September 13, hours 1-2: Non Commutative Gaussian Elimination

September-11-11
6:11 PM

MAT 1100 Core Algebra.

DROR BAR-NATAN

I don't know core algebra!

[website: search]

To do. 1. print "About".
2. print NCGE. (two sides)
3. Video tape?

on book

Goal: Within your lifetime, understand $G = \langle g_1 \dots g_m \rangle \subset S_n$:
1. $|G| = ?$ 2. $\sigma \in G$? 3. $\sigma = W(g_1, \dots g_m)$ 4. random

Two pre-requisites 1. Groups, S_n, silly uniquenesses, cancellation, $(ab)^{-1} = b^{-1}a^{-1}$, subgroups, the subgroup generated by $\{\sigma_\alpha\}$.

2. Row reduction for real.

$$\boxed{f \cdot g = f \circ g}$$

Algorithm as in handout.

Claim 1 Every σ_{ij} in T is in G.

Claim 2 Anything fed to T is now a monotone product $\sigma_{1j_1}\sigma_{2j_2}\sigma_{3j_3}\dots$ $\quad j_i \geq i$

Claim 3 If two monotone products are equal,

$$\sigma_{1j_1} \dots \sigma_{nj_n} = \sigma_{1j_1'} \dots \sigma_{nj_n'}$$

then all the indices are equal, $\forall i\ j_i = j_i'$.

Claim 4 Let $M_k = \left\{\begin{matrix}\text{monotone products}\\ \text{beginning with } k\end{matrix}\right\} = \{\sigma_{kj_k} \dots \sigma_{nj_n}\}$, then for every k, $M_k \cdot M_k \subset M_k$ (and so each M_k is a subgroup of S_n.

Proof Clearly $M_nM_n \subset M_n$. Now assume that $M_5M_5 \subset M_5$ and show that $M_4M_4 \subset M_4$. Start with $\sigma_{8,j}M_4 \subset M_4$:

and show that $M_4 M_4 \subset M_4$. Start with $\sigma_{8,j} M_4 \subset M_4$:

$$\sigma_{8,j}(\sigma_{4,j_4} M_5) \overset{1}{=} (\sigma_{8,j}\sigma_{4,j_4}) M_5 \overset{2}{\subset} M_4 M_5$$

$$\overset{3}{=} \sigma_{4,j_4}(M_5 M_5) \overset{4}{\subset} \sigma_{4,j_4} M_5 \subset M_4$$

Claim 5 $M_1 = G$ and we have achieved all of our goals [except there is a hidden problem].

$\rightarrow$ then do goals 1, 2, 3, 4 and the 0: "in our lifetime".

don't line

Example $\sigma_1 = (123) = 2314$ $\quad \sigma_2 = (12)(34) = 2143$, in S_4

11 I			
12 $\sigma_1 = 2314$ [1]	22 I		
13 $\sigma_{12}^2 = 3124$ [2]	23 $\sigma_{12}^{-1}\sigma_2 = 1342$ [3]	33 I	
14 $\sigma_{23}\sigma_{13} = 4132$ [5]	24 $\sigma_{13}^{-1}\sigma_{23}\sigma_{12} = 1423$ [4]	34	44 I

Feed $\sigma_1 = 2314$ ... Fed @ σ_{12}

Feed $\sigma_{12}^2 = 3124$ ... Fed @ σ_{13}

Feed $\sigma_2 = 2143$ ... Feed $\sigma_{12}^{-1}\sigma_2 = 1342$ .. Fed @ σ_{23}

Feed $\sigma_{12}\sigma_{23} = 2143$ ... Feed $\sigma_{12}^{-1}\sigma_{12}\sigma_{23} = \sigma_{23}$ ....

No point feeding $\sigma_{ij}\sigma_{kl}$ if $i<k$?

Feed $\sigma_{23}\sigma_{12} = 3412$ ... Feed $\sigma_{13}^{-1}\sigma_{23}\sigma_{12} = 1423$ ... to σ_{24}

Feed $\sigma_{23}\sigma_{13} = 4132$ .. to σ_{14}

Feed $\sigma_{24}\sigma_{12} = 4213$ ... feed $\sigma_{14}^{-1}\sigma_{24}\sigma_{12} = 1423$ ... drop.

$\Rightarrow |G| = 4 \cdot 3 \cdot 1 \cdot 1 = 12$. Is $4123 \in G$?

write 2431 in terms of $\sigma_{1,2}$.

---

* Go over the "about" handout

* Go over the "about" handout.

September 15, hour 3: Non Commutative Gaussian Elimination, Homomorphisms, Kernels and Images

September-15-10
6:53 PM

1. Finish tracing the NCGE handout; along do the S_4 example.
2. Go over the "about" handout.
3. Group homomorphisms, the "category" of groups, images and kernels. Example: S_3 is an image of S_4, but not a kernel.
4. Normal subgroups, kernels are normal.
5. Question: Is there a normal subgroup of S_4 which is isomorphic to S_3?

not done

Announce Selick!

<u>Example</u> $\sigma_1 = (123) = 2314$ $\sigma_2 = (12)(34) = 2143$, in S_4

On board (minus fills)

11 I			
12 $\sigma_1 = 2314$ 1	22 I		
13 $\sigma_{12}^2 = 3124$ 2	23 $\sigma_{12}^{-1}\sigma_2 = 1342$ 3	33 I	
14 $\sigma_{23}\sigma_{13} = 4132$ 5	24 $\sigma_{13}^{-1}\sigma_{23}\sigma_{12} = 1423$ 4	34	44 I

Feed $\sigma_1 = 2314$ ... Fed @ σ_{12}

Feed $\sigma_{12}^2 = 3124$ ... Fed @ σ_{13}

Feed $\sigma_2 = 2143$ ... Feed $\sigma_{12}^{-1}\sigma_2 = 1342$ .. Fed @ σ_{23}

Feed $\sigma_{12}\sigma_{23} = 2143$ ... Feed $\sigma_{12}^{-1}\sigma_{12}\sigma_{23} = \sigma_{23}$ ....

No point feeding $\sigma_{ij}\sigma_{kl}$ if $i<k$!

Feed $\sigma_{23}\sigma_{12} = 3412$ ... Feed $\sigma_{13}^{-1}\sigma_{23}\sigma_{12} = 1423$ ... to σ_{24}

Feed $\sigma_{23}\sigma_{13} = 4132$ .. to σ_{14}

Feed $\sigma_{24}\sigma_{12} = 4213$ ... feed $\sigma_{14}^{-1}\sigma_{24}\sigma_{12} = 1423$ ... drop.

$\Rightarrow |G| = 4\cdot 3\cdot 1\cdot 1 = 12$. Is $4123 \in G$?

write 2431 in terms of $\sigma_{1,2}$.

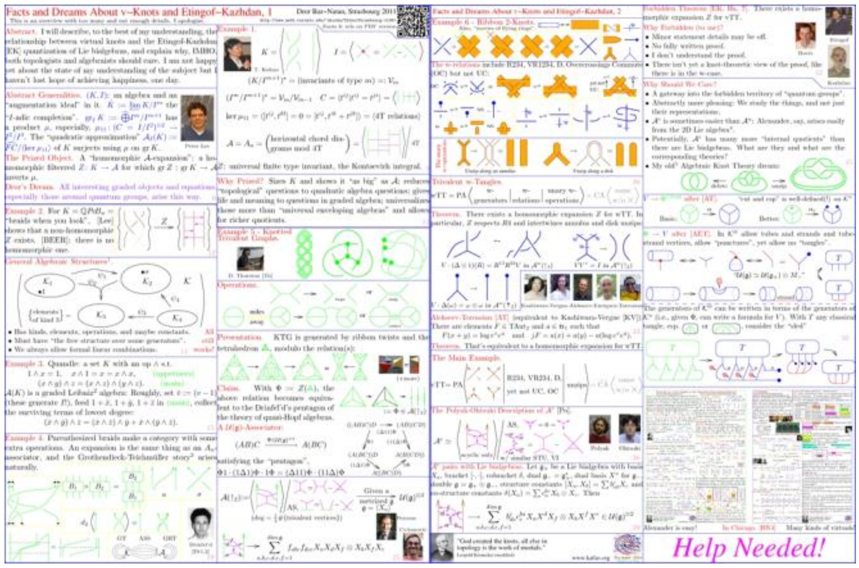
September 20 and 22, hours 4-6, Lectures by Selick

September-23-11
12:17 PM

I was in Strasbourg: http://www.math.toronto.edu/drorbn/Talks/Strasbourg-1109/

Material covered by Selick: the isomorphism theorems, the symmetric group and the alternating group, to the proof of simplicity but with the end of that proof rushed.

The Selick Week



Dror's week: http://www.math.toronto.edu/~drorbn/Talks/Strasbourg-1109/

Warnings. For Dror,

1. $x^g = g^{-1}xg$ so that $(x^g)^h = x^{(gh)}$

2. If $\sigma, \tau \in S_n$, then $\sigma\tau = \sigma \circ \tau$

Definitions. Homomorphism, isomorphism, subgroup, cosets, normal subgroup, $C_G(X)$, $Z(G)$, $N_G(X)$.

Proposition. Every normal subgroup is the kernel of a homomorphism & vice versa. (Pf: Define G/N!)

The 1st Isomorphism Thm. If $\phi: G \to H$ is a morphism, then $G/\ker\phi \cong \mathrm{im}(\phi)$

Claim. For $H, K < G$, $HK < G$ iff $HK = KH$.

Claim. If $H \subset N_G(K)$ then $HK = KH$, $K \triangleleft HK$, & $H \cap K \triangleleft H$.

The 3rd Isomorphism Thm. If $K, H \triangleleft G$ & $K < H$, then $\dfrac{G/K}{H/K} \cong G/H$

The 2nd isomorphism theorem. If $H < N_G(K)$, then $HK/K \cong H/H\cap K$

$$\begin{array}{ccc} & HK & \\ H & & \Vert\!\wr \\ \wr\Vert & & K \\ & H\cap K & \end{array}$$

The 4th Isomorphism Thm. If $N \triangleleft G$ then $\pi: G \to G/N$ induces a "faithful" bijection between subgroups of G/N and $\{H : N < H < G\}$:

* $A < B \Leftrightarrow \pi(A) < \pi(B)$ (& then, $[B:A] = [\pi(B):\pi(A)]$)
* $A \triangleleft B \Leftrightarrow \pi(A) \triangleleft \pi(B)$
* $\pi(A \cap B) = \pi(A) \cap \pi(B)$.

Permutation Groups. S_n, $|S_n| = n!$, $\mathrm{sign}: S_n \to \{\pm 1\}$ by

$$\mathrm{sign}(\sigma) = (-1)^\sigma = \prod_{i<j} \mathrm{sign}(j-i)$$

is a homomorphism, so $A_n := \ker(\mathrm{sign}) \triangleleft S_n$, $|A_n| = \frac{n!}{2}$.

Thm. For $n \neq 4$, A_n is "simple" — it has no normal subgroups except the trivial one and itself.

Thanks, Paul, for teaching for me, and **Parker** for the detailed notes!

September 27, hours 7-8: Isomorphism Theorems review, Jordan-Holder, Simplicity of A_n

September-25-11
11:58 PM

On board. 1. Class photo at 10:55!

2. HW1 is on web!

3. $x^g = g^{-1}xg$ so $(x^g)^h = x^{gh}$ (For Selick: $(x^g)^h = x^{(hg)}$)

4. If $\sigma, \tau \in S_n$, then $\sigma\tau = \sigma \circ \tau$!

5. Today's Agenda: 1, Jordan Hölder.

2. A_n is simple.

Go over the "Selick" handout;

Example: 1. $\phi : S_4 \to S_3$

2. Is there a normal subgroup of S_4 which is isomorphic to S_3 ?

The Jordan-Hölder Theorem. Let G be a finite group. Then there exist a sequence

$$G = G_0 \rhd G_1 \rhd G_2 \rhd \dots \rhd G_n = \{e\} \text{ s.t. } H_i = G_i / G_{i-1}$$

is simple. Furthermore, the sequence (H_i), the "composition series" of G, is unique up to a permutation.

$4 \to A_4 \to A_3$

$\quad\;\;\; 12 \quad\;\; 3$

Example $\underset{24}{S_4} \rhd \underset{12}{A_4} \rhd \underset{4}{\begin{matrix}(12)(34)\\(13)(24)\\(14)(23)\end{matrix}} \rhd \underset{2}{(12)(34)} \rhd \{e\}$

Proof by induction on $|G|$.

Existance: Let G_1 be a maximal normal

Subgroup.

Uniqueness: Use the "diamond principle":

$$\begin{tikzcd}[column sep=small]
 & G \arrow[dl, dash, "H_1"'] \arrow[dr, dash, "H_1'"] & \\
G_1 \arrow[dr, dash, "H_1'"'] & & G_1' \arrow[dl, dash, "H_1"] \\
 & G_1 \cap G_1' &
\end{tikzcd}$$

$G \rhd G_1 \rhd G_2 \cdots$

$G \rhd G_1' \rhd G_2' \cdots$

Claim $G = G_1 G_1'$

Pf $G_1 G_1'$ is normal in G yet bigger that G_1, G_1'.

Theorem. A_n is simple for $n \neq 4$. [Proof as in Lang's]

Cycle Decomposition. $(12)(345) = [21453] = 21453$

Claim If $\sigma = (a_1 \dots a_k)$ and $\tau = [\tau_1 \tau_2 \dots \tau_n]$, then

$$\sigma^\tau = \tau^{-1} \sigma \tau = (\tau^{-1}(a_1), \tau^{-1} a_2, \dots)$$

Corollary σ is conjugate to σ' iff they have the same cycle lengths

Corollary $\#(\text{Conjugacy classes of } S_n) = p(n)$

done line

Lemma 1. Every element of A_n is a product of 3-cycles.

Pf $(12)(23) = (123)$, $(123)(234) = (12)(34)$ ...

