal{F}(Y) \to \mathcal{F}(X \times Y)$

$\mu(\sum \alpha_i \varphi_i \otimes \psi_i)(x,y) = \sum \alpha_i \varphi_i(x) \cdot \psi_i(y)$

$\varphi_i \in \mathcal{F}(X)$, $\psi_i \in \mathcal{F}(Y)$

Alternatively, there is a bilinear $\mu_0 : \mathcal{F}(X) \times \mathcal{F}(Y) \to \mathcal{F}(X \times Y)$

$(\varphi, \psi) \overset{\mu_0}{\mapsto} \varphi(x) \cdot \psi(y)$

So by the universal property $\exists!\ \mu : \mathcal{F}(X) \otimes \mathcal{F}(Y) \to \mathcal{F}(X \times Y)$ s.t the diagram commutes.

$\mathcal{F}(X) \otimes \mathcal{F}(Y) \cong \mathcal{F}(X \times Y)$ are isomorphic if X and Y are finite. We could either define the map directly, or use the universal property on the obvious bilinear map.

There are some properties always true about μ:

① μ is always 1-1 (challenging)

② Isomorphism if X or Y is finite. (easy)

③ If X and Y are infinite, not surjective (challenging)

Example: If $q \equiv \gcd(a,b)$ in a U.F.D, and $q = sa + tb$, then

$$\frac{R}{\langle a \rangle} \otimes \frac{R}{\langle b \rangle} \cong \frac{R}{\langle q \rangle}$$

$$\underbrace{\frac{\mathbb{Z}}{\langle 3 \rangle} \otimes \frac{\mathbb{Z}}{\langle 7 \rangle} = \{0\} \quad \frac{\mathbb{Z}}{\langle 3 \rangle} \oplus \frac{\mathbb{Z}}{\langle 7 \rangle} = \frac{\mathbb{Z}}{\langle 21 \rangle}}_{\text{very different behaviour!}}$$

Warning! Do not confuse direct sums with tensor products.

lower case tensor.

Proof: $[r_1]_a \otimes [r_2]_b \longmapsto [r_1 r_2]_q$.

Obviously well defined since if we change r_1 by a multiple of a then the result changes by a multiple of a, but $q \mid a$ so the result changes by a multiple of q. The same is true for r_2 with b.

For the first direction, define the obvious map $[r_1]_a \otimes [r_2]_b \longmapsto [r_1 r_2]_q$ and check it is well-defined.

$c(m \otimes n) = cm \otimes n$ — $r[1]_a \otimes [1]_b \longleftarrow [r]_q = r[1]_q$

$[r]_a \otimes [1]_b = [1]_a \otimes [r]_b$.

(~~If we change r~~)

We need to check well defined:

$$[q] \mapsto [q]_a \otimes [1]_b = q[1]_a \otimes [1]_b$$

$$= (sa + tb)[1]_a \otimes [1]_b$$

$$= \cancel{[sa]_a \otimes [}$$

$$= [sa]_a \otimes [1]_b + [1]_a \otimes [tb]_b$$

$$= 0.$$

$sa([1]_a \otimes [1]_b) + tb([1]_a \otimes [1]_b)$

For the other direction, define the obvious map.

To check well-defined, let q = sa + tb and simplify.

Thus, they are isomorphic:

Thus our map is well defined.

$$\frac{R}{\langle q\rangle} \mapsto \frac{R}{\langle a\rangle}\otimes\frac{R}{\langle b\rangle} \mapsto \frac{R}{\langle q\rangle}.$$

$$[r]_q \mapsto r[1]_a\otimes[1]_b \mapsto r[1]_q = [r]_q.$$

$$\frac{R}{\langle a\rangle}\otimes\frac{R}{\langle b\rangle} \mapsto \frac{R}{\langle q\rangle} \mapsto \frac{R}{\langle a\rangle}\otimes\frac{R}{\langle b\rangle}$$

$$[r_1]_a\otimes[r_2]_b \mapsto [r_1 r_2]_q \mapsto r_1 r_2[1]_q$$

$$\to r_1 r_2[1]_a\otimes[1]_b = [r_1]_a\otimes[r_2]_b.$$

Properties of tensor products

Theorem: $(R\text{-mod}, \oplus, \otimes, \{0\}, R)$ is a "ring".

$$\left.\begin{array}{l} (1)\ M\oplus(N\oplus P)\cong(M\oplus N)\oplus P. \\ (2)\ M\oplus N\cong N\oplus M. \\ (3)\ M\oplus 0\cong M. \\ (4)\ M\otimes R\cong M. \\ (5)\ (M\otimes N)\otimes P\cong M\otimes(N\otimes P) \\ (6)\ M\otimes N\cong N\otimes M. \\ (7)\ M\otimes(N\oplus P)\cong M\otimes N\oplus M\otimes P. \end{array}\right\}$$

all trivial but (4) takes some thinking.

$$\left.\begin{array}{l} m\otimes r\mapsto r\cdot m \\ m\mapsto m\otimes 1. \end{array}\right\}$$ all properties work.

