14-1100 Sep 8, hours 1-2: Non Commutative Gaussian Elimination

September-11-11 6:11 PM

MAT 1100 Core Algebra.

DROR BAR-NATAN

To do. 1. print "About".
2. print NCGE. (two sides)

on board

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 σ

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.

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

Example $\sigma_1=(123) = 2314$ $\sigma_2=(12)(34) = 2143$, 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 $\sigma_{i,2}$.

---

* Go over the "about" handout.

14-1100 Sep 11, hour 3: Kernels, normal subgroups, quotients

September-08-14 3:53 PM

$$\sigma_{8,j}(\sigma_{4,j_4}M_5) \overset{1}{=} (\sigma_{8,j}\sigma_{4,j_4})M_5 \overset{2}{\subset} M_4M_5$$

$$\overset{3}{=} \sigma_{4,\boxed{j_4'}}(M_5M_5) \overset{4}{\subset} \sigma_{4,j_4'}M_5 \subset M_4$$

on board.

Read Along: Selick's notes 1.1, 1.2.1, 1.4; Lang's book I1-3.

Very quickly: groups, uniqueness of 1, $^{-1}$, $(ab)^{-1} = b^{-1}a^{-1}$
order of an element.

Group homomorphisms, "the category of groups"
The group $\mathrm{Aut}(G)$

Conjugation: $g^h = h^{-1}gh = C_h(g)$ $\quad (g_1g_2)^h = g_1^h g_2^h \quad g^{h_1h_2} = (g^{h_1})^{h_2}$

$h \mapsto C_h$ is an anti-homomorphism $G \longrightarrow \mathrm{Aut}(G)$

Images, kernels, subgroups.

Example: S_3 is an image of S_4, but not a kernel.

Normal subgroups, kernels are normal.

<u>Question</u> Is every normal subgroup the kernel of a homomorphism? Given $N \triangleleft G$, can we find a surjective homomorphism $\phi: G \to H$, with $\ker \phi = N$?

Set Theoretic aside: Surjections are the same as equivalence relations.

(def'n, explanation ...)

done line.

Sol'n Suppose we had ϕ, consider the resulting equiv:

Sol'n Suppose we had ϕ, consider the resulting equiv:

$g_1 \sim g_1 n$ or $g_1 \sim g_2$ iff $g_1^{-1} g_2 \in N$.

Let $H = G/\sim = \{[g]\}$ where $[g] = gN$

with $\phi : G \to H$ being $\phi(g) = [g]$

define $[g_1][g_2] = [g_1 g_2]$ (well defined?)

$[g]^{-1} = [g^{-1}]$

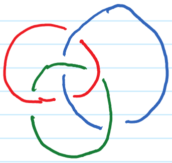
Claim $H = G/\sim$ is a group & ϕ is a morphism whose kernel is N ... we write $H = G/N$.

Theorem (The First Isomorphism Theorem) Given any morphism $\phi : G \to H$, $G/\ker\phi \cong \operatorname{im}\phi$.

14-1100 Sep 15, hours 4-5: quotients, isomorphism theorems

September-11-14 2:45 PM

Riddle Along. Can you draw 4 linked loops, so that if you drop any one of them, the remaining 3 are not linked?



Read Along. Selick 1.1–1.4

Today's menu. Quotients and the isomorphism thms

Reminder: Given $N \triangleleft G$ ($\forall g\in G\ N^g = g^{-1}Ng = N$), we seek $\sim$ on G s.t. $\phi: G \to G/\sim =: H$ will be a group homomorphism with $\ker\phi = N$.

on board

$$g_1\sim g_2 \iff \phi(g_1)=\phi(g_2) \iff \phi(g_1g_2^{-1})=e \iff$$

$$\iff g_1g_2^{-1}\in N \iff g_1\in g_2N \iff g_1N=g_2N$$

Let $H = G/\sim = \{[g]\}$ where $[g]=gN$

with $\phi: G\to H$ being $\phi(g)=[g]$

define $[g_1][g_2]=[g_1g_2]$ (well defined?)

$[g]^{-1}=[g^{-1}]$

Claim $H=G/\sim$ is a group & ϕ is a morphism whose kernel is N ... we write $H=G/N$.

Theorem (The First Isomorphism Theorem) Given any morphism $\phi:G\to H$, $G/\ker\phi \cong \operatorname{im}\phi$.