Lemma 2. If $N \lhd A_n$ contains a 3-cycle, then $N = A_n$

Pf WLOG, $(123) \in N$. Claim For $\sigma \in S_n$, $(123)^\sigma \in N$ $\left(\begin{matrix}\sigma \in A_n \checkmark \\ \sigma = (12)\sigma' \checkmark\end{matrix}\right)$

So N contains all 3-cycles... $\square$

Now take $N \lhd A_n$ w/ $N \neq \{1\}$

Case 1. N contains an element w/ cycle of length ≥ 4

$\sigma = (123456)\sigma' \in N \qquad \sigma^{-1}(123)\sigma(123)^{-1} = (136)$

Case 2. N contains an element $\sigma = (123)(456)\sigma'$

Consider $\sigma^{-1}(124)\sigma(124)^{-1} = (14263)$

Case 3. N contains $\sigma = (123)($ product of pairs$)$

Then $\sigma^2 = (132) \ldots$

Case 4. Every element of N is a product of disjoint 2-cycles.

$\sigma = (12)(34)\sigma' \Rightarrow \sigma^{-1}(123)\sigma(123)^{-1} = (13)(24) = \tau \in N$

$\Rightarrow \tau^{-1}(125)\tau(125)^{-1} = (13452) \in N$

September 27 Scratch

September-26-11
11:16 AM

Jordan-Hölder:

$$\begin{tikzcd}
 & G \arrow[dl, dash, "H_1"'] \arrow[dr, dash, "H_1'"] & \\
G_1 \arrow[dr, dash, "H_1'"'] & & G_1' \arrow[dl, dash, "H_1"] \\
 & G_1 \cap G_1' &
\end{tikzcd}$$

$G \triangleright G_1 \triangleright G_2 \ldots$

$G \triangleright G_1' \triangleright G_2' \ldots$

Claim $G = G_1 G_1'$

Pf $G_1 G_1'$ is normal in G yet bigger that G_1, G_1'.

October 4, hours 9-10: Simplicity of A_n, Group Actions

October-02-11
7:10 AM

* Agenda: Simplicity of A_n, group actions.
* Makeup class: Thursday at 9AM? (provincial elections day!)

Read Along?

* Go over handouts.

Definition A G-set (left-G-set) $G \times X \to X$
s.t. $(g_1 g_2)x = g_1(g_2 x)$, $ex = x$. Same as $\alpha: G \to S(X)$.
G-sets are a category!
Examples. 1. G itself, under conjugation.
2. Subgroups(G), under conjugation. } not done.
Examples: 1. G/H when H is not-necessarily normal
Sub-example: S_n/S_{n-1} $\sigma S_{n-1} = \sigma' S_{n-1}$ iff
$\sigma(n) = \sigma'(n)$. Let $\tau_i(n) = i$, then
$\sigma \tau_i S_{n-1} = \tau_{\sigma i} S_{n-1}$. So S_n/S_{n-1} is $\{1 \ldots n\}$...
2. If X_1, X_2 are G-sets, then so is $X_1 \sqcup X_2$.
3. $S^2 = SO(3)/SO(2)$

done line

Theorem. 1. Every G-set is a disjoint union of "transitive G-sets"
2. If X is a transitive G set and $x \in X$, then $X \cong G/\mathrm{stab}_X(x)$. (So $|X| \mid |G|$)

Theorem. If X is a G set and x_i are representatives of the orbits, then

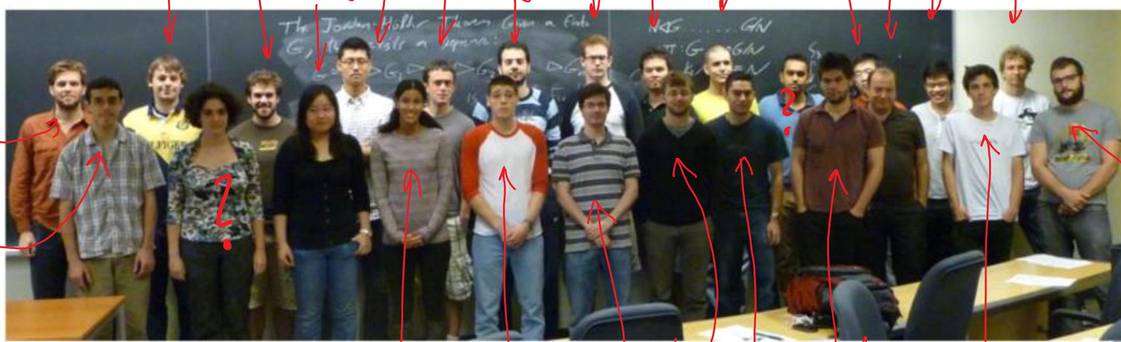
$$|X| = \sum_i \frac{|G|}{|\mathrm{stab}_X(x_i)|}$$

Example. If G is a p-group, the centre of G is not empty.

The Class Photo

From Drorbn

Our class on September 27, 2011:



Class Photo: click to enlarge

Please identify yourself in this photo! There are two ways to do that:

- Log in to this Wiki and edit this page. Put your name, userid, email address and location in the picture in the alphabetical list below.
- Send Dror an email message with this information.

A statistical observation: People in the front row are less web-savvy.

The first option is more fun but less private.

Who We Are... [edit]

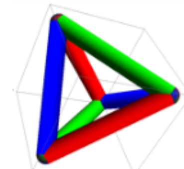
First name	Last name	UserID	Email	In the photo	Comments
Dror	Bar-Natan	Drorbn	drorbn@ math.toronto.edu	facing everybody, as the photographer	Take this entry as a model and leave it first. Otherwise alphabetize by last name. Feel free to leave some fields blank. For better line-breaking, leave a space next to the "@" in email addresses.
Vanessa	Foster	vanessa.foster	vanessa.foster@ mail.utoronto.ca	front row, 4th person from the left	Wearing a long sleeve T with stripes
Parker	Glynn-Adey	pgadey	parker. glynn. adey@ math.toronto.edu	Fifth from the right in the back row	Glowing bald guy with yellow shirt.
Mary	He	ymhe	yanmary.he@ utoronto.ca	Third from the left in the front row	navy sweater
Daniel	Hirschmeier	Dhirschm	daniel.hirschmeier@ utoronto.ca	back row farthest to the right	blonde guy, white t-shirt with a cowboy on it.
Tyler	Holden	tholden	tholden @ math.toronto.edu	Roughly in the middle, under the $N \triangleleft G$ but obscuring the π	Wearing a black polo.
Philip	Mar	Pallenmar	pallenmar@gmail.com	4th from right	white shirt among white shirts
James	Mracek	jmracek	jmracek @ math.toronto.edu	7th from the right (or left) in the back row	Glasses with black and white t-shirt.
Jerrod	Smith	Smith36j	jerrod.smith{at} utoronto{dot}ca	Back row, 3rd from left	Brown t-shirt
Arben	Tapia	Arben	arbentapia@gmail.com	5th from right	dark brown shirt.
Louis-Philippe	Thibault	Lp.thibault	lp.thibault@ utoronto.ca	Back row, 2nd from left	Yellow and Blue t-shirt
Nan	Wu	Wunan3	n.wu@utoronto.ca	3rd from right,back row	red shirt
Lei	Zhang	Zhanglei	leizhang@ comm.utoronto.ca	4th from left, back row	Glasses, white shirt.

The Simplicity of the Alternating Groups

Suggestion for a good deed: TeX this up nicely!

This handout is to be read twice: first read red only, to ascertain that everything in red is easy and boring, then read black and red, to actually understand the proof.

Theorem. The alternating group $A_n \triangleleft S_n$ is simple for $n \neq 4$.



Remark. Easy for $n \leq 3$, false for $n=4$ as there is $\phi: A_4 \twoheadrightarrow A_3$, so assume $n \geq 5$.

Lemma 1. Every element of A_n is a product of 3-cycles.

Pf. Every $\sigma \in A_n$ is a product of an even number of 2-cycles, and $(12)(23)=(123)$ & $(123)(234)=(12)(34)$.

Lemma 2. If $N \triangleleft A_n$ contains a 3-cycle, then $N=A_n$.

Pf. WLOG, $(123) \in N$. Then for all $\sigma \in S_n$, $(123)^\sigma \in N$: if $\sigma \in A_n$, this is clear. Otherwise $\sigma=(12)\sigma'$ w/ $\sigma' \in A_n$, and then as $(123)^{(12)}=(123)^2$, $(123)^\sigma=((123)^2)^{\sigma'} \in N$. So N contains all 3-cycles.

Case 1. N contains an element w/ cycle of length ≥ 4.

Resolution. $\sigma=(123456)\sigma' \in N \Rightarrow \sigma^{-1}(123)\sigma(123)^{-1}=(136) \in N$.

Case 2. N contains an element w/ 2 cycles of length 3.

Res. $\sigma=(123)(456)\sigma' \in N \Rightarrow \sigma^{-1}(124)\sigma(124)^{-1}=(14263) \in N$.

Case 3. N contains $\sigma=(123)\cdot$(a product of disjoint 2-cycles).

Res. $\sigma^2=(132) \in N$

Case 4. Every element of N is product of disjoint 2-cycles.

Res. $\sigma=(12)(34)\sigma' \Rightarrow \sigma^{-1}(123)\sigma(123)^{-1}=(13)(24)=\tau \in N$

$\Rightarrow \tau^{-1}(125)\tau(125)^{-1}=(13452) \in N$ $\square$

Theorem. 1. Every G-set is a disjoint union of "transitive G-sets"

2. If X is a transitive G set and $x \in X$, then $X \cong G/\mathrm{stab}_X(x)$. (So $|X| \,\big|\, |G|$)

Theorem. If X is a G set and x_i are representatives of the orbits, then

$$|X| = \sum_i \frac{|G|}{|\mathrm{stab}_X(x_i)|}$$

Example. If G is a p-group, the centre of G is not empty.

THE SYLOW THEOREMS. Lovely notation: $p^\alpha \| |G|$

$|G| = p^\alpha m$, p prime, $p \nmid m$; $\mathrm{Syl}_p(G) := \{P < G : |P| = p^\alpha\}$ are "Sylow p-subgroups of G". A "p-subgroup" in general, is any subgroup of G of order a power of p.

Sylow I $\mathrm{Syl}_p(G) \neq \emptyset$. Also see comment at bottom.

Proof. By induction on $|G|$, if G has a normal subgroup of order p (or p^β) or if G has a subgroup of order divisible by p^α, we are done. The existance of one of the said types follows from the class equation:

The centre of G the centralizer of y_i in G

Either both are divisible by p,

$$|G| = |Z(G)| + \sum_i (G : C_G(y_i))$$

Either both are divisible by p, or neither. Do 2^{nd} case first.

Where $\{y_i\}$ are representatives from the non-central conjugacy classes of G. $\square$

Theorem. If G is a finite Abelian group of order divisible by a prime p, then G contains an element of order p. "Cauchy's Thm" D&F pp 102

Proof. Enough to find an element of order divisible by p; if z is of order $p \cdot n$, z^n would be of order p. Pick $x \in G, x \neq 1$. If $p \mid |x|$, we're done. Otherwise $p \mid |G/\langle x\rangle|$, so by induction, $\exists y \in G$ s.t. $|\bar{y}| = p$ in $G/\langle x\rangle$. So $y^p \in \langle x\rangle$, i.e., $y^p = x^\alpha$ for some α. Write $|y| = pk + r$ with $0 \leq r < p$, get $e = y^{pk+r} = x^{\alpha k} y^r \Rightarrow y^r \in \langle x \rangle \Rightarrow r = 0$, as $|\bar{y}| = p$. So the order of y is divisible by p. $\square$

See below (A)

done

(A) would have been better to state and prove:

claim: if $\phi : G \to H$ is a morphism & $y \in G$, then $|\phi(y)| \mid |y|$.

Proof. If $|\phi(y)| = n$, $|y| = m$, $m = nq + r$, Then

$$e = \phi(y^m) = \phi(y^{nq})\phi(y^r) = ((\phi(y))^n)^q \phi(y)^r = \phi(y)^r$$

So $r = 0$.

Theorem. 1. Sylow p-groups always exist; $Syl_p(G) \neq \emptyset$.

2. Every p-group is contained in a Sylow-p group.

3. All Sylow-p subgroups of G are conjugate, and

stated $n_p(G) := |Syl_p(G)| = 1 \mod p$ & $n_p(G) \mid |G|$

Groups of order 15.

P_5 is normal in G, P_3 is done normal in G. Any $y \in P_3$ commutes with P_5 [otherwise, $|y| \mid |Aut P_5| = 4$],

(**Aside.** $Aut(\mathbb{Z}/p) = (\mathbb{Z}/p)^*$ so $|Aut(\mathbb{Z}/p)| = p-1$)

So $G = x^i y^j = y^j x^i$ for generators $x \in P_5$, $y \in P_3$.

Aside. If $G = G_1 \cdot G_2$, $G_1 \cap G_2 = \langle e \rangle$, $[G_1, G_2] = \{e\}$, then $G = G_1 \times G_2$

Aside. $\mathbb{Z}/p \times \mathbb{Z}/q = \mathbb{Z}_{pq}$

So $G_{15} = \mathbb{Z}/15$.

Preliminary Lemma.
A group of order p is $\mathbb{Z}/p$.

Aside. $n_p \mid pq \Rightarrow n_p \mid q$, (or $n_p = 1$)
$n_p = 1 \mod p \Rightarrow q = 1 \mod p$
$= p \mid q-1$

This also works for order pq, $p<q$ primes, $p \nmid q-1$.

Groups of order 21. P_7 is normal, P_3 might not be

P_3 may act on P_7. If $P_7 = \langle x \rangle$, $P_3 = \langle y \rangle$, we have $x^y = x$, or x^2, or x^4

Aside. $Aut(\mathbb{Z}/p)$ is cyclic;
$Aut(\mathbb{Z}/7) = \langle x \mapsto x^3 \rangle$
1 3 2 6 4 5

Defn. What does this mean?