Monday December 1

A functor is a map F:C -> D where C,D are categories, such that if $\phi : A \to B$, there is a morphism $F\phi : FA \to FB$ such that $F(\phi\circ\psi) = F\phi\circ F\psi$. Moreover, the identity morphisms are mapped to identity morphisms.

A bifunctor is a map $F : \mathcal{C}\times\mathcal{D}\to\mathcal{E}$, where C,D,E are categories, such that F is a functor in each variable separately.

Example 3.25. $\bigotimes$ is a bifunctor. That is, fix a module N, then the map $M \mapsto M\bigotimes N$ is a functor, and similarly if we fix a module M then the map $N\mapsto M\bigotimes N$ is also a functor. In more detail, suppose that $M_1 \to^f M_2$. Then there is a map $f\otimes N : M_1\bigotimes N \to M_2\bigotimes N$, which is given by the linear extension of $m_1\otimes n\mapsto f(m_1)\otimes n$. One needs to check that this is well-defined, but this is not difficult, since f is a module morphism. One also needs to check that if $M_1\mapsto^g M_2\mapsto^f M_3$, then $(f\circ g)\otimes N = f\otimes N\circ g\otimes N$. This is also obvious. Note that if we have morphisms $f : M_1\to M_2$ and $g : N_1\to N_2$ then there is a map $f\otimes g : M_1\bigotimes N_1\to M_2\bigotimes N_2$, given by the linear extension of $m_1\otimes n_1\mapsto f(m_1)\otimes g(n_1)$.

Example of tensor products.

Examples:

1) Over $R=\mathbb{Z}$ — also a $\mathbb{Z}$-mod since abelian — $\mathbb{Q}$ is a module over $\mathbb{Z}$ (since abelian)

$$\mathbb{Q}\otimes_{\mathbb{Z}}\mathbb{Z}^n = \mathbb{Q}\otimes(\mathbb{Z}\oplus\dots\oplus\mathbb{Z})$$
$$= \mathbb{Q}\otimes\mathbb{Z}\oplus\mathbb{Q}\otimes\mathbb{Z}\oplus\dots\oplus\mathbb{Q}\otimes\mathbb{Z}$$

Since $\mathbb{Z}$ multiplicative identity. $= \mathbb{Q}\oplus\dots\oplus\mathbb{Q}=\mathbb{Q}^n$

In general, given a ring morphism $\phi: R\to S$ $(\mathbb{Z}\to\mathbb{Q})$ it turns S into an R-module.

Now given an R-module M, set
$$M_S := S\otimes_R M$$
is an S-module by $s'\cdot(s\otimes m) := (s's)\otimes m$ (check well defined and turns $S\otimes_R M$ into an S-module)

and $R_S^n = S^n$

Field of Fractions defined by universal property:

Proposition: Given any domain R, there exists a unique (up to isomorphism) field $Q(R)$ "the field of fractions of R" s.t.

$$\begin{tikzcd} R \arrow[r, "\iota"', "1\text{-}1"] \arrow[dr, "\forall \text{ map } \alpha"'] & Q(R) \arrow[d, dashed, "\exists!"] \\ & F \end{tikzcd}$$

$(1\text{-}1)$? need to verify but need this

F a field

Proof (Start): $Q(R) = \underbrace{\text{"}a\text{"}}_{}$ where $a,b\in R$, $b\neq 0$.
 b

think of as a funny ordered pair

(Didn't actually prove this theorem)

Localization

Def'n: want $\frac{r_1}{s_1}=\frac{r_2}{s_2}$ ... $\frac{r_1}{s_1}\sim\frac{r_2}{s_2}$

$$S^{-1}R = \left(\left\{\frac{r}{s} : \begin{matrix} r\in R \\ s\in S\end{matrix}\right\} \Big/ s_2r_1 = s_1r_2,\ 0=\frac{0}{1},\ 1=\frac{1}{1},\ \frac{a}{b}+\frac{c}{d}=\frac{ad+bc}{bd},\ \frac{a}{b}\cdot\frac{c}{d}=\frac{ac}{bd}\right)$$

"the localization of R at S".

Uniqueness for the Structure Theorem

$$M \cong R^k \oplus \bigoplus \frac{R}{\langle p_i^{s_i} \rangle}$$

A module M is a **torsion** module if for all m \in M, there exists nonzero r \in R such that rm = 0.