Pf construct $R: \longrightarrow$ by $[g]\longmapsto \phi(g)$

$L: \longleftarrow$ by $h \longmapsto [g]$ s.t. $\phi(g)=h$.

Aside G/H when $H<G$ & Lagrange's thm.

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

Pf. $\Leftarrow$ $(h_1k_1)(h_2k_2) = h_1h_2'k_2'k_2$

$\Rightarrow$ $(hk)^{-1} = h'k' = k^{-1}h^{-1}$ ....

Definition. $C_G(X) := \{g \in G : \forall x \in X \ \ g^{-1}xg = x\}$

$Z(G) := C_G(G)$

$N_G(X) := \{g \in G : \ g^{-1}Xg = X\}$

all are subgroups

$\Downarrow$

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

Pf. trivial.

The 2nd isomorphism theorem.

If $H < N_G(K)$, then

$$HK/K \simeq H/H\cap K$$

$$\begin{tikzcd}
 & HK \arrow[dl, dash] \arrow[d, dash, "\simeq"] \\
H \arrow[d, dash, "\simeq"'] & K \\
H\cap K \arrow[ur, dash] &
\end{tikzcd}$$

Pf. R: $\rightarrow$: $[h]_K \longrightarrow [h]_{H\cap K}$ L: $\leftarrow$: obvious.

The 3rd Isomorphism Thm.

If $K, H \triangleleft G$ & $K < H$, then $\dfrac{G/K}{H/K} \simeq G/H$

Pf. R: $\rightarrow$: $[[g]_K]_{H/K} \longrightarrow [g]_H$

well defined? $[[g_1]_K]_{H/K} = [[g_2]_K]_{H/K} \Rightarrow$

$\Rightarrow [g_1]_K[g_2]_K^{-1} = [h]_K \Rightarrow g_1g_2^{-1} = hk = h$

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, $[B:A] = [\pi(B):\pi(A)]$)

* $A \triangleleft B \Leftrightarrow \pi(A) \triangleleft \pi(B)$

* $\pi(A \cap B) = \pi(A) \cap \pi(B)$.

Also did: $\operatorname{sign}(\sigma) := \operatorname{sign}\left(\prod_{i<j}(\sigma_i - \sigma_j)\right)$

14-1100 Sep 18, hour 6: Jordan-Holder

September-17-14 2:07 PM

Read Along. Pavel Etingof's "Groups Around Us", Lang's page 57.

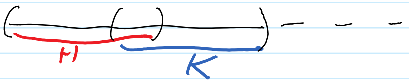
Riddle Along. Your turn!

Today's Menu. Jordan-Hölder.

Reminders.

on board

$\phi: G \to H$:	$H < N_G(K)$:
$G/\ker\phi \cong \operatorname{im}\phi$ $\dim V - \operatorname{nullity} L = \operatorname{rank} L$	$HK/K \cong H/H\cap K$
$\dfrac{G/K}{H/K} \cong G/H$	$G \rhd N$: $\left\{\begin{matrix}\text{subgroups}\\ \text{of } G/N\end{matrix}\right\} \leftrightarrow \{H : N<H<G\}$



Definition A simple group.

"A prime", (in fact, $\mathbb{Z}/n$ is simple iff n is a prime)

yet $S_3 \rhd A_3 = \langle(123)\rangle = \mathbb{Z}_3$; $S_3/A_3 = \mathbb{Z}/2$

$\mathbb{Z}/6 \rhd 2\mathbb{Z}/6 = \{0,2,4\} = \mathbb{Z}/3$; $\mathbb{Z}/6 \big/ 2\mathbb{Z}/6 = \mathbb{Z}/2$

The Jordan-Hölder Theorem. Let G be a finite group. Then there exist a sequence $G = G_0 \rhd G_1 \rhd G_2 \rhd \dots \rhd G_n = \{e\}$ 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.

$4 \to \underset{12}{A_4} \to \underset{3}{A_3}$

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 proper subgroup.

Uniqueness: Use the "diamond principle":

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

$G \rhd G_1 \rhd G_2 - - -$

$G \rhd G_1' \rhd G_2' - - -$

Claim $G = G_1 G_1'$

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

done line

sign: $S_n \to \{\pm 1\}$ by $\text{sign}(\sigma) = (-1)^{\sigma} = \text{sign}\left(\prod_{i<j}(\sigma i - \sigma j)\right)$

$$= \prod_{\{i,j\} \subset \{1, \dots n\}} S_{i,j}(\sigma) \qquad S_{i,j}(\sigma) = \text{sign}\left(\frac{\sigma i - \sigma j}{i - j}\right)$$

$$(-1)^{\sigma\tau} \overset{?}{=} \text{Sign}\left[\prod_{\{i,j\}} \frac{\sigma\tau i - \sigma\tau j}{\tau i - \tau j} \frac{\tau i - \tau j}{i - j}\right] = (-1)^{\sigma}(-1)^{\tau}$$

Every permutation is a product of transpositions, the parity is the parity of the number of transpositions.