This also works for order pq, $p<q$ primes, $p \mid q-1$.

not done

Also did the "extension lemma":

Lemma 1. If $P \in Syl_p(G)$ & $H < N_G(P)$ is a p-group, then $H \subset P$

2. If $P \in Syl_p(G)$, $|x| = p^\beta$, $x \in N_G(P)$, then $x \in P$.

Reformulation: $P \in Syl_p(G)$, $|H| = p^\beta \Rightarrow N_H(P) = H \cap P$

Stronger Sylow 1. If $p^\beta \mid |G|$, then G has a subgroup of order p^β.

Proof. Let $X = \{ S \subseteq G : |S| = p^\beta \}$, and write
(subset)

$|G| = p^{\alpha+\beta} m$ w/ maximal α. By counting & binomial nonsense, $p^\alpha \,|\, |X|$ yet $p^{\alpha+1} \nmid |X|$. G acts on X by translations, so there must be $S_0 \in X$ s.t. $p^{\alpha+1} \nmid |G \cdot S_0|$, hence $p^\beta \,|\, |H = \mathrm{stab}_G(S_0)|$. Yet if $x \in S_0$ then $g \mapsto gx$ is an injection $H \to S_0$, so $|H| \leq |S_0| = p^\beta$, so $|H| = p^\beta$.

October 11, hours 13-14: Finish Sylow, examples, semi-direct products

October-07-11
4:40 PM

On board. 1. HW1 due, HW2 on web.

Theorem. 1. Sylow p-groups always exist; $Syl_p(G) \neq \emptyset$. ✓

2. Every p-group is contained in a Sylow-p group.

3. All Sylow-p subgroups of G are conjugate, and

$$n_p(G) := |Syl_p(G)| = 1 \mod p \quad \& \quad n_p(G) \mid |G|$$

Lemma. 1. If $P \in Syl_p(G)$ & $H < N_G(P)$ is a p-group, then $H \subset P$

2. If $P \in Syl_p(G)$, $|x| = p^\beta$, $x \in N_G(P)$, then $x \in P$.

Reformulation: $P \in Syl_p(G)$, $|H| = p^\beta \Rightarrow N_H(P) = H \cap P$

Agenda. Finish Sylow, do examples, talk about "semi-direct products.

Claim If $H \triangleleft HK$, $K \triangleleft HK$, $H \cap K = \{e\}$, then $HK \cong H \times K$.

Proof $[h,k] = hkh^{-1}k^{-1} \in H \cap K = \{e\}$ .....

Corollary. If $|G| = 15$, $G = P_3 \times P_5 = \mathbb{Z}/15$.

Claim. If $(a,b) = 1$, then $\mathbb{Z}/a \times \mathbb{Z}/b \cong \mathbb{Z}/ab$

Proof. Find s, t s.t. $as + bt = 1$, and write

$$\begin{tikzcd} & \mathbb{Z}/a \arrow[dr, "\cdot b"] & \\ \mathbb{Z}/ab \arrow[ur, "\cdot t"] \arrow[dr, "\cdot s"'] & \times & \mathbb{Z}/ab \\ & \mathbb{Z}/b \arrow[ur, "\cdot a"'] & \end{tikzcd}$$

Proposition. If $P \in Syl_p(G)$, then $|\text{conjugates of } P| = 1 \mod p$. (and $n_p \mid |G|$, of course)

Proof. P acts on the set of its conjugates by conjugation. The orbit $\{P\}$ is a singleton; by lemma, the sizes of all other orbits are divisible by p.

Proposition. If H is a p-subgroup & $P \in Syl_p(G)$, then H is contained in a conjugate of P. [In particular, all]

Proposition. If H is a p-subgroup & $P \in Syl_p(G)$, then H is contained is a conjugate of P. [In particular, all Sylow-p subgroups are conjugates]

Proof. H acts on the set of conjugates of P by conjugation. There must be a singleton orbit — a P' s.t. $H < N_G(P')$.

Semi-Direct Products. If $N < G$, $H < G$, compare $N \times H$ with NH.

There's always $\mu: N \times H \to NH$ by $(n, h) \mapsto nh$.

In general, nothing to say.

If $N \cap H = \{e\}$, injective but image might not be a group.

If $N \cap H = \{e\}$ & $N \triangleleft G$ & $H \triangleleft G$, then $[N, H] = \{e\}$ &

$$NH \cong N \times H.$$

The interesting case is when $N \cap H = \{e\}$, $N \triangleleft G$, H may not.

Get $H \xrightarrow{\phi} Aut(N)$ by $h \mapsto (n \mapsto n^{h^{-1}} = h n h^{-1})$

or $\phi_h(n) = h n h^{-1}$

$$n_1 h_1 n_2 h_2 = n_1 h_1 n_2 h_1^{-1} h_1 h_2 = n_1 \phi_{h_1}(n_2) h_1 h_2$$

Definition. Given abstract N, H & $\phi: H \to Aut(N)$, the semi-direct product $N \rtimes H$.

---

done line

Prop. 1. In the above case, $\mu: N \rtimes H \to NH$ is an isomorphism.

2. $N \triangleleft (N \rtimes H)$ and $N \rtimes H / N \cong H$.

October 11 Scratch

October-07-11
4:50 PM

Claim. If $K \lhd KH$, $H \lhd KH$, $\underbrace{\text{then}}$ and $K \cap H = \{e\}$ then $KH = K \times H$.

$$K \to KH \to KH/H \cong K$$

$$k_1h_1 = k_2h_2 \Rightarrow k_2^{-1}k_1 = h_1h_2^{-1} \Rightarrow k_1 = k_2,\ h_1 = h_2$$

$$hk = kh^k = k^{h^{-1}}h \Rightarrow h^k = h \Rightarrow [h,k] = e.$$

$$h^k h^{-1} = k^{-1}k^{h^{-1}} \Leftrightarrow k^{-1}hkh^{-1} \in H \cap K = \{e\}$$

October 13, hour 15: Semi-direct products

October-11-11
5:51 PM

Agenda. 1 Semi-direct products & examples. / web Comments:

1. Filenames must begin w/ 11-1100
2. what's not linked doesn't exist.

Read Along. Selick 1.8, 1.10.

Riddle Along.

1. Can you find uncountably many nearly-disjoint $[\forall \alpha,\beta\ |A_\alpha \cap A_\beta| < \infty]$ subsets of $\mathbb{N}$?
2. Can you find an uncountable chain $[\forall \alpha,\beta,\ (A_\alpha \subset A_\beta) \vee (A_\beta \subset A_\alpha)]$ of subsets of $\mathbb{N}$?

Semi-Direct Products. Given N, H & $\phi: H \xrightarrow{\text{mor}} \mathrm{Aut}(N)$,

$$N \rtimes_\phi H := \left(N \times H,\ (n_1,h_1)\cdot(n_2 h_2) = (n_1 \phi_{h_1}(n_2),\ h_1 h_2)\right)$$

Thm. 1. $G := N \rtimes_\phi H$ is a group, $H < G$, $N \triangleleft G$ and $G/N \cong H$, and $G = NH$.

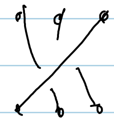
2 If $G = NH$, $N \triangleleft G$, $H < G$, $H \cap N = \emptyset$ then $G \cong N \rtimes_\phi H$.

Small Examples. 1. $D_{2n} = \mathbb{Z}/n \rtimes \{\pm 1\}$

2. $\{ax+b\} = \mathbb{R}^+_b \rtimes \mathbb{R}^\times_a$

3. $\{Ax+b : A \in GL(V), b \in V\} = V_b \rtimes GL(V)_A$

4 "The Poincare Relativity Group" $= \mathbb{R}^4 \rtimes SO(3,1)$

Big Example. $B_n = \pi_1\left(\left(\mathbb{C}^2 - \{\text{diags}\}\right)/S_n\right) =$ 

$$B_n = \left\langle \sigma_1, \ldots \sigma_{n-1} : \begin{array}{l} \sigma_i \sigma_{i+1} \sigma_i = \sigma_{i+1} \sigma_i \sigma_{i+1} \\ \sigma_i \sigma_j = \sigma_j \sigma_i \quad |i-j| > 1 \end{array} \right\rangle$$

an aside on free groups, generators & relations.

Some line

$\pi : B_n \to S_n$ $\qquad PB_n = \ker \pi$

$PB_n \triangleleft B_n$ yet not $B = PB_n \rtimes S_n$  Two reasons why I like this one:

$PB_n \triangleleft B_n$ yet not $B_n = PB_n \rtimes S_n$

Two reasons why I like this one:
1. knotted \$20's.
2. Borromean.

$\rho : PB_n \to PB_{n-1}$ $\quad \ker\rho \cong F_{n-1}$ and

$$PB_n = F_{n-1} \rtimes PB_{n-1} = F_{n-1} \rtimes \left(F_{n-2} \rtimes \left(\ldots \left(F_2 \rtimes \mathbb{Z}\right) \ldots \right)\right)$$

Groups of order 21. $\mathbb{Z}/21$, $\mathbb{Z}/7 \rtimes \mathbb{Z}/3 = \langle x \rangle \rtimes \langle y \rangle$

$\mathrm{Aut}(\mathbb{Z}/7) = \mathbb{Z}/6 = \langle \phi_3 \rangle$; $\phi_3(x) = x^3$; $\quad x^y = x$ or $\underbrace{x^2 \text{ or } x^4}_{\text{isomorphic}}$

$\left(\text{iso: if } x^y = x^2 \text{ \& } \bar{y} = y^2 \text{ then } x^{\bar{y}} = x^4\right)$

Groups of order 12. If $|G| = 12$, $P_4 = \mathbb{Z}/4$ or $(\mathbb{Z}/2)^2$, $P_3 = \mathbb{Z}/3$, and at least one of those is normal, for there's not enough room for 4 P_3 & 3 P_4's. So G is a semi-direct product:

$\mathbb{Z}/4 \rtimes \mathbb{Z}_3$: must be $\mathbb{Z}/4 \times \mathbb{Z}/3 = \mathbb{Z}/12$

$(\mathbb{Z}/2 \times \mathbb{Z}/2) \rtimes \mathbb{Z}_3$: Either direct; $\mathbb{Z}/2 \times \mathbb{Z}/6$

or the fun action of $\underset{\langle (123) \rangle}{\mathbb{Z}/3}$ on $(\mathbb{Z}/2)^2$, giving A_4

$$\begin{array}{c} e \\ (12)(34) \\ (13)(24) \\ (14)(23) \end{array}$$

$\mathbb{Z}/3 \rtimes (\mathbb{Z}/2 \times \mathbb{Z}/2)$: Either direct or $D_6 \times \mathbb{Z}/2 = D_{12}$

$\mathbb{Z}/3 \rtimes \mathbb{Z}/4$: Either direct or $\mathbb{Z}/3 \rtimes \mathbb{Z}/4$

October 18, hours 16-17: Braids, some groups of small order, solvable groups, rings

October-16-11
8:25 PM

Read Along. Selick 1.8, 1.10, 1.11, 2.1.

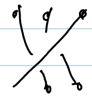
Riddle Along. $\boxed{\forall \alpha\in\mathbb{R}\ \exists a_i\in\mathbb{Q} \text{ s.t. } a_i\to\alpha}$ $\boxed{\mathbb{Q}\cap[0,\alpha]}$ what do these solve?

Term Test. material: everything; sample: See 2010.

Agenda. more semi-directs; tiny bit on solvable groups; rings.

Semi-Direct Products. Given N, H & $\phi: H \xrightarrow{\text{mor}} \mathrm{Aut}(N)$,

$$N\rtimes_\phi H := \left(N\times H,\ (n_1,h_1)\cdot(n_2 h_2) = (n_1\phi_{h_1}(n_2),\ h_1h_2)\right)$$

Big Example. $B_n = \pi_1\left(\left(\mathbb{C}^2 - \{\text{diags}\}\right)/S_n\right) =$ 

$$B_n = \left\langle \sigma_1,\dots\sigma_{n-1} :\ \begin{matrix}\sigma_i\sigma_j=\sigma_j\sigma_i & |i-j|>1\\ \sigma_i\sigma_{i+1}\sigma_i=\sigma_{i+1}\sigma_i\sigma_{i+1}\end{matrix}\right\rangle$$

an aside on free groups, generators & relations.

new class

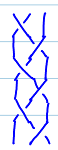
done line

$\pi: B_n\to S_n$ $\qquad PB_n = \ker\pi$

$PB_n \lhd B_n$ yet not $B_n = PB_n\rtimes S_n$

$\rho: PB_n\to PB_{n-1}$ $\qquad \ker\rho = F_{n-1}$ and

$PB_n = F_{n-1}\rtimes PB_{n-1} = F_{n-1}\rtimes(F_{n-2}\rtimes(\dots(F_2\rtimes\mathbb{Z})\dots))$



3 reasons why I like this one: 1. knotted $100's. 2. Borromean. 3. juggling

Groups of order 21. $\mathbb{Z}/21$, $\mathbb{Z}/7\rtimes\mathbb{Z}/3 = \langle x\rangle\rtimes\langle y\rangle$

$\mathrm{Aut}(\mathbb{Z}/7) = \mathbb{Z}/6 = \langle\phi_3\rangle$; $\phi_3(x)=x^3$; $x^y = x$ or x^2 or x^4 (isomorphic)

(iso: if $x^y = x^2$ & $\bar y = y^2$ then $x^{\bar y} = x^4$)

Groups of order 12. If $|G|=12$, $P_4 = \mathbb{Z}/4$ or $(\mathbb{Z}/2)^2$, $P_3 = \mathbb{Z}/3$, and at least one of those is normal, for there's not enough room for 4 P_3 & 3 P_4's. So G is a semi-direct product: $\mathbb{Z}/4\rtimes\mathbb{Z}_3$: must be $\mathbb{Z}/4\times\mathbb{Z}/3 = \mathbb{Z}/12$

$(\mathbb{Z}/2\times\mathbb{Z}/2)\rtimes\mathbb{Z}_3$: Either direct; $\mathbb{Z}/2\times\mathbb{Z}/6$

or the fun action of $\mathbb{Z}/3$ on $(\mathbb{Z}/2)^2$, giving A_4

$\langle(123)\rangle$ $\qquad$ e, $(12)(34)$, $(13)(24)$, $(14)(23)$

$\mathbb{Z}/3\rtimes(\mathbb{Z}/2\times\mathbb{Z}/2)$: Either direct or $D_6\times\mathbb{Z}/2 = D_{12}$

$\mathbb{Z}/3\rtimes\mathbb{Z}/4$: Either direct or $\mathbb{Z}/3\rtimes\mathbb{Z}/4$ $\qquad$ done, but A_4 &

$\mathbb{Z}/3 \rtimes \mathbb{Z}/4$: Either direct or $\mathbb{Z}/3 \rtimes \mathbb{Z}/4$ done, but A_4 &

Solvable Groups. Def G is solvable if all quotients Do not well done
in its Jordan-Hölder series are Abelian.