Claim: $R/\langle a \rangle$ is torsion:
Proof: if $m \in R/\langle a \rangle$ then $am = 0$.

Claim: If M is torsion, then $M_{Q(R)} = 0$.
Proof: $m \in M$ and since M torsion $\exists\, r \neq 0$ s.t. $rm = 0$.
In $M_{Q(R)} = Q(R) \otimes M$

$$m = 1 \otimes m = r \cdot \left(\left(\frac{1}{r} \right) \otimes m \right) = \frac{1}{r} \otimes rm = 0$$

To show that k is unique:

$\therefore M_{Q(R)} = Q(R) \otimes (R^k \oplus \bigoplus R/\langle p_i^{s_i} \rangle)$
$= Q(R)^k \otimes 0 = Q(R)^k.$
$\dim_{Q(R)} Q(R) \otimes M = k$ so k is invariant under M
$\Rightarrow k$ is unique.

To show that the torsion part is unique, consider $\dim_{R/\langle p \rangle} M_{R/\langle p \rangle}$.

extension of coefficients even though reduced

$$\dim_{R/\langle p \rangle} M_{R/\langle p \rangle} = \dim_{R/\langle p \rangle} \left(\frac{R}{\langle p \rangle} \right)^k \oplus \bigoplus \left(\frac{R}{\langle p \rangle} \otimes \frac{R}{\langle p_i^{s_i} \rangle} \right)$$

$$\Rightarrow \dim_{R/\langle p\rangle} \left(\frac{R}{\langle p\rangle}\right)^k \oplus \bigoplus \left(\frac{R}{\langle p\rangle} \otimes \frac{R}{\langle p_i^{s_i}\rangle}\right) = k + |\{i : p_i = p\}|$$

So the number of times p appears in the list of (p_i) is fixed (determined). This is not quite uniqueness. We also need to show that the multiplicities are fixed. (Reminder: p_i's can repeat)

Proofs: ① $\operatorname{Im}\hat{p}^s = p^s \cdot R \xleftarrow[p^s a \,\leftarrow\, a]{p^s\cdot a \,\leftarrow\, a} R$

② $(p^s, q^t) = 1 \Rightarrow (1 = \sigma p^s + \tau q^t)$ $\forall\, \sigma, \tau \in R$ s.t. $\sigma p^s + \tau q^t = 1$

In $R/\langle q^t\rangle$, $1 = 1 - \tau q^t = \sigma p^s = \hat{p}^s = \sigma$

$\Rightarrow 1 \in \operatorname{im}\hat{p}^s$ so everything else in the image.

③ In $R/\langle p^t\rangle$, $p^s = 0$ so $\hat{p}^s \cong 0$ so $\operatorname{im}\hat{p}^s = 0$.

④ 1 ~~dunno~~. $\operatorname{Im}\hat{p}^s = p^s R / p^t R \cong R/\langle p^{t-s}\rangle$

$p^s a \longleftarrow\!\!| \; a$

$p^s a \xmapsto{\text{divide}} a$.

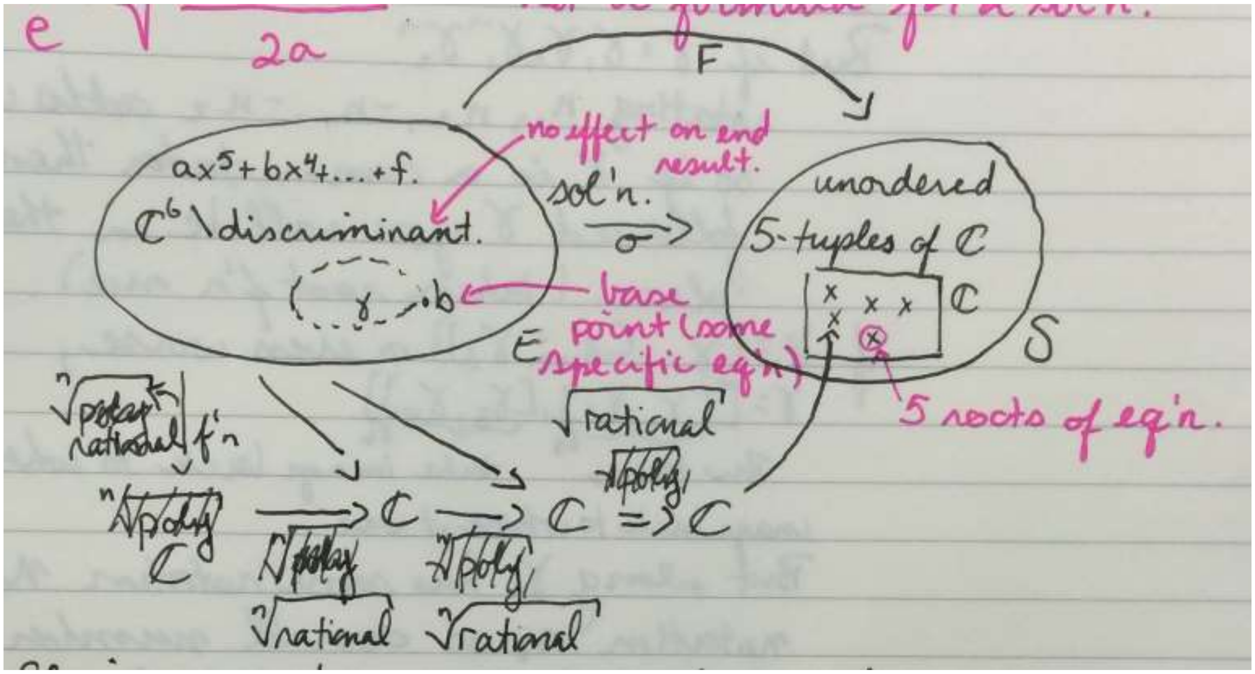
$$\dim_{R/\langle p\rangle} (\operatorname{im}\hat{p}^s)_{R/\langle p\rangle} = K + \#\left\{i : p_i = p \;\&\; s_i > s\right\}$$