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

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

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

Corollary #(Conjugacy classes of S_n) $= P(n)$

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 ... □

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

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

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

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 $\sigma^2 = (132)$ ...

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

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

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

14-1100 Sep 22, hours 7-8: Simplicity of A_n, group actions

September-17-14 2:07 PM

HW1 is out !

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 $\mathbb{N}$?

Today's Menu. Simplicity of A_n, Group actions.

Reminder. $\operatorname{sign}: S_n\to\{\pm1\}$ by $\operatorname{sign}(\sigma)=(-1)^\sigma=\operatorname{sign}\left(\prod_{i<j}(\sigma i-\sigma j)\right)$

$$=\prod_{\{i,j\}\subset\{1,\dots n\}} S_{i,j}(\sigma) \qquad S_{i,j}(\sigma)=\operatorname{sign}\left(\frac{\sigma i-\sigma j}{i-j}\right)$$

$$(-1)^{\sigma\tau}=\operatorname{sign}\left[\prod_{\{i,j\}}\frac{\sigma\tau i-\sigma\tau j}{\tau i-\tau j}\,\frac{\tau i-\tau j}{i-j}\right]=(-1)^\sigma(-1)^\tau$$

Every permutation is a product of transpositions, The parity is the parity of the number of transpositions.

Theorem. A_n is simple for $n\neq4$.

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

Now follow handout....

Jordan-Hölder for S_n: $S_n\rhd A_n\rhd\{e\}$ $(n\geq5)$

Definition A G-set (left-G-set) $G\times X\to X$

s.t. $(g_1g_2)x=g_1(g_2x)$, $ex=x$. Same as $\alpha: G\to S(X)$.

G-sets are a category!

Examples. 0. G itself, under mult. on the left.

1. G itself, under conjugation.

2. Subgroups(G), under conjugation.

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 $\{1 \dots n\}$...

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

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

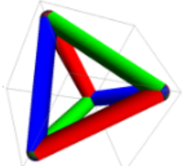
Example. If G is a p-group, the Centre of G is more than $\{e\}$.

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.

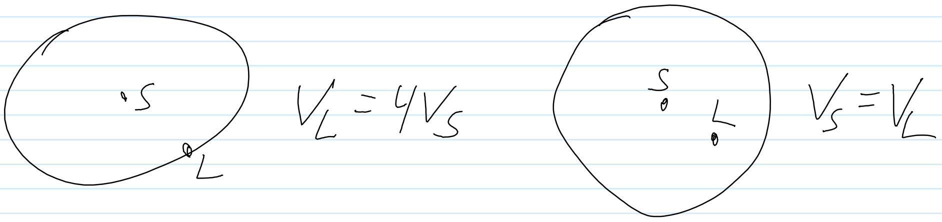
Res. $\sigma=(12)(34)\sigma' \Rightarrow \sigma^{-1}(123)\sigma(123)^{-1}=(13)(24)=\tau \in N$

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

Class photo at end!

HW1 is out V_6

Riddle Along.



Today's Menu. Group actions.

Reminder. $G \circlearrowleft X$, $X \circlearrowright G$, both are categories! G/H

start 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 $|X| \,|\, |G|$)

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

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

The class equation:

$$|G| = \underset{\text{The centre of } G}{|Z(G)|} + \sum_i \underset{\text{the centralizer of } y_i \text{ in } G}{(G : C_G(y_i))}$$

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

Example. If G is a p-group, the centre of G is more than $\{e\}$.

done line

is more than $\{e\}$.

done line

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 1 $\mathrm{Syl}_p(G) \neq \emptyset$.

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:

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

Either both are divisible by p, or neither. Do 2nd 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 $G/\langle x \rangle$. Now use the following claim. □

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 $r = 0$.