Thm 1. If $N \trianglelefteq G$, G is solvable iff N & G/N are.

2. If $H < G$ and G is solvable, so is H.

$A \triangleleft B$ $H \cap A \triangleleft H \cap B$? ✓ $\frac{H \cap B}{H \cap A} \longrightarrow B/A$ by $[b]_{H\cap A} \to [b]_A$ is injective.

Rings.

Definition 2.1.1. *A* ***ring*** *consists of a set R together with binary operations + and · satisfying:*

1. $(R, +)$ *forms an abelian group,*
2. $(a \cdot b) \cdot c = a \cdot (b \cdot c)$ $\forall a, b, c \in R$,
3. $\exists 1 \neq 0 \in R$ *such that* $a \cdot 1 = 1 \cdot a = a$ $\forall a \in R$, *and*
4. $a \cdot (b + c) = a \cdot b + a \cdot c$ *and* $(a + b) \cdot c = a \cdot c + b \cdot c$ $\forall a, b, c \in R$.

Also define: Commutative ring.

Examples. $\mathbb{Z}$, $R[x]$, $M_{n\times n}(R)$

Morphisms, (Examples: 1. $\mathbb{Z} \longrightarrow \mathbb{Z}/n$
2. $R \longrightarrow R[x]$ at deg 0
3. $R \to M_{n\times n}(R)$ as diag
4. $ev_u : R[x] \to R$ (if R is commutative)
5. $M_{n\times n}(R[x]) \cong M_{n\times n}(R)[x]$)

October 20, hour 18: Solvable groups, rings

October-18-11
11:30 PM

Read Along. Selick 1.11, 2.1

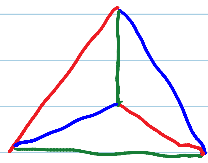
HW 2 due.

Term test Tuesday. my OH today 11:30–12:30; Schuyler OH 10:30–12:30 Mon 5–7 Huron 1028 } monday

Riddle Along ?

Agenda 12, Solvable, rings.

Claim $(\mathbb{Z}/2\times\mathbb{Z}/2)\rtimes\mathbb{Z}/3\cong A_4$



Solvable Groups. Def G is solvable if all quotients in its Jordan-Hölder series are Abelian.

Thm 1. If $N\lhd G$, G is solvable iff N & G/N are.

2. If $H<G$ and G is solvable, so is H.

$A\lhd B$ $\quad H\cap A\lhd H\cap B$? ✓ $\quad \frac{H\cap B}{H\cap A}\to B/A$ by $[b]_{H\cap A}\to[b]_A$ is injective.

Cor. If a group contains A_n, $n\neq 4$, it is not solvable.

Term test line.

Rings.

Definition 2.1.1. *A* **ring** *consists of a set R together with binary operations + and · satisfying:*

1. $(R,+)$ *forms an abelian group,*
2. $(a\cdot b)\cdot c=a\cdot(b\cdot c)\ \forall a,b,c\in R$,
3. $\exists 1\neq 0\in R$ *such that* $a\cdot 1=1\cdot a=a\ \forall a\in R$, *and*
4. $a\cdot(b+c)=a\cdot b+a\cdot c$ *and* $(a+b)\cdot c=a\cdot c+b\cdot c\ \forall a,b,c\in R$.

Also define: Commutative ring.

Done line

Examples. $\mathbb{Z}$, $\mathbb{R}[x]$, $M_{n\times n}(\mathbb{R})$

Morphisms, Examples: 1. $\mathbb{Z}\to\mathbb{Z}/n$
2. $R\to R[x]$ at deg 0
3. $R\to M_{n\times n}(R)$ as diag
4. $ev_u: R[x]\to R$ (if R is commutative)
5. $M_n(R[x])\cong M_n(R)[x]$

(if R is commutative)

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

im, subring, ker, ideal.

Q. Is every ideal a quotient.

Ans. Define R/I.

Good luck w/ term test!

October 25, hours 19-20: Term Test

October-23-11
3:21 PM

See http://katlas.math.toronto.edu/drorbn/index.php?title=11-1100/Term_Test

Subjects. 1. The NCGE story.

2. The isomorphism theorems.

3. Jordan Hölder, Solvable groups.

4. Permutations, simplicity of A_n. ✓

5. G-sets. ✓

6. The Sylow theorems, small examples ✓

7. Semi-direct products, braids. ✓

---

1. Let n be odd. Prove that a subgroup of S_n which contains both (123) & $(123\dots n)$ is A_n.

(Hint: Conjugate your way up, do not use NCGE).

$(123)(345)=(12345)$

$(123)(234)=(12)(34)$

$(12)(34)(123)=(1)(243)$

$(12)(34)(23)(45)=(12453)$

$(123)^{(345)}\sim(124)$

2. Prove that the G-sets G/H_1 & G/H_2 are isomorphic iff H_1 is conjugate to H_2.

$H_1 \overset{\phi}{\longmapsto} gH_2$

$gH_2 \longmapsto H_1$

$h\in H_1 \mapsto hg\in gH_2$

$g^{-1}hg\in H_2$

$$gH_2 \longmapsto H_1$$
$$H_2 \longmapsto g^{-1}H_1$$

3\. 1. Prove that the semi-direct product of two torsion-free groups is torsion-free.

2\. Prove that there is no braid β s.t. $\beta^n = e$.

4\. Sylow-1. (modeled on last year).

Aside: $S_3/\langle(12)\rangle = \left\{ \begin{array}{l} \{[123], [213]\} \\ \{[132], [312]\} \\ \{[231], [321]\} \end{array} \right\}$

Rough Grading Key:

Solve the following 4 problems. Each problem is worth 25 points. You have an hour and fifty minutes. **Neatness counts! Language counts!**

Problem 1. Let G be a finite group, let p be a prime number, and let α be the largest natural number such that $p^\alpha \mid |G|$.

-3

~~18~~ 14 1. Prove that there is a subgroup P of G whose order is p^α. (You are not allowed to use the Sylow theorems, of course). one case wrong.

(-3) $|x|=p$ 11 2. Suppose that $x \in G$ is an element whose order is a power of p, and suppose that x normalizes P. Show that $x \in P$.

Problem 2. A group G is said to be "torsion free" if every non-trivial element thereof has infinite order.

15 1. Prove that a semi-direct of two torsion free groups is again torsion free. (-6) only deduced $h = e_H$ not $g = e_G$.

10 2. Let β be a pure braid on n strands. Prove that if $\beta^7 = e$ then $\beta = e$.

Problem 3. Let H_1 and H_2 be subgroups of some group G. Prove that the left G-sets G/H_1 and G/H_2 are isomorphic (as left G-sets) iff the subgroups H_1 and H_2 are conjugate.

Problem 4.

12 1. Let G be a subgroup of S_n that contains both the transposition (12) and the n-cycle $(123\ldots n)$. Prove that $G = S_n$. (Hint: Conjugate your way up, do not use non commutative Gaussian elimination).

12 2. Let n be odd and let G be a subgroup of S_n that contains both the 3-cycle (123) and the n-cycle $(123\ldots n)$. Prove that $G = A_n$. (Hint: For the lower bound, conjugate your way up, do not use non commutative Gaussian elimination).

4 3. In the previous part, what if n is even?

78

Good Luck!

Problem 3:

$\Leftarrow$: If $H_2 = g^{-1}H_1 g$

5 define $\Psi: G/H_1 \to G/H_2$ by $\Psi(xH_1) = xgH_2$

2 check well-def: $xh_1H_1 \xrightarrow{\Psi} xh_1gH_2 = xgh_1^g H_2 = xgH_2$

2 check G-set morphism.

2 check injectivity.

2 check surjectivity.

$\Rightarrow$: If $\phi: G/H_1 \to G/H_2$ is an isomorphism,

5 $\phi(H_1) = gH_2$ for some g

4 $gH_2 = \phi(h_1H_1) = h_1gH_2 \Rightarrow g^{-1}h_1g \in H_2 \Rightarrow g^{-1}H_1g \subset H_2$

3 but also $\phi^{-1}(gH_2) = H_1$ so

$$\phi^{-1}(H_2) = g^{-1}H_1$$

so by analogy, $gH_2g^{-1} \subset H_1$

$$\Rightarrow g^{-1}H_1g = H_2$$

$gx = y \Rightarrow x = g^{-1}y$

Further Thoughts

Upon further thought and after talking to some students and some email exchanges, I think I made (at least) three mistakes around this term exam:

- It was too long, overall, especially given my insistence that "neatness counts, language counts". Asking just three of the four questions would have been enough.
- Question 3 required too much abstract thought given the time constraints. I should have either given a significant hint or left it out.
- I shouldn't have "rushed to publish" - I should have given myself a little more time to think before returning the exams. Marking up is always possible, but it is better done before the grades are first published, not after.

Anyway, in light of the first point above, I will consider this exam as if the perfect mark in it was 75, effectively multiplying every grade by a factor of 4/3. The few people whose grade now is more than 100 get to keep those extra points, though the maximal possible grade in this class remains an A+.

People who haven't tried don't realize how hard learning may be, forcing you to confront your fears and insecurities (yet it is well worth it!). Try teaching (recommended!) and you'll see it's hard too. After more than 20 years I still make mistakes.

Pasted from <http://katlas.math.toronto.edu/drorbn/index.php?title=11-1100/Term_Test>

October 27, hour 21: Rings, ideals, isomorphism theorems, prime and maximal ideals

October-25-11
11:22 AM

Read Along. Selick 2.1-2.3 **Term test.** Discussion at 10:45 also return HW2.

Goal. 1. Rings, ideals, isomorphisms.

2. Prime & maximal ideals, domains and fields.

Definition 2.1.1. *A **ring** consists of a set R together with binary operations $+$ and $\cdot$ satisfying:*

1. *$(R, +)$ forms an abelian group,*
2. *$(a \cdot b) \cdot c = a \cdot (b \cdot c)$ $\forall a, b, c \in R$,*
3. *$\exists 1 \neq 0 \in R$ such that $a \cdot 1 = 1 \cdot a = a$ $\forall a \in R$, and*
4. *$a \cdot (b + c) = a \cdot b + a \cdot c$ and $(a + b) \cdot c = a \cdot c + b \cdot c$ $\forall a, b, c \in R$.*

Also define: Commutative ring.

Examples. $\mathbb{Z}$, $R[x]$, $M_{n\times n}(R)$

Morphisms, (Examples: 1. $\mathbb{Z} \to \mathbb{Z}/n$ 2. $R \to R[x]$ at deg 0 3. $R \to M_{n\times n}(R)$ as diag 4. $ev_u : R[x] \to R$ (if R is commutative) 5. $M_{n\times n}(R[x]) \cong M_{n\times n}(R)[x]$)

im, subring, ker, ideal.

done line

Q. Is every ideal a quotient?

Ans. Define R/I.

The Isomorphism theorems. 1. $f : R \to S \Rightarrow R/\ker(f) = \operatorname{im} f$.

2. $\dfrac{A+I}{I} \cong A/_{A\cap I}$ $A \subset R$ subring, $I \subset R$ ideal.

3. $I \subset J \subset R$ ideals $\Rightarrow \dfrac{R/I}{J/I} \cong R/J$

4. Given an ideal I of R, there's a bijection between ideals $I \subset J \subset R$ & ideals of R/I.

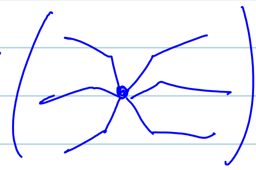
November 1, hours 22-23: Ideals, isomorphism theorems, prime and maximal ideals

October-28-11
3:10 PM

Agenda. Quotients, isomorphism thms, "better rings".

Read Along. Selick 2.1–2.3.

HW3 on web.

G() = ?

Def. $I \subset R$ is an ideal...

Claim. If $\phi : R \to S$ is a morphism of rings, then $\ker(\phi)$ is an ideal in R.

Q. Is every ideal a quotient?

Ans. Define R/I.

Example. $\mathbb{R}[x]/\langle x^2+1 \rangle = R_1$

The Isomorphism theorems. 1. $f : R \to S \Rightarrow R/\ker(f) = \operatorname{im} f$.

(Example: $ev_i : \mathbb{R}[x] \to \mathbb{C} \Rightarrow R_1 \cong \mathbb{C}$)

2. $\frac{A+I}{I} \cong A/A\cap I$ $\quad$ $A \subset R$ subring, $I \subset R$ ideal.

3. $I \subset J \subset R$ ideals $\Rightarrow \frac{R/I}{J/I} \cong R/J$

4. Given an ideal I of R, there's a bijection between ideals $I \subset J \subset R$ & ideals of R/I.

Better Rings. 1. The ultimate:

Field [commutative, $F \setminus \{0\}$ a group]

[almost all of high-school & freshman algebra carries through]

("division ring", if not commutative

Example: $\mathbb{H} = \{a+bi+cj+dk\} / \; i^2=j^2=k^2=-1, \; ij=k$

useful for 3D rotations, etc...)

2. (Integral) domains: commutative, has no 0-divisors.

How make? For ideals which, R/I is a field or a domain?

.... From now on, R is commutative.