This proves uniqueness.

Wednesday December 3

Topological Proof of why you can't solve the quantic

Main diagram:



Proof by Contradiction. Suppose there is such an equation for roots.

Claim 1:

Let E be the set of degree 5 polynomials, subtract the ones with double roots.

This is a homomorphism: 1. $\pi_1(E) \xrightarrow{\sigma} \cancel{\pi_1(S)} \twoheadrightarrow S_5$.

Basically, this is because you can move around on the left side, so that it corresponds to a permutation of the roots. More precisely,

Suppose you had a path of equations; the base point of the path corresponds to the solution given here. As I move within the space of equations, I can keep my 5 fingers on the solutions and they will continue to move as well and they never coincide because I moved the discriminant and I never have confusion over which finger goes where. So my fingers go a certain way, or, at the base point I have a specific collection of solutions and I will number them 1-5 and then when I move in the space of equations the corresponding solutions move and maybe one will come back to where it was (because the equation comes back to where it was) and I will get some permeantation. If you have ever seen covering space, this is really what I am telling you.

Claim 2:

1. $\pi_1(E) \xrightarrow{\sigma} \cancel{\pi_1(S)} \twoheadrightarrow S_5$ is surjective.

Suppose you have some permutation. In fact, for every arrangement of solutions, I can always call them x-1 up to x-5. If I move in this space in some way, then this polynomial changes in a certain way and at the end it comes back to where it was because if the end of the solution comes back to where they were, then the equation doesn't change.

Claim 3:

3. $\forall \gamma \in \pi_1(E)$, $F \circ \gamma$ always points at a root. ∎

If gamma is a member of pi E, then F composed with gamma (F being this entire system) makes sense and it always points at a root.

Claim 4:

In particular, if gamma is the curve here which induces the cyclic permutation 123, or sigma, then F composed with gamma points at solution number 1 both at t=0 and t=1, and this will be a contradiction.

Proof:

If you have a closed path in the complex plane and you evaluate the nth root and you continuously change a branch of the nth root, then the nth root at the end of the path is not necessarily equal to the nth root at the beginning of the path. Suppose you have a path that circles around the origin; when you go a full circle, the square root is always a path of the angle. If you have a path whose rotation number around the origin is 0, and you compute the square root and you make a continuous choice of the nth root along this path then at the end it comes back to where it was. When you compute this rational function of the coefficients, the image of this rational function does some funny path in the plane, which may or may not come back to where it was. However, if gamma is equal to gamma 1, gamma 2, gamma 1 inverse, gamma 2 inverse, then the rotation number of this rational function would have to be zero because you rotate a certain amount going each gamma (forward for gamma and backwards for gamma inverse)...you would eventually go back to where you started. If gamma is a commutator, then after you followed gamma, over here you're in the same place after you've taken the root function once. What if gamma is a commutator of two commutators? If you go along gamma 5 and gamma 6, the input for this whole function is a closed root. Along gamma 5 and 6 they have some rotation number and so the nth root, along gamma, comes back to where it was.

The only remaining thing to show is: claim (123) is a commutator of any order.

$(abc)(cde)(abc)^{-1}(cde)^{-1} = (adc)$

Let $a=1$, $d=2$ $c=3$.

QED.