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

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

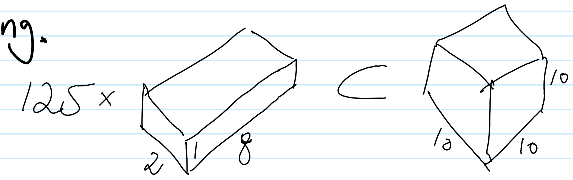
$|G| = p^{\alpha+\beta} m$ w/ maximal α. By counting & binomial nonsense, $p^\alpha \mid |X|$ yet $p^{\alpha+1} \nmid |X|$. G acts on X by translations, so there must be $S_0 \in X$ s.t. $p^{\alpha+1} \nmid |G \cdot S_0|$, hence $p^\beta \mid |H = \text{stab}_G(S_0)|$. Yet if $x \in S_0$ then $g \mapsto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

14-1100 Sep 29, hours 10-11: The Sylow theorems

September-27-14 1:18 PM

class photo on web!

Riddle Along.



Today's Menu. Sylow 1 2 3, some classification.

Reminders.

$$G \circlearrowright X \Rightarrow |X| = \sum_i \frac{|G|}{|\mathrm{Stab}_X(x_i)|}$$

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

G a p-group $\Rightarrow Z(G)$ non-trivial

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 1 $\mathrm{Syl}_p(G) \neq \emptyset$.

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:

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

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

$|G| = |Z(G)| + \sum_i (G : C_G(y_i))$ } or [illegible]. Do 2nd 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 $G/\langle x \rangle$. Now use the following claim. $\square$

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 $r = 0$.

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

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

$|G| = p^{\alpha+\beta} m$ w/ maximal α. By counting & binomial nonsense, $p^\alpha \mid |X|$ 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 $p^{\beta} \mid |H = \mathrm{stab}_G(S_0)|$. 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 $|H| = p^{\beta}$.

Theorem. 1. Sylow p-groups always exist; $\mathrm{Syl}_p(G) \neq \emptyset$.

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

3. All Sylow-p subgroups of G are conjugate, and $n_p(G) := |\mathrm{Syl}_p(G)| = 1 \bmod p$ & $n_p(G) \mid |G|$

Groups of order 15.

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

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

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

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

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

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

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

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

In fact, 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

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

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

done line (but only 15 & 21, not general $p \cdot q$)

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

Debt. What does this mean?

Aside. $\mathrm{Aut}(\mathbb{Z}/p)$ is cyclic;

$\mathrm{Aut}(\mathbb{Z}/7) = \langle x \mapsto x^3 \rangle$

1 3 2 6 4 5

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

14-1100 Oct 2, hour 12: The Sylow theorems, II

September-27-14 1:18 PM

Riddle Along. Your turn again!

Today's Menu. G_{pq}, proofs of Sylow 2-3.

Reminders. 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

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

Groups of order 15. $P_3\triangleleft G$, $P_5\triangleleft G$, $G=P_3\times P_5=\mathbb{Z}/3\times\mathbb{Z}/5=\mathbb{Z}/15$

Groups of order 21. $P_7\triangleleft G$, P_3 may not be normal

If normal, $G=P_3\times P_7=\mathbb{Z}/21$.

Otherwise, $P_7=\langle x\rangle$, $P_3=\langle y\rangle$, we have $x^y=x$, or x^2, or x^4.

Defn. What does this mean?

Aside. $\underset{(\mathbb{Z}/p)^*}{\underset{\shortparallel}{\mathrm{Aut}}}(\mathbb{Z}/p)$ is cyclic;

$\mathrm{Aut}(\mathbb{Z}/7)=\langle x\mapsto x^3\rangle$

skip

Groups of order pq. $n_p \mid pq \Rightarrow n_p \mid q$, (or $n_p=1$)

$n_p=1 \mod p \Rightarrow q=1 \mod p \Rightarrow p \mid q-1$

If $p<q$, $p\nmid q-1 \Rightarrow G=\mathbb{Z}/pq$

if $p \mid q-1$, small may act on big....

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

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.

done line

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. $H < N_G(P')$.

14-1100 Oct 6, hours 13-14: Finish Sylow, examples, semi-direct products

September-27-14 1:18 PM

HW1 due!

Riddle Along. $\boxed{\begin{array}{c}\forall \alpha\in\mathbb{R}\ \exists a_i\in\mathbb{Q}\\ \text{s.t. } a_i\to\alpha\end{array}}$ $\boxed{\mathbb{Q}\cap[-\infty,\alpha]}$ So what?

Today's Menu. Finish Sylow, semi-direct products

Reminders. **Theorem.** 1. Sylow p-groups always exist; $\mathrm{Syl}_p(G)\neq\emptyset$.