Maximal Ideals. 1. Definition.

2. $I \subset R$ is maximal $\iff$ R/I is a field.

Fishy proof: Use the 4th isomorphism theorem.

Honest proof: $\Rightarrow$: $x \notin I \Rightarrow Rx + I = R \Rightarrow \exists y \in R \; yx + I = 1 + I$

$\Leftarrow$ $J \supsetneq I$, $x \in J \setminus I \Rightarrow [x]_I \neq 0 \Rightarrow \exists y \; xy - 1 \in I \Rightarrow 1 \in J$

Examples. 1. $p\mathbb{Z}$ is a maximal ideal in $\mathbb{Z}$.

2. $S = \ell^\infty = \left\{ \begin{matrix} \text{bndd seq's} \\ \text{in } \mathbb{R} \end{matrix} \right\}$ $A_n = \{(a_i) : a_n = 0\}$

done line

Fishy

Theorem. Every ideal is contained in a maximal ideal.

Proof using Zorn's Lemma.

Theorem There exists a function

$$\mathrm{Lim} : \left\{ \begin{matrix} \text{bndd seq's} \\ \text{in } \mathbb{R} \end{matrix} \right\} \to \mathbb{R} \quad \text{s.t.}$$

1. If (a_n) is convergent, $\lim a_n = \mathrm{Lim}\, a_n$.
2. $\mathrm{Lim}\,(a_n + b_n) = \mathrm{Lim}\,(a) + \mathrm{Lim}\,(b_n)$
3. $\mathrm{Lim}\,(a_n b_n) = \mathrm{Lim}\,(a_n) \cdot \mathrm{Lim}\,(b_n)$

+ more....

Proof. $S = \{\text{bndd seq's in } \mathbb{R}\}$ $I = \{(a_n) : a_n \neq 0 \text{ for finitely many } n\text{'s}\}$

J - a maximal ideal containing I.

$$\mathrm{Lim} : S \to S/J \underset{?}{=} \mathbb{R}$$

Prime Ideals. 1. Definition $P \subset R$ is prime if $ab \in P$
$\Rightarrow a \in P$ or $b \in P$.

2. Theorem. R/P is a domain iff P is prime.

Proof. $\Rightarrow$ $ab \in P \Rightarrow [ab] = 0 \Rightarrow [a][b] = 0 \Rightarrow$ $[a]=0 \Rightarrow a \in P$ or $[b]=0 \Rightarrow b \in P$.

$\Leftarrow$ $[a][b] = 0 \Rightarrow [ab] = 0 \Rightarrow ab \in P \Rightarrow$ $a \in P \Rightarrow [a]=0$ or $b \in P \Rightarrow [b]=0$

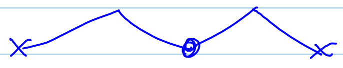
Theorem. A maximal ideal is prime.

November 3, hour 24: Prime and maximal ideals

November-01-11
9:55 PM

Appeals deadline noon! No class on Tuesday!

Read Along. Selick 2.1-2.3

Riddle Along. $\mathcal{G}($  $) = ?$

Agenda. "better ideals".

.... From now on, R is commutative.

Maximal Ideals. 1. Definition.

2. $I \subset R$ is maximal $\Longleftrightarrow R/I$ is a field.

Example. $S = \ell^\infty = \left\{ \begin{array}{c} \text{bndd seq's} \\ \text{in } \mathbb{R} \end{array} \right\}$ $\quad A_n = \{(a_i) : a_n = 0\}$

Fishy **Theorem.** Every ideal is contained in a maximal ideal.

Proof using Zorn's Lemma.

Theorem There exists a function

$$\mathrm{Lim} : \left\{ \begin{array}{c} \text{bndd seq's} \\ \text{in } \mathbb{R} \end{array} \right\} \to \mathbb{R} \quad \text{s.t.}$$

1. If (a_n) is convergent, $\lim a_n = \mathrm{Lim}\, a_n$.
2. $\mathrm{Lim}\,(a_n + b_n) = \mathrm{Lim}\,(a) + \mathrm{Lim}\,(b_n)$ + more....
3. $\mathrm{Lim}\,(a_n b_n) = \mathrm{Lim}\,(a_n) \cdot \mathrm{Lim}\,(b_n)$

Proof. $S = \{\text{bndd seq's in } \mathbb{R}\}$ $\quad I = \left\{ (a_n) : \begin{array}{c} a_n \neq 0 \text{ for} \\ \text{finitely many } n\text{'s} \end{array} \right\}$

J - a maximal ideal containing I.

$$\mathrm{Lim} : S \to S/J \overset{?}{=} \mathbb{R}$$

Prime Ideals. 1. Definition $P \subset R$ is prime if $ab \in P$
$\Rightarrow a \in P$ or $b \in P$.

2. Theorem. R/P is a domain iff P is prime.

Proof $\Rightarrow$ $ab \in P \Rightarrow [ab] = 0 \Rightarrow [a][b] = 0 \Rightarrow$ $[a]=0 \Rightarrow a \in P$ or $[b]=0 \Rightarrow b \in P$.

$\Leftarrow$ $[a][b] = 0 \Rightarrow [ab] = 0 \Rightarrow ab \in P \Rightarrow$ $a \in P \Rightarrow [a]=0$ or $b \in P \Rightarrow [b]=0$

Theorem. A maximal ideal is prime.

From this point, R is a Domain (commutative, no 0-divisors)

Primes. 1. $a|b$ $\qquad (a|b \wedge b|a \Rightarrow a = ub)$

done line

2. $\gcd(a,b) = q$; $\gcd = q$ & $\gcd = q' \Rightarrow q' = uq$.

3. Primes: $p \neq 0$ non-unit $\qquad p|ab \Rightarrow p|a$ or $p|b$

p is prime iff $\langle p \rangle$ is prime ideal.

4. Irreducible $x = ab \Rightarrow a \in R^* \vee b \in R^*$

Claim. prime $\Rightarrow$ irreducible

$p = ab \Rightarrow p|a \Rightarrow a = pc$

$\Rightarrow p = pcb \Rightarrow cb = 1 \Rightarrow b \in R^*$

Counterexample: in $\mathbb{Z}[\sqrt{-5}]$, 2 is irred (for norm reasons) but not prime, as $2 | (1-\sqrt{-5})(1+\sqrt{-5}) = 6$

Continues 10-1100/Lims.

$S = \{\text{bndd seq's in } \mathbb{R}\}$ $I = \{(a_n) : a_n \neq 0 \text{ for finitely many } n\text{'s}\}$

J - a maximal ideal containing I.

Thm. $\text{Lim}: S \longrightarrow S/J \underset{!}{=} \mathbb{R}$ extends lim.

Definition. Say that $A \subset \mathbb{N}$ is "essential" if $1_A \notin J$.

Claim. $\{A : A \text{ is essential}\} = \mathcal{U}$ is a non-principal ultrafilter on $\mathbb{N}$.

Proof. J is prime $\Rightarrow (A, B \in \mathcal{U} \Rightarrow A \cap B \in \mathcal{U})$

$\mathbb{N} \in \mathcal{U}$ because $1_S = 1_{\mathbb{N}}$ is not in J.

$A \in \mathcal{U} \Leftrightarrow 1_A \notin J \Leftrightarrow (1_{\mathbb{N}} - 1_A) \in J \Leftrightarrow 1_{A^c} \in J \Leftrightarrow A^c \notin \mathcal{U}$

Monotonicity because J is an ideal: $A \subset B, B \notin \mathcal{U}$ $\Rightarrow 1_B \in J \Rightarrow 1_A = 1_B \cdot 1_A \in J \Rightarrow A \notin \mathcal{U}$.

Principality from the definition of I.

Definition. $\hat{J} = \{(a_n) : \forall \epsilon > 0 \ \{n : |a_n| < \epsilon\} \text{ is essential}\}$

Claim. $J \subset \hat{J}$

Proof. Suppose $(a_n) \in J$, and $\epsilon > 0$ is such that $\{n : |a_n| \geq \epsilon\}$ is essential.

Let $b_n = \begin{cases} \frac{1}{a_n} & |a_n| \geq \epsilon, \\ 0 & \text{otherwise.} \end{cases}$

Then $a_n \cdot b_n = 1$ on an essential set,

so $\overline{a_n}\,\overline{b_n} \neq 0$, so $\overline{a_n} \neq 0$ so $a_n \notin J$ $\Rightarrow\Leftarrow$.

Now by the maximallity of J, $J = \hat{J}$.

Claim. For every $(a_n) \in S$ there is some $\alpha \in \mathbb{R}$ s.t. $a_n - \alpha I \in \hat{J}$

(follows from convergence on ultrafilters)

$\Longrightarrow$ $\mathrm{Lim}(a_n) = \mathrm{Lim}(\alpha I)$

Claim. The map $\mathbb{R} \longrightarrow S/J$ via $\alpha \longmapsto \alpha I$ is injective and surjective.

Proof. surjectivity was just shown. Injectivity is because any morphism of fields is injective, as field have no ideals to serve as kernels.

$\Longrightarrow$ Using $\alpha \longmapsto \alpha I$ to identify S/J with $\mathbb{R}$, the resulting Lim has all the required properties. $\square$

November 10, hour 25: Primes, UFDs, One Theorem Two Corollaries Four Weeks

November-04-11
9:22 AM

Local goal. Prime ideals & primes

Euclidean $\Rightarrow$ PID $\Rightarrow$ UFD

Read Aluffi. slides 2.2, 2.7, (2.8, 2.9)

~~Publish~~ link or perish

Global goal "v.s." "f.d." "$\mathbb{Z}, F[x]$"

IT2C4W: M f.g. over a PID $R \Rightarrow$ Uniquely

$$M \cong R^k \oplus \bigoplus R/(p_i^{s_i}) \quad p_i \text{ prime}, \; s_i \geq 1$$

Cor 1. A f.g. Abelian $\Rightarrow$

$$A \cong \mathbb{Z}^k \oplus \bigoplus \mathbb{Z}/p_i^{s_i}$$

Cor 2. $A \in M_{n\times n}(\mathbb{C})$ has a "Jordan form"

(Comment on linking at http://katlas.math.toronto.edu/drorbn/index.php?title=User:Lp.thibault)

Did: Maximal & prime ideals, Fields & domains.

R is a commutative integral domain.

Primes. 1. $a|b$ "a, b are associates" $(a|b \wedge b|a \Rightarrow a = ub)$

2. $\gcd(a,b) = q$; $\gcd = q$ & $\gcd = q' \Rightarrow q' = uq$.

3. Primes: $p \neq 0$ non-unit $\quad p|ab \Rightarrow p|a$ or $p|b$

p is prime iff $\langle p \rangle$ is prime ideal.

4. Irreducible $x = ab \Rightarrow a \in R^* \vee b \in R^*$

Claim. prime $\Rightarrow$ irreducible

$p = ab \Rightarrow p|a \Rightarrow a = pc$

$\Rightarrow p = pcb \Rightarrow cb = 1 \Rightarrow b \in R^*$

Counterexample: in $\mathbb{Z}[\sqrt{-5}]$, 2 is irred (for norm reasons) but not prime, as $2 \mid (1-\sqrt{-5})(1+\sqrt{-5}) = 6$

UFDs. Def. Every non-zero element can be factored into primes.

Thm. Uniqueness up to units & a permutation.

done line.

Thm. In a UFD, Prime $\Leftrightarrow$ irreducible.

Pf. If an irrd. is decomposed, the decomposition must have length 1.

Thm. UFD $\Leftrightarrow$ every $x \neq 0$, has a unique decomposition into irreducibles. Pf need irred $\Rightarrow$ prime. If x is irred & $x \mid ab$, then $zx = \underbrace{a_1 \dots a_n b_1 \dots b_m}_{\text{irreds}} \Rightarrow x \sim a_i$ or $x \sim b_j \Rightarrow x \mid a \vee x \mid b$.

Thm. In a UFD gcd's always exist.

November-14-11
4:53 PM

HW3 due, HW4 on web soon.

Global goal: IT2C4W: M f.g. module over a PID $R \Rightarrow$ uniquely

$M \cong R^k \oplus \bigoplus R/(p_i^{s_i})$ p_i prime, $s_i \geq 1$

Cor 1. A f.g. Abelian $\Rightarrow A \cong \mathbb{Z}^k \oplus \bigoplus \mathbb{Z}/p_i^{s_i}$

Cor 2. $A \in M_{n\times n}(\mathbb{C})$ has a "Jordan form"

No Joy Agenda. Euc $\Rightarrow$ PID $\Rightarrow$ UFD.

UFDs. Def. Every non-zero element can be factored into primes.

Thm. Uniqueness up to units & a permutation.

Thm. In a UFD, prime $\Leftrightarrow$ irreducible.

Pf If an irrd. is decomposed, the decomposition must have length 1.

Thm. UFD $\Leftrightarrow$ every $x \neq 0$ has a unique decomposition into irreducibles.

Pf need irrd $\Rightarrow$ prime. If x is irrd & $x|ab$, then $zx = \underbrace{a_1 \dots a_n b_1 \dots b_m}_{\text{irreds}} \Rightarrow x \sim a_i$ or $x \sim b_j \Rightarrow x|a \vee x|b$.

Thm. In a UFD gcd's always exist.

How show UFD? Norm $\Rightarrow$ "PID" $\Rightarrow$ UFD.

Def. Euclidean domain: has a "norm" $e: R - \{0\} \to \mathbb{N}$ s.t.

1. $e(ab) \geq e(a)$
2. $\forall a, b\ \exists q, r$ s.t. $a = qb + r$ & $r = 0$ or $e(r) < e(b)$

Example. 1. $\mathbb{Z}$

2. $F[x]$

Example $a = x^3 - 2x^2 - 5x + 12$, $b = x^2 + 1$

$\dots\ r = -6x + 14$
$a(i) = 14 - 6i$ } why?

theorem. A Euclidean domain is a "PID" (def).
(Thm: a PID is a UFD, later)

Proposition. In a PID, every prime ideal is maximal.