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

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

$n_p(G) := |\mathrm{Syl}_p(G)| = 1 \bmod p$ & $n_p(G) \mid |G|$

The extension trick: Can't extend a Sylow by something of order p.

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

Proposition. If H is a p-subgroup & $P\in\mathrm{Syl}_p(G)$, 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.

Example: $\langle(123)\rangle, \langle(345)\rangle \subset S_5$

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 maybe not.

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

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

$$n_1h_1n_2h_2 = n_1h_1n_2h_1^{-1}h_1h_2 = n_1\phi_{h_1}(n_2)\,h_1h_2$$
$$(nh)^{-1} = h^{-1}n^{-1} = h^{-1}n^{-1}hh^{-1} = \phi_{h^{-1}}(n^{-1})\cdot h^{-1}$$

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

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

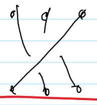
2. $H < N\rtimes H$, $N \triangleleft (N\rtimes H)$ and $N\rtimes H/N \cong H$.

Small Examples. 1. $D_{2n} = \mathbb{Z}/n \rtimes \{\pm1\}$

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

I should have started the discussion of PB_n w/ an intro to free groups and w/ $\pi_1(\textcircled{\scriptsize xxx}) = F_n$

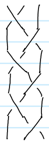
done line

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

an aside on free groups, generators & relations.

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

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



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

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

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

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 $\underbrace{x^2 \text{ or } x^4}_{\text{isomorphic}}$

(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 $\mathbb{Z}/4\times\mathbb{Z}/3 = \mathbb{Z}/12$ $(\mathrm{Aut}(\mathbb{Z}/4) = \mathbb{Z}/2!)$

$(\mathbb{Z}/2\times\mathbb{Z}/2)\rtimes\mathbb{Z}/3$: 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

$\langle (234) \rangle$

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 $\mathbb{Z}/3 \rtimes \mathbb{Z}/4$

Scratch 141005

October-05-14 8:10 PM

$(12)\cdot(123)$ $9 \nmid 120$

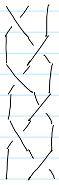
$(123)(345)$

$(12)(234)$ $6 / 24$

14-1100 Oct 9, hour 15: Finish semi-direct products, groups of order 12

September-27-14 1:18 PM

HW2 discussion. I should have added to HW2: $G \rtimes G \cong G \times G$ conj. action

Aside. 

Two reasons why I like this one:
1. knotted \$20's
2. Borromean.
3. It is a commutator.

Q. Can you find a 4-component Brunnian link?

Today's Menu. semi-direct products, groups of order 12✓

Reminders. Given $N, H, \phi: H \to \mathrm{Aut}(N)$,

$$N \rtimes H := \{nh\};\quad n_1h_1 \cdot n_2h_2 = n_1\phi_{h_1}(n_2)h_1h_2$$

Thm 1. $N \rtimes H$ is a group, $H < N \rtimes H$, $N \triangleleft N \rtimes H$,

$N \cap H = \{e\}$ $\quad (N \rtimes H / N = H)$

2. In general, if $G = NH$, $N \triangleleft G$, $H < G$, $N \cap H = \{e\}$,

Then $G \cong N \rtimes_\phi H$ w/ $\phi_h(n) = hnh^{-1}$

$PB_n := \pi_1(\mathbb{C}^n \setminus \text{diags}) =$ "Pure braids on n strands"

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

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

Aside.

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

an aside on free groups, generators & relations.

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

$\mathrm{Aut}(\mathbb{Z}/7) = \mathbb{Z}/6 = \langle \phi \rangle$; $\phi(x) = x^3$; $\quad y \mapsto \phi^0$ or ϕ^2 or ϕ^4

$$yxy^{-1} = \underbrace{x}_{\mathbb{Z}/21} \text{ or } \underbrace{x^2 \text{ or } x^4}_{\text{isomorphic}}$$

iso: if $yxy^{-1} = x^2$ & then $y^2xy^{-2} = x^4$, so

$$G_2 = \langle x \rangle \rtimes_{\phi^2} \langle y \rangle \longrightarrow \langle \bar{x} \rangle \rtimes_{\phi^4} \langle \bar{y} \rangle = G_4$$

$$\begin{pmatrix} x \\ y^2 \end{pmatrix} \begin{pmatrix} y \end{pmatrix} \longmapsto \begin{pmatrix} \bar{x} \\ \bar{y} \end{pmatrix} \begin{pmatrix} \bar{y}^2 \end{pmatrix}$$

is iso.

skipped

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 $\mathbb{Z}/4 \times \mathbb{Z}/3 = \overset{\text{done}}{\mathbb{Z}/12}$ ✓ $(\mathrm{Aut}(\mathbb{Z}/4) = \mathbb{Z}/2!)$

$(\mathbb{Z}/2 \times \mathbb{Z}/2) \rtimes \mathbb{Z}/3$: Either direct; $\mathbb{Z}/2 \times \mathbb{Z}/6$ done

or the fun action of $\mathbb{Z}_3$ on $(\mathbb{Z}/2)^2$, giving A_4 skipped

$\langle (234) \rangle$

e
$(12)(34)$
$(13)(24)$
$(14)(23)$

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

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

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.

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

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

14-1100 Oct 16, hour 16: G12, G21, Solvable groups

October-10-14 1:09 PM

Further return HW1

HW2 due!

TT next class, Mon. oct 20 1:10 – 3PM here

Material: Everything on groups. See oldies.

Final exam: Mondy Dec 8 Top; Wed Dec 10 Analysis; Thu Dec 11 PDE

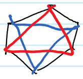
Algebra: Fri Dec 12 or Mon Dec 15? Time?

Groups of order 12. $P_4 = \mathbb{Z}/4$ or $(\mathbb{Z}/2)^2$, $P_3 = \mathbb{Z}/3$, at least one of those is normal, so:

on board

$G = \mathbb{Z}/3 \rtimes \mathbb{Z}/4$: $\mathrm{Aut}(\mathbb{Z}/3) = \mathbb{Z}/2$ so

$\mathbb{Z}/12$ or no-name $\mathbb{Z}/3 \rtimes_{\text{parity}} \mathbb{Z}/4$

$G = \mathbb{Z}/3 \rtimes (\mathbb{Z}/2 \times \mathbb{Z}/2)$: $\mathbb{Z}/6 \times \mathbb{Z}/2$ or $S_3 \times \mathbb{Z}/2 = D_{12}$ 

$G = \mathbb{Z}/4 \rtimes \mathbb{Z}/3$ $\mathrm{Aut}(\mathbb{Z}/4) = \mathbb{Z}/2 \Rightarrow$ $\mathbb{Z}/12$

$G = (\mathbb{Z}/2 \times \mathbb{Z}2) \rtimes \mathbb{Z}/3$ $\mathrm{Aut}(\mathbb{Z}/2 \times \mathbb{Z}/2) = S_3 \Rightarrow$

(direct) $\mathbb{Z}/6 \times \mathbb{Z}/2$

or the fun action of $\underset{\langle(234)\rangle}{\mathbb{Z}_3}$ on $(\mathbb{Z}/2)^2$, giving A_4

e
$(12)(34)$
$(13)(24)$
$(14)(23)$

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

$\mathrm{Aut}(\mathbb{Z}/7) = \mathbb{Z}/6 = \langle \nu \rangle$; $\nu(x) = x^3$; $y \overset{\phi_0}{\mapsto} \nu^0$ or $\overset{\phi_2}{\nu^2}$ or $\overset{\phi_4}{\nu^4}$

$$yxy^{-1} = \underbrace{x}_{\mathbb{Z}/21} \text{ or } \underbrace{x^2 \text{ or } x^4}_{\text{isomorphic}}$$

Exercise: $\phi : H \to \mathrm{Aut}(N)$; $\eta \in \mathrm{Aut}\,H$, $\nu \in \mathrm{Aut}(N)$

$\phi\eta : H \to \mathrm{Aut}(N)$ $(\phi^\nu)_h = \nu^{-1} \circ \phi_h \circ \nu$

$\phi^\nu \in \mathrm{Hom}(H, \mathrm{Aut}(N))$

Then $N \rtimes_\phi H \simeq N \rtimes_{\phi\eta} H \simeq N \rtimes_{\phi^\nu} H$.

In our case $\phi_4 = \phi_2 \circ \eta$ where $\eta : \mathbb{Z}/3 \to \mathbb{Z}/3$

In our case $\phi_4 = \phi_2 \circ \eta$ where $\eta : \mathbb{Z}/3 \to \mathbb{Z}/3$ is multiplication by 2.

done line

Solvable Groups.