Pf. $I = \langle p \rangle$ prime, $I \subset J = \langle x \rangle \subset R \Rightarrow p = ax \Rightarrow$

$(a \in R^* \Rightarrow I = J) \vee (x \in R^* \Rightarrow J = R)$

..

theorem. PID $\Rightarrow$ UFD.

What proof. Take $x=x_1$; unless $x_1 \in R^*$, $x_1 \in M_1$ where M_1 is a maximal ideal containing $\langle x_1 \rangle$. $M_1 = \langle p_1 \rangle$, p_1 prime. So $x_1 = p_1 x_2$; unless $x_2 \in R^*$ $x_2 \in \langle x_2 \rangle \subset M_2$ maximal $M_2 = \langle p_2 \rangle$, $x_2 = p_2 x_3, \ldots$ if process was infinite,

$\langle x_1 \rangle \subsetneq \langle x_2 \rangle \subsetneq \langle x_3 \rangle \subsetneq \ldots$

$\langle x_n \rangle \subset \langle x_{n+1} \rangle$ as $x_n = p_n x_{n+1}$
if $x_{n+1} \in \langle x_n \rangle$, $x_{n+1} = a x_n$ so
$x_n = p_n a x_n$ & p's not prime.

But a PID is "Noetherian", so the process must terminate.

So $x = x_1 = p_1 x_2 = p_1 p_2 x_3 = \ldots = p_1 p_2 \ldots p_n u$

theorem. In a PID $\langle a,b \rangle = \langle \gcd(a,b) \rangle$. (so $\gcd(a,b) = sa+tb$)

The Euclidean Algorithm. In a Euc. Domain, a practical algorithm for finding $s(a,b)$ & $t(a,b)$ as above: WLOG, $e(a) \geq e(b)$

If $\langle a,b \rangle = \langle b \rangle$, take $(s,t) = (0,1)$. Otherwise $a = bq + r$, $e(r) < e(b)$,

$\langle a,b \rangle = \langle b,r \rangle$ so if $g = s'b + t'r$, then

$$g = s'b + t'(a-bq) = \underbrace{t'}_{s} a + \underbrace{(s'-t'q)}_{t} b$$

---

theorem. R is a PID iff it has a "Dedekind-Hasse" norm: $d: R - \{0\} \to \mathbb{N}_{>0}$ [or add $d(0)=0$]
s.t. if $a,b \neq 0$ either $a \in \langle b \rangle$ or $\exists\, 0 \neq x \in \langle a,b \rangle$ w/ $d(x) < d(b)$.

pf. $\Leftarrow$ as before. $\Rightarrow$ Replace every prime by 2, get even a "multiplicative" D-H norm.

done line

If time: Modules, $\mathbb{Z}$, V, $T: V \to V$.

November 17, hour 28: The ring of modules

November-16-11
8:55 AM

IT2C3W: [M f.g./R PID $\Rightarrow M \cong R^k \oplus \bigoplus R/\langle p_i^{s_i} \rangle$]

$\Rightarrow$ Structure of f.g. Abelian groups, J.C.F.

Riddle Along. Allowing AC but not CH, can you find a chain ($A, B \in \mathcal{B} \Rightarrow (A \subset B) \vee (B \subset A)$) of measure 0 subsets of $\mathbb{R}$ whose union isn't of measure 0?

Today. The "ring" of modules.

Reminder. An R-module: "A vector space over a ring".

Examples. 1. V.S. over a field.

2. Abelian groups over $\mathbb{Z}$.

3. Given $T: V \to V$, V over $F[x]$.

4. Given ideal $I \subset R$, R/I over R.

5. Column vectors R^n over $M_{n\times n}$ (Left module R-mod)
row vectors $(R^n)^T$ over $M_{n\times n}$ (right module mod-R)

Def/Claim. R-mod & mod-R are categories.

Def/claim. Submodules, $\ker \phi$, $\operatorname{im} \phi$, M/N

Boring Theorems. 1. $\phi: M \to N \Rightarrow M/\ker\phi \cong \operatorname{im}\phi$

2. $A, B \subset M \Rightarrow \dfrac{A+B}{B} \cong A/A\cap B$

3. $A \subset B \subset M \Rightarrow M/A \,/\, B/A \cong M/B$

4. Also dull.

Direct sums. $M, N \Rightarrow M \oplus N$

$$\begin{tikzcd} M \arrow[dr] \arrow[drr, bend left] & & \\ & M\oplus N \arrow[r, dashed, "\exists!"] & P \\ N \arrow[ur] \arrow[urr, bend right] & & \end{tikzcd}
\qquad
\begin{tikzcd} & & M \\ P \arrow[r, dashed, "\exists!"] \arrow[urr, bend left] \arrow[drr, bend right] & M\oplus N \arrow[ur] \arrow[dr] & \\ & & N \end{tikzcd}$$

Product

$$\left(\begin{tikzcd} & M \arrow[dr] & \\ P \arrow[ur] \arrow[dr] \arrow[rr, dashed, "\exists!"] & & M\oplus N \\ & N \arrow[ur, "\text{sum}"'] & \end{tikzcd} \qquad \begin{tikzcd} & M \arrow[dr] & \\ M\oplus N \arrow[ur] \arrow[dr] \arrow[rr, dashed, "\exists!"] & & P \\ & N \arrow[ur, "\text{product}"'] & \end{tikzcd}\right)$$

$$\begin{tikzcd} & M\oplus N \arrow[r, dashed, "\exists!"] & P \\ N \arrow[ur] \arrow[urr, "\text{sum}"'] & & \end{tikzcd} \qquad \begin{tikzcd} P \arrow[r, dashed, "\exists!"] \arrow[rr, bend right] & M\oplus N \arrow[r] & N \text{ product} \end{tikzcd}$$

differ for infinite families!

$$\mathrm{Hom}\left(\bigoplus^{n} N_j, \bigoplus^{m} M_i\right) = \left\{\begin{pmatrix} a_{11} & a_{1n} \\ a_{m1} & a_{mn} \end{pmatrix} : a_{ij} \in \mathrm{Hom}(M_i, N_j)\right\}$$

done lin

Example: $\dim(V\oplus W) = \dim V + \dim W$.

Example: if $\gcd(a,b)=1$ $\quad 1 = sa+tb$ [e.g., if R is a PID]

$$\frac{R}{\langle a\rangle} \oplus \frac{R}{\langle b\rangle} \cong \frac{R}{\langle ab\rangle} \quad \text{via} \quad \begin{tikzcd} R/\langle a\rangle \arrow[dr, "t\cdot b"] & & & R/\langle a\rangle \\ \oplus & R/\langle ab\rangle \arrow[urr, "1"] \arrow[drr, "1"'] & & \oplus \\ R/\langle b\rangle \arrow[ur, "s\cdot a"'] & & & R/\langle b\rangle \end{tikzcd}$$

$$\mathbb{Z}/7 \oplus \mathbb{Z}/11 \oplus \mathbb{Z}/13 \cong \mathbb{Z}/77 \oplus \mathbb{Z}/13 \cong \mathbb{Z}/1{,}001$$ "the chinese remainder theorem"

November 22, hours 29-30: Proof of the Structure Theorem - Existence

November-20-11
12:22 PM

IT2C2W: [M f.g./R PID $\Rightarrow M \cong R^k \oplus \bigoplus R/\langle p_i^{s_i}\rangle$]

$\Rightarrow$ structure of f.g. Abelian groups, J.C.F.

Goal: The existence part, the "ring" of modules.

Read Along: You tell me!

Let R be a PID...

Sketch $\{\text{matrices}\}/\text{row \& col. ops \& more} \xrightarrow{\text{onto}} \{\text{f.g. modules}\}$

Finite by infinite, but the infinity is just a nuisance.

So we're back to Gaussian elimination!

Def M is "finitely generated" if $\exists\, g_1 \ldots g_n \in M$ s.t. $M = \{\sum a_i g_i : a_i \in R\}$.

$$R^X \xrightarrow{A} R^g \xrightarrow{\pi} M \qquad \ker \pi = \langle r_x : x \in X\rangle$$

$$A = \underbrace{(\qquad\qquad)}_{X}\}g \qquad A \in M_{g\times X}(R)$$

... In general, every $g\times X$ matrix determined a f.g. module, and every f.g. modules arises in this way.

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

$$\begin{tikzcd} R^X \arrow[r, "A"] \arrow[dr, phantom, "\circlearrowleft"] & R^g \arrow[d, "P"] \\ R^X \arrow[u, "Q"] \arrow[r, "A'"] & R^g \end{tikzcd}$$

Claim if P, Q are invertible on the left, then $M = R^g/\operatorname{im} A$ and $M' = R^g/\operatorname{im} A'$ are isomorphic.

Pf $\Phi : M \to M'$ by $[\alpha]_{\operatorname{im} A} \to [P\alpha]_{\operatorname{im} A'}$

P can be interpreted as $g \times g$ matrix
Q can be interpreted as an $X \times X$ column-finite matrix; $A' = PAQ$

.... Can do arbitrary invertible row operations on A, and arbitrary invertible column ops, provided each column is touched finitely many times.

Of all the matrices reachable from A, let A' be the one having an entry with the smallest D-H norm; w.l.o.g., that entry is a_{11}.

Claim a_{11} divides all other entries in its row & column.

Pf 1 For a Euclidean domain.

Pf 2 In a PID, if $q = \gcd(a,b) = sa + tb$, then

$$(a \ b)\begin{pmatrix} s & -b/q \\ t & a/q \end{pmatrix} = (q \ 0), \text{ while } \begin{pmatrix} s & -b/q \\ t & a/q \end{pmatrix}^{-1} = \begin{pmatrix} a/q & b/q \\ -t & s \end{pmatrix} \qquad \square$$

$\Longrightarrow$ W.l.o.g, the row & column of a_{11} are 0 (except for a_{11})

$\Longrightarrow$ all entries of A are divisible by a_{11}:

$$A = \begin{pmatrix} a_{11} & \text{---} \ 0 \ \text{---} \\ 0 & \\ \vdots & A_1 \ \substack{\text{all entries} \\ \text{divisible} \\ \text{by } a_{11}} \\ 0 & \end{pmatrix}$$

Continue to get $A \sim \left(\begin{array}{cc|c} a_{11} & & \\ & a_{22} & 0 \\ \hline & 0 & 0 \end{array}\right)$ (w.l.o.g., A is square) continue to get $A \sim \left(\begin{array}{c|c} \ddots & 0 \\ \hline 0 & 0 \end{array}\right)$ (□ is square)

So $M \cong \bigoplus_{i=1}^{g} R/\langle a_{ii}\rangle \cong R^k \oplus \bigoplus R/\langle a_i\rangle$

$a_1 \mid a_2 \mid \dots \mid a_n$

Claim. If $\gcd(a,b)=1$ $\quad 1 = sa+tb$ $\quad$ [e.g., if R is a PID]

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

Aside: $\mathbb{Z}/7 \oplus \mathbb{Z}/11 \oplus \mathbb{Z}/13 \cong \mathbb{Z}/77 \oplus \mathbb{Z}/13 \cong \mathbb{Z}/1{,}001$

"the chinese remainder theorem"

Proof 1. as before, use

$$\begin{tikzcd} R/\langle a\rangle \arrow[dr, "t\cdot b"] & & R/\langle a\rangle \\ & R/\langle ab\rangle \arrow[ur, "1"] \arrow[dr, "1"'] & \oplus \\ R/\langle b\rangle \arrow[ur, "s\cdot a"'] & & R/\langle b\rangle \end{tikzcd}$$ □

Proof 2. Using the techniques above, $\begin{pmatrix} a & 0 \\ 0 & b\end{pmatrix} \sim \begin{pmatrix} 1 & 0 \\ 0 & ab\end{pmatrix}$. □ □

done line

Recall that $(R\text{-mod}, \oplus)$ is an "Abelian group" (really, an Abelian semi-group, and even this is not precise)

Tensor Products. Given M, N

$$M \otimes_R N := \left\{ \sum_{i=1}^{n} a_i (m_i \otimes n_i) : n \in \mathbb{N}, a_i \in R \right\} \Big/ \begin{array}{l} (am)\otimes n = a(m\otimes n) = m\otimes(an) \\ (m_1+m_2)\otimes n = \dots \\ m\otimes(n_1+n_2) = \dots \end{array}$$

$M \times N \xrightarrow{\text{bilinear}}$

Example. $\dim V\otimes W = (\dim V)\cdot(\dim W)$

Example. If $q \in \gcd(a,b)$, $q = sa+tb$ $\quad \frac{R}{\langle a\rangle} \otimes \frac{R}{\langle b\rangle} \cong \frac{R}{\langle q\rangle}$

pf. $[r_1]_a \otimes [r_2]_b \longrightarrow [r_1 \cdot r_2]_q$ $\qquad [q]\otimes[1] = [sa+tb]\otimes[1] = 0$

$[r]_q \longrightarrow [r]_a \otimes [1]_b$ $\qquad [r_1 r_2]\otimes[1] = [r_1][r_2]$

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

theorem. $(M,N) \longmapsto M\otimes N$ is a "bifunctor".

Nov 22 Preps

November-20-11
12:41 PM

$$\begin{tikzcd}
R_M \arrow[r, hook] \arrow[d] & F^m \arrow[r] \arrow[d] & M \arrow[r] \arrow[d] & 0 \\
R_N \arrow[r] & F^n \arrow[r] & N \arrow[r] & 0
\end{tikzcd}$$

$$\begin{tikzcd}
F^{n_1} \arrow[r, hook] \arrow[d] & F^{m_1} \arrow[dr] \arrow[d] & & \\
& & M \arrow[r] & 0 \\
F^{n_2} \arrow[r] & F^{m_2} \arrow[ur] & &
\end{tikzcd}$$

November 24, hour 31: The "ring" of modules

November-22-11
10:59 PM

$\frac{1}{2}$T2C2W: $\left[M \text{ f.g.}/R \text{ PID} \Rightarrow M \overbrace{\cong R^k \oplus \bigoplus R/\langle p_i^{s_i}\rangle}^{\text{unique}}\right]$

$\Rightarrow$ structure of f.g. Abelian groups, J.C.F.