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

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

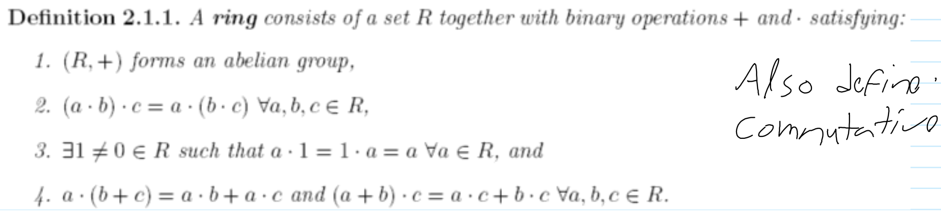
2. If $H < G$ and G is solvable, so is H.

$A \triangleleft B$ $\quad H \cap A \triangleleft H \cap B$? ✓ $\quad \frac{H \cap B}{H \cap A} \longrightarrow B/A$ 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 $\cdot$ 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. $\mathbb{Z}$, $R[x]$, $M_{n \times n}(R)$

Morpisms, (Examples: 1. $\mathbb{Z} \longrightarrow \mathbb{Z}/n$ 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. $M_{n \times n}(R[x]) \simeq M_{n \times n}(R)[x]$)

im, subring, ker, ideal.

Q. Is every ideal a quotient.

Ans. Define R/I.

Good luck w/ term test!

14-1100 Oct 20, hours 17-18: Term Test

October-22-14 4:06 PM

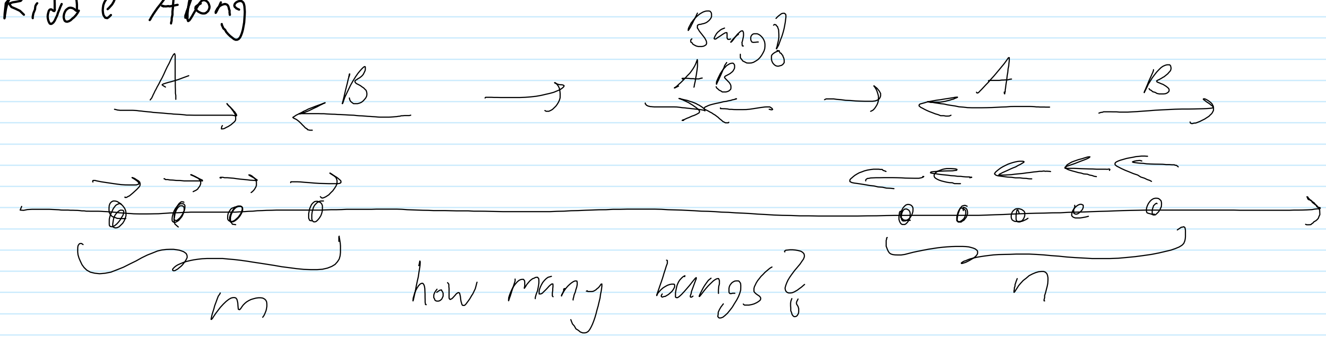
14-1100 Oct 23, hour 19: Solvable groups, rings

October-10-14 1:09 PM

Return TT, etc.

HW3 on web, more may be added next week.

Riddle Along



how many bangs?

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

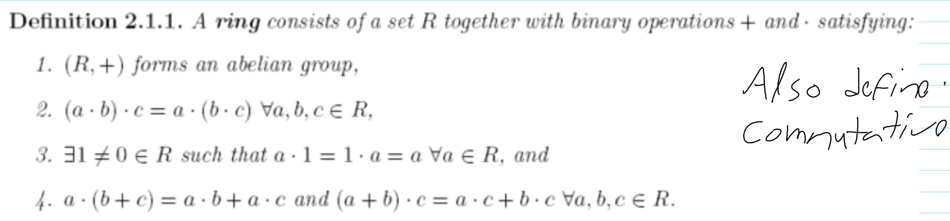
Thm 1. If $N \triangleleft G$, G is solvable iff N & G/N are.

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

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

Cor. If a group contains A_n $n \geq 5$, it is not solvable.

Rings.