Goal: The "ring" of modules.

Recall that $(R\text{-mod}, \oplus)$ is an "Abelian group" (really, an Abelian semi-group, and even this is not precise)

Tensor Products. Given M, N

$$M \otimes_R N := \left\{ \sum_{i=1}^{n} a_i (m_i \otimes n_i) : n \in \mathbb{N},\ a_i \in R \right\} \Big/ \begin{array}{l} (am)\otimes n = a(m\otimes n) = m\otimes(an) \\ (m_1+m_2)\otimes n = \dots \\ m\otimes(n_1+n_2) = \dots \end{array}$$

$$M \times N \xrightarrow{\text{bilinear}} (m_i \otimes n_i)$$

Example. $\dim V \otimes W = (\dim V)(\dim W)$

Example. If $q \in \gcd(a,b)$, $q = sa+tb$, $\frac{R}{\langle a\rangle} \otimes \frac{R}{\langle b\rangle} \cong \frac{R}{\langle q\rangle}$

Pf. $[r_1]_a \otimes [r_2]_b \longrightarrow [r_1 \cdot r_2]_q$ $\qquad [q]\otimes[1] = [sa+tb]\otimes[1] = 0$

$[r]_q \longrightarrow [r]_a \otimes [1]_b$ $\qquad [r_1 r_2]\otimes[1] = [r_1][r_2]$

done line

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

Theorem. $(M,N) \longmapsto M\otimes N$ is a "bifunctor".

Theorem. The universal property.

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

November 29, hours 32-33: Uniqueness

November-24-11
12:08 PM

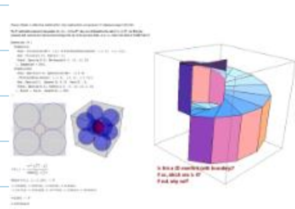
$\frac{1}{2}$ T2C2W: $\left[M \text{ f.g.} / R \text{ PID} \Rightarrow M \cong \overbrace{R^k \oplus \bigoplus R/\langle p_i^{s_i} \rangle}^{\text{unique}} \right]$

$\Rightarrow$ structure of f.g. Abelian groups, J.C.F.

Goal: Uniqueness.

HW4 due, HW5 & last week's schedule on web.

Riddle solutions. ∞, Möbius. Nov24Riddles.png:



Tensor Products. Given M, N

$$M \otimes_R N := \left\{ \sum_{i=1}^{n} a_i (m_i \otimes n_i) : n \in \mathbb{N}, a_i \in R \right\} \Big/ \begin{array}{l} (am)\otimes n = a(m\otimes n) = m \otimes (an) \\ (m_1 + m_2) \otimes n = \dots \\ m \otimes (n_1 + n_2) = \dots \end{array}$$

Example. If $q \in \gcd(a,b)$, $q = sa + tb$, $\quad \frac{R}{\langle a \rangle} \otimes \frac{R}{\langle b \rangle} \cong \frac{R}{\langle q \rangle}$

Proof. $[r_1]_a \otimes [r_2]_b \longrightarrow [r_1 \cdot r_2]_q$ $\quad$ well-def: $[q] \otimes [1] = [sa + tb] \otimes [1] = 0$

$[r]_a \otimes [1]_b \longleftarrow [r]_q$ $\quad$ Inverseness: $[r_1 r_2] \otimes [1] = [r_1][r_2]$

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

Theorem. The universal property.

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

not done

theorem. $(M, N) \longmapsto M \otimes N$ is a "bifunctor".

Example. $\mathbb{Q} \otimes_{\mathbb{Z}} \mathbb{Z}^n \cong \mathbb{Q}^n$ "Extension of Scalars".

a $\mathbb{Q}$-module!

In general, given $\phi: R \to S$ a ring morphism, S is an R module & set $M_S := S \otimes_R M$. Then M_S is an S-module and $R^n_S = S^n$.

Prop. For any domain R there is a unique field $Q(R)$ "the field of fractions"

s.t.
$$\begin{tikzcd} R \arrow[r, "1-1"] \arrow[dr] & Q(R) \arrow[d, dashed, "\exists!"] \\ & F \end{tikzcd}$$

Proof later.

Claim If M is torsion $\left[\forall m\in M\ \exists r\in R\setminus\{0\}\ rm=0\right]$ then $M_{Q(R)}=0$.

Prop If $M\cong R^K\oplus\bigoplus R/\langle p_i^{s_i}\rangle$, then

1. $\dim_{Q(R)} M_{Q(R)}=K$
2. $\dim_{R/\langle p\rangle} M_{R/\langle p\rangle}=K+|\{i: p_i\sim p\}|$
3. $\dim_{R/\langle p\rangle} \operatorname{im}(m\mapsto p^s m)_{R/\langle p\rangle}=K+|\{i: p_i\sim p\ \&\ s<s_i\}|$

not done

as
$$\operatorname{im}(m\mapsto p^s m)\cong\begin{cases} p^sR\cong R & \text{on } R \\ R/\langle q^t\rangle & \text{on } R/\langle q^t\rangle\quad q\not\sim p \\ 0 & \text{on } R/\langle p^t\rangle\quad s\geq t \\ R/\langle p^{t-s}\rangle & \text{on } R/\langle p^t\rangle\quad s<t\end{cases}$$

and
$$\ker(m\mapsto p^s m)\cong\begin{cases} 0 & \text{on } R \\ 0 & \text{on } R/\langle q^t\rangle\quad q\not\sim p \\ R/\langle p^t\rangle & \text{on } R/\langle p^t\rangle\quad s\geq t \\ R/\langle p^s\rangle & \text{on } R/\langle p^t\rangle\quad s<t \end{cases}$$
$R/\langle p^s\rangle\mapsto\ker$ by $[r]_{p^s}\mapsto[p^{t-s}r]_{p^t}$

So such a decomposition is unique!

Localization & Fields of Fractions. Let R be a commutative domain

Def A multiplicative subset S of $R\setminus\{0\}$. (contains 1, closed under $\times$)

Examples $R\setminus\{0\}$, $R\setminus P$ (P prime), Powers of $a\neq 0$.

Definition $S^{-1}R=\left\{\frac{r}{s}\right\}\Big/\frac{r_1}{s_1}\sim\frac{r_2}{s_2}$ if $r_1s_2=r_2s_1$

$\left[\frac{r_1}{s_1}\sim\frac{r_2}{s_2},\ \frac{r_2}{s_2}\sim\frac{r_3}{s_3}\Rightarrow r_1s_2=r_2s_1,\ r_2s_3=r_3s_2\Rightarrow\right.$

$\left.r_1s_2s_3=r_2s_1s_3=s_1r_3s_2\Rightarrow r_1s_3=r_3s_1\right]$

$\frac{r_1}{s_1}+\frac{r_2}{s_2}=\ldots$

$\frac{r_1}{s_1}\cdot\frac{r_2}{s_2}=\ldots$

$R\setminus\{0\}$ — "Field of Fractions $Q(R)$"

$R\setminus P$ — "localization at P"

$R\to S^{-1}R$ is injective

$R \setminus P$ – "localization at P" is injective

$\{2^n\}$ – "dyadic rationals"

done line

Abelian groups & the mult. groups of finite fields

$$A \cong \mathbb{Z}^k \oplus \bigoplus \mathbb{Z}/p_i^{s_i} \cong \mathbb{Z}^k \oplus \mathbb{Z}/a_1 \oplus \mathbb{Z}/a_2 \oplus \cdots$$

$$a_1 \mid a_2 \mid a_3 \cdots$$

Theorem If F is finite, F^* is cyclic.

Proof otherwise, $x^{a_1} - 1$ has too many roots.

(Aside: λ is a root of $f \in F[x] \iff x - \lambda \mid f$, so f may have at most $\deg(f)$ roots)

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

Theorem. $(M,N)\longmapsto M\otimes N$ is a "bifunctor".

Theorem. The universal property.

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

Example. $\mathbb{Q}\otimes_{\mathbb{Z}}\mathbb{Z}^n \cong \mathbb{Q}^n$ ← a $\mathbb{Q}$-module. "Extension of scalars".

In general, given $\phi: R\to S$ a ring morphism, S is an R module & set $M_S := S\otimes_R M$. Then M_S is an S-module and $R^n_S = S^n$.

Prop. For any domain R there is a unique field $Q(R)$ s.t.

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

"The field of fractions"

Proof later.

<u>Claim</u> If M is torsion $\left[\forall m\in M\ \exists r\in R,\ r\neq 0,\ rm=0\right]$ Then $M_{Q(R)}=0$.

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

<u>Prop</u> If $M\cong R^k \oplus \bigoplus R/\langle p_i^{s_i}\rangle$, then

1. $\dim_{Q(R)} M_{Q(R)} = k$
2. $\dim_{R/\langle p\rangle} M_{R/\langle p\rangle} = k + |\{i : p_i \sim p\}|$
3. $\dim_{R/\langle p\rangle} \operatorname{im}(m\mapsto p^s m)_{R/\langle p\rangle} = k + |\{i : p_i\sim p \ \&\ s< s_i\}|$

$$\operatorname{im}(m \mapsto p^s m) \overset{\text{as}}{\cong} \begin{cases} p^s R \cong R & \text{on } R \\ R/\langle q^t \rangle & \text{on } R/\langle q^t \rangle \quad q \nmid p \\ 0 & \text{on } R/\langle p^t \rangle \quad s \geq t \\ R/\langle p^{t-s} \rangle & \text{on } R/\langle p^t \rangle \quad s < t \end{cases}$$

$R/\langle p^{t-s} \rangle \cong \operatorname{im} p^s$ on $R/\langle p^t \rangle$ via

$$r \longmapsto p^s \cdot r$$

$$r \longleftarrow p^s r + p^t r'$$

Localization & Fields of Fractions.

Let R be a commutative domain

<u>Def</u> A multiplicative subset S of $R \setminus \{0\}$. (contains 1, closed under $\times$)

<u>Examples</u> $R \setminus \{0\}$, $R \setminus P$ (P prime), Powers of $a \neq 0$.

<u>Definition</u> $S^{-1}R = \left\{ \frac{r}{s} \right\} \Big/ \frac{r_1}{s_1} \sim \frac{r_2}{s_2}$ if $r_1 s_2 = r_2 s_1$

$\Big[\frac{r_1}{s_1} \sim \frac{r_2}{s_2},\ \frac{r_2}{s_2} \sim \frac{r_3}{s_3} \Rightarrow r_1 s_2 = r_2 s_1,\ r_2 s_3 = r_3 s_2 \Rightarrow$

$r_1 s_2 s_3 = r_2 s_1 s_3 = s_1 r_3 s_2 \Rightarrow r_1 s_3 = r_3 s_1 \Big]$

$\frac{r_1}{s_1} + \frac{r_2}{s_2} = \dots$

$\frac{r_1}{s_1} \cdot \frac{r_2}{s_2} = \dots$

$R \setminus \{0\}$ — "Field of Fractions $Q(R)$"

$R \setminus P$ — "localization at P"

$\{2^n\}$ — "dyadic rationals".

$R \to S^{-1}R$ is injective

Abelian groups & the mult. groups of finite fields

$$A \cong \mathbb{Z}^k \oplus \bigoplus \mathbb{Z}/p_i^{s_i} \cong \mathbb{Z}^k \oplus \mathbb{Z}/a_1 \oplus \mathbb{Z}/a_2 \oplus \dots$$

$$a_1 \mid a_2 \mid a_3 \dots$$

<u>Theorem</u> If F is finite, F^* is cyclic.

<u>Proof</u> otherwise, $x^{a_1} - 1$ has too many roots.

December 1, hour 34: Uniqueness, Corollaries

November-30-11
6:47 PM

Discuss the Final!

Goal. $M = R^k \oplus \bigoplus R/\langle p_i^{s_i} \rangle$. Uniqueness & corollaries.

Reminder. In a PID, $R/\langle a \rangle \otimes R/\langle b \rangle \cong R/\langle \gcd(a,b) \rangle$

Prop If $M \cong R^k \oplus \bigoplus R/\langle p_i^{s_i} \rangle$, then

1. $\dim_{Q(R)} M_{Q(R)} = k$
2. $\dim_{R/\langle p \rangle} M_{R/\langle p \rangle} = k + |\{i : p_i \sim p\}|$
3. $\dim_{R/\langle p \rangle} \operatorname{im}(m \mapsto p^s m)_{R/\langle p \rangle} = k + |\{i : p_i \sim p \;\&\; s < s_i\}|$

as

$$\operatorname{im}(m \mapsto p^s m) \cong \begin{cases} p^s R \cong R & \text{on } R \\ R/\langle q^t \rangle & \text{on } R/\langle q^t \rangle \quad q \not\sim p \\ 0 & \text{on } R/\langle p^t \rangle \quad s \geq t \\ R/\langle p^{t-s} \rangle & \text{on } R/\langle p^t \rangle \quad s < t \end{cases}$$

and

$$\ker(m \mapsto p^s m) \cong \begin{cases} 0 & \text{on } R \\ 0 & \text{on } R/\langle q^t \rangle \quad q \not\sim p \\ R/\langle p^t \rangle & \text{on } R/\langle p^t \rangle \quad s \geq t \\ R/\langle p^s \rangle & \text{on } R/\langle p^t \rangle \quad s < t \end{cases}$$

$R/\langle p^s \rangle \hookrightarrow \ker$ by $[r]_{p^s} \mapsto [p^{t-s} r]_{p^t}$

So such a decomposition is unique! [Though not "canonical"] no do

$F[x]$ and the J.C.F. $T : V \to V$ makes V an $F[x] = R$ module, so $V \cong R^k \oplus \bigoplus R/\langle p_i^{s_i} \rangle$. As $f(T) = 0$ for some f, $k = 0$. If F is alg. closed, $p_i = x - \lambda_i$

Q. What does $F[x]/(x-\lambda)^s$ look like as a vector space?

done line

Basis: $1, x-\lambda, (x-\lambda)^2, \ldots, (x-\lambda)^{s-1}$

$T - \lambda$ acts by "shift to the right" $\begin{pmatrix} 0 & 0 & & \\ 1 & 0 & & \\ 0 & 1 & \ddots & \\ \vdots & & \ddots & \end{pmatrix}$

So T acts by $\begin{pmatrix} \lambda & & \\ 1 & \lambda & \\ & 1 & \lambda \end{pmatrix}$

Corollary 2. *Over an algebraically closed field* $\mathbb{F}$, *every square matrix* A *is conjugate to a block diagonal matrix* $B = \begin{pmatrix} B_1 & 0 & \cdots & 0 \\ 0 & B_2 & \cdots & 0 \\ \vdots & \vdots & \ddots & \vdots \\ 0 & 0 & \cdots & B_n \end{pmatrix}$, *where each* B_i *is either a* 1×1 *matrix* (λ_1) *for some* $\lambda_i \in \mathbb{F}$, *or an* $s_i \times s_i$ *matrix with* λ_i*'s on the diagonals, 1's right below the diagonal, and 0's elsewhere,*

$$\begin{pmatrix} \lambda_i & 0 & \cdots & \cdots & 0 & 0 \\ 1 & \lambda_i & \ddots & & & 0 \\ 0 & \ddots & \ddots & \ddots & & \vdots \\ \vdots & \ddots & \ddots & \ddots & \ddots & \vdots \\ 0 & & \ddots & \ddots & \lambda_i & 0 \\ 0 & 0 & \cdots & 0 & 1 & \lambda_i \end{pmatrix},$$

for some $\lambda_i \in \mathbb{F}$ *and for some* $s_i \geq 2$. *Furthermore,* B *is unique up to a permutation of its blocks* B_i.
(Corollary: good old diagonalization.)

Challenge.
Open all the boxes!

Find an algorithm to find B_j is it the same [at least when all λ_i's are different] as the one you learned in Junior high?

Plan. UFD blunder, JCF abstractly & in practice.

I said "I think in a UFD every prime ideal is maximal"

JCF. V a f.d.v.s, $A: V \to V$ linear, makes V a module over $F[x]$ via $xu = Au$. Then $V \cong \bigoplus F[x]/(x-\lambda_i)^{s_i}$. What's $F[x]/(x-\lambda_i)^{s_i}$?

UFD Blunder. The above statement is nonsense. In $\mathbb{Q}[x,y] = \mathbb{Q}[x][y]$, $\langle x \rangle$ is prime but not maximal.

Basis: $1, x-\lambda, (x-\lambda)^2, \ldots, (x-\lambda)^{s-1}$

$A-\lambda$ acts by "shift to the right" $\begin{pmatrix} 0 & 0 & & \\ 1 & 0 & & \\ 0 & 1 & \ddots & \\ \vdots & & & \end{pmatrix}$

So A acts by $\begin{pmatrix} \lambda & & \\ 1 & \lambda & \\ & 1 & \lambda \end{pmatrix}$

Corollary 2. *Over an algebraically closed field $\mathbb{F}$, every square matrix A is conjugate to a block diagonal matrix* $B = \begin{pmatrix} B_1 & 0 & \cdots & 0 \\ 0 & B_2 & \cdots & 0 \\ \vdots & \vdots & \ddots & \vdots \\ 0 & 0 & \cdots & B_n \end{pmatrix}$, *where each B_i is either a 1×1 matrix (λ_1) for some $\lambda_i \in \mathbb{F}$, or an $s_i \times s_i$ matrix with λ_i's on the diagonals, 1's right below the diagonal, and 0's elsewhere,*

$$\begin{pmatrix} \lambda_i & 0 & \cdots & \cdots & 0 & 0 \\ 1 & \lambda_i & \ddots & & & 0 \\ 0 & \ddots & \ddots & \ddots & & \vdots \\ \vdots & \ddots & \ddots & \ddots & \ddots & \vdots \\ 0 & & \ddots & \ddots & \lambda_i & 0 \\ 0 & 0 & \cdots & 0 & 1 & \lambda_i \end{pmatrix},$$

for some $\lambda_i \in \mathbb{F}$ and for some $s_i \geq 2$. Furthermore, B is unique up to a permutation of its blocks B_i.
(Corollary: good old diagonalization.)

Now lets do that in practice ....

step 1. Find a presentation matrix for $V \in R\text{-mod}$.

w.l.o.g $V = F^n$ and $A \in M_{n\times n}(F)$.

$\ker \pi = \{$

$r_i := x e_i - A e_i \in \ker \pi$

claim $\langle r_i \rangle = \ker \pi$

pf Consider

$$R^n \xrightarrow{xI - A} R^n \xrightarrow{\pi} F^n$$
$$e_i \longrightarrow e_i$$
$$x^k e_i \longrightarrow A^k e_i$$

$$\begin{tikzcd} F^n \arrow[r, "\text{onto?}", "\beta\ \text{v.s. map}"'] \arrow[rrr, bend right, "I"'] & R^n/\langle r_i \rangle \arrow[r, "1-1?", "\alpha\ \text{well-def?}"'] & R^n/\ker\pi \arrow[r, "\sim"] & F^n \end{tikzcd}$$

We want to know if α is $1-1$; it is enough to show that β is onto; i.e., that any $x^k e_i$ can be written, modulo $\langle r_i \rangle$, as a combination of e_i's. Indeed,

$$x^k e_i = x^{k-1}(x e_i) = x^{k-1} A e_i = \dots = A^k e_i$$

Go over handout, first in the distinct-eigval's case:

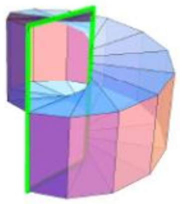
Row and Column Operations

Row operations are performed by left-multiplying N by some properly-positioned 2×2 matrix and at the same time left-multiplying the "tracking matrix" P by the same 2×2 matrix. Column operations are similar, with left replaced by right and P by Q.

```
RowOp[i_, j_, mat_] := Module[{TT = II},
   TT[[{i, j}, {i, j}]] = mat;
   NN = Simplify[TT.NN]; PP = Simplify[TT.PP];
  ];
ColOp[i_, j_, mat_] := Module[{TT = II},
   TT[[{i, j}, {i, j}]] = mat;
   NN = Simplify[NN.TT]; QQ = Simplify[QQ.TT];
  ];
```

Swapping Rows and Columns

```
SwapRows[i_, j_] := RowOp[i, j, {{0, 1}, {1, 0}}];
SwapColumns[i_, j_] := ColOp[i, j, {{0, 1}, {1, 0}}];
SwapBoth[i_, j_] := (SwapRows[i, j]; SwapColumns[i, j];)
```



?

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 divisoir (and a zero!), using invertible row operations. A similar trick works for rows.

```
GCDTrick[{i_, j_}, k_] := Module[{a, b, q, s, t},
   {q, {s, t}} = PolynomialExtendedGCD[a = NN[[i, k]], b = NN[[j, k]], x];
   RowOp[i, j, {{s, t}, {-b/q, a/q}}]
  ];
GCDTrick[k_, {i_, j_}] := Module[{a, b, q, s, t},
   {q, {s, t}} = PolynomialExtendedGCD[a = NN[[k, i]], b = NN[[k, j]], x];
   ColOp[i, j, {{s, -b/q}, {t, a/q}}]
  ];
```

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

```
SplitToSum[i_, j_, a_, b_] := Module[
   {q, s, t, T1, T2},
   {q, {s, t}} = PolynomialExtendedGCD[a, b, x];
   If[q == 1,
    RowOp[i, j, {{s a, 1}, {-t b, 1}}]; ColOp[i, j, {{a, -b}, {t, s}}];
   ]
  ];
```

Recovering C from P?

$$\begin{array}{ccccc}
R^n & \xrightarrow[M]{Ix-A} & R^n & \xrightarrow{\pi_A} & F^n \\
Q\big\uparrow & & \big\downarrow P & & \big\downarrow C \\
R^n & \xrightarrow{Ix-B} & R^n & \xrightarrow{\pi_B} & F^n
\end{array}$$

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

$\Longrightarrow C = \sum B^k P_k$ ... complete run 1

The "Jordan Trick":

Then go through run 2 & run 3 ......

A repeated application of the identity $\begin{pmatrix} p^{k-1} & -1 \\ 1 & 0 \end{pmatrix} \cdot \begin{pmatrix} 1 & 0 \\ 0 & p^k \end{pmatrix} \cdot \begin{pmatrix} 1 & p \\ 0 & 1 \end{pmatrix} = \begin{pmatrix} p^{-1+k} & 0 \\ 1 & p \end{pmatrix}$ will bring a matrix like $\begin{pmatrix} 1 & 0 & 0 & 0 \\ 0 & 1 & 0 & 0 \\ 0 & 0 & 1 & 0 \\ 0 & 0 & 0 & p^4 \end{pmatrix}$ to the "Jordan" form of $\begin{pmatrix} p & 0 & 0 & 0 \\ 1 & p & 0 & 0 \\ 0 & 1 & p & 0 \\ 0 & 0 & 1 & p \end{pmatrix}$, using invertible row and column operations.

```
JordanTrick[i_, j_, p_, s_] := (RowOp[i, j, {{p^(s-1), -1}, {1, 0}}]; ColOp[i, j, {{1, p}, {0, 1}}]);
```

done line

(debt) **Theorem.** The universal property for tensor products

1. Holds
2. Determines $M\otimes N$ up to a unique isomorphism.

$$\begin{array}{ccc}
M\times N & \xrightarrow[\text{bilinear}]{\nu} & M\otimes N \\
& \underset{\text{bilinear}}{\searrow} & \big\downarrow \exists!\, ? \\
& & P
\end{array}$$

December 6 Planning

December-03-11
10:19 AM

Debts.

Polynomials over a UFD make a UFD.

Lang page 180-183 .... mostly a discussion of contents.

Unboxing.

---

1. Fix the UFD blunder
2. Complete the "abstract" JCF story.
3. Do the computational JCF story following the handout.
   a. The presentation matrix.
   b. Reductions. } handout really only does this part.
   c. Reading off the end result.

December 6 Debts

November-30-11
7:50 PM

Abelian groups & the mult. groups of finite fields

$$A \cong \mathbb{Z}^k \oplus \bigoplus \mathbb{Z}/p_i^{s_i} \cong \mathbb{Z}^k \oplus \mathbb{Z}/a_1 \oplus \mathbb{Z}/a_2 \oplus \dots$$

$$a_1 \mid a_2 \mid a_3 \dots$$

<u>Theorem</u> If F is finite, F^* is cyclic.

<u>Proof</u> otherwise, $x^{a_1}-1$ has too many roots.

(Aside: λ is a root of $f \in F[x] \Leftrightarrow x-\lambda \mid f$, so f may have at most $\deg(f)$ roots)

Theorem. The universal property for tensor products.

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

Cayley-Hamilton. Let R be any commutative ring, let $A \in M_{n \times n}(R)$, let $\chi_A(t) = \det(tI - A) \in R[t]$. Then $\chi_A(A) = 0$.

Proof I. Substitute $t = A$, so

$\chi_A(A) = \det(A \cdot I - A) = \det(0) = 0$.

[$\operatorname{tr}(tI-A) = nt - \operatorname{tr} A$
so $nA - (\operatorname{tr} A)I = 0$
so all matrices are diagonal?!]

Proof II. Recall that every matrix B has an "adjoint" B^* s.t. $B^*B = BB^* = \det(B) \cdot I$. Then

$$\underset{\textstyle \sum B_k t^k}{\underset{\shortparallel}{(tI-A)^*}}(tI-A) = \chi_A(t) I$$

as elements of $M_n R[t]$ & even $C_A[t]$, where $C_A = \{B : AB = BA\}$

There is a well-defined $\underbrace{\mathrm{ev}_A}_{\text{multiplicative}} : C_A[t] \to C_A[t]$. Applying to both sides, get

$$\left(\sum B_k A^k\right) \cdot (A - A) = \chi_A(A) I \qquad \square$$

December 6 Scratch

December-03-11
11:04 AM

$$\begin{pmatrix} 1 & 0 \\ 0 & p^2 \end{pmatrix} \sim \begin{pmatrix} p & 0 \\ 1 & p \end{pmatrix}$$

$$\begin{pmatrix} p & 0 \\ 1 & p \end{pmatrix} \to \begin{pmatrix} 1 & p \\ p & 0 \end{pmatrix} \to \begin{pmatrix} 1 & p \\ 0 & -p^2 \end{pmatrix}$$

$$\to \begin{pmatrix} 1 & 0 \\ 0 & p^2 \end{pmatrix}$$

$$\begin{pmatrix} p & 0 \\ 1 & p^{n-1} \end{pmatrix} \to \begin{pmatrix} 0 & -p^n \\ 1 & p^{n-1} \end{pmatrix} \to \begin{pmatrix} 0 & -p^n \\ 1 & 0 \end{pmatrix} \to \begin{pmatrix} 1 & 0 \\ 0 & p^n \end{pmatrix}$$

$$\begin{pmatrix} p^{n-1} & 0 \\ 1 & p \end{pmatrix} \to \begin{pmatrix} p^{n-1} & -p^n \\ 1 & 0 \end{pmatrix} \to \begin{pmatrix} 0 & -p^n \\ 1 & 0 \end{pmatrix} \to \begin{pmatrix} 1 & 0 \\ 0 & +p^n \end{pmatrix}$$

col: $\begin{pmatrix} 1 & 0 \\ 0 & 1 \end{pmatrix} \to \begin{pmatrix} 1 & -p \\ 0 & 1 \end{pmatrix}$

row: $\begin{pmatrix} 1 & 0 \\ 0 & 1 \end{pmatrix} \longrightarrow \begin{pmatrix} 1 & -p^{n-1} \\ 0 & 1 \end{pmatrix} \to \begin{pmatrix} 0 & 1 \\ -1 & +p^{n-1} \end{pmatrix}$

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