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

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)

done line

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

6. If $\varphi : G \to H$, $\varphi_* : RG \to RH$)

Cayley-Hamilton A matrix annihilates its characteristic poly:

Let $A \in M_{n\times n}(R)$, R commutative. Set

$\chi_A(t) = \det(tI - A)$. Then $\chi_A(A) = 0$

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

Nonesense! Would have worked for trace just as well! $\chi_A^{tr} = tr(tI - A) = nt - tr(A)$

So $A = \frac{trA}{n} I$

The issue:

$$\begin{tikzcd}
M_{n\times n}(R)[t] \arrow[r, "\det"] \arrow[d, "ev_A"] & R[t] \arrow[d, "ev_A"] \\
M_{n\times n}(R) \arrow[r, "?"] & M_{n\times n}(R)
\end{tikzcd}$$

Right proof.

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

now substitute $t=A$. The B_i's commute with A because $(tI-A)\,adj(tI-A) = adj(tI-A)(tI-A)$.

---

im, subring, ker, ideal.

Q. Is every ideal a quotient.

Ans. Define R/I.

14-1100 Oct 27, hours 20-21: Rings, Cayley-Hamilton, quotients and isomorphism theorems

October-10-14 1:09 PM

HW3 2 questions added!

Riddle Along $\boxed{1}\ \boxed{2}\ \boxed{3}\ \boxed{4}\ \boxed{5}\ \boxed{6}\ \boxed{7}\ \boxed{8}\ \boxed{9}$

Two players alternate drawing cards from the above deck. The first player to have 3 cards that add up to 15, wins. Would you like to be the first to move or the second?

Reminders 1. Rings: $(R, +, \times, 0\neq 1)$

2. $R[x]$, $M_{n\times n}(R)$, RG

3. Morphisms (Make rings a "category") $\boxed{F(1)=1}$

Further examples.

1. If $\varphi: G\to H$, $\varphi_*: RG\to RH$

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

Cayley-Hamilton A matrix annihilates its characteristic poly: Let $A\in M_{n\times n}(R)$, R commutative. Set

$\chi_A(t) = \det(tI-A)$. Then $\chi_A(A)=0$

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

Nonsense! Would have worked for trace just as well! $\chi_A^{tr} = tr(tI-A) = nt - tr(A)$ So $A = \frac{trA}{n} I$

The issue:

$$\begin{tikzcd} M_{n\times n}(R)[t] \arrow[r, "\det"] \arrow[d, "ev_A"] & R[t] \arrow[d, "ev_A"] \\ M_{n\times n}(R) \arrow[r, "?"] & M_{n\times n}(R) \end{tikzcd}$$

not mentioned.

Right proof.

in $M_{n\times n}(R[t])$ in $M_{n\times n}(R)[t]$

$\det(tI-A)\cdot I = adj(tI-A)(tI-A) = (\sum B_i t^i)(tI-A)$ in

see 2015-12

now substitute $t=A$. The B_i's commute with A because $(tI-A)\,adj(tI-A) = adj(tI-A)(tI-A)$.

im, subring, ker, ideal. (ideals are subrings but never proper subrings)

Q. Is every proper ideal a Kernel?

Ans. Define R/I.

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

The Isomorphism Theorems. 1. $\varphi: R \to S \Rightarrow R/\ker\varphi = \operatorname{im}\varphi$.

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

done line

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

From This point, our goal is "modules over PID"

Better Rings. 1. The ultimate:

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

("division ring", if not commutative

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

useful for 3D rotations, etc...)

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

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 $\Longleftrightarrow R/I$ 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. $S=\ell^\infty=\{\text{bndd seq's in } \mathbb{R}\}$ $A_n=\{(a_i): a_n=0\}$

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

Proof using Zorn's Lemma.

Theorem There exists a function

$\mathrm{Lim} : \left\{ \substack{\text{bndd seq's} \\ \text{in } \mathbb{R}} \right\} \to \mathbb{R}$ 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. $S = \{\text{bndd seq's in } \mathbb{R}\}$ $I = \{(a_n) : \substack{a_n \neq 0 \text{ for} \\ \text{finitely many } n\text{'s}}\}$

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. $\Rightarrow$ $ab \in P \Rightarrow [ab] = 0 \Rightarrow [a][b] = 0 \Rightarrow \begin{matrix} [a] = 0 \Rightarrow a \in P \\ \text{or} \\ [b] = 0 \Rightarrow b \in P. \end{matrix}$

$\Leftarrow$ $[a][b] = 0 \Rightarrow [ab] = 0 \Rightarrow ab \in P \Rightarrow \begin{matrix} a \in P \Rightarrow [a] = 0 \\ \text{or} \\ b \in P \Rightarrow [b] = 0 \end{matrix}$

Theorem. A maximal ideal is prime.

target line

From this point on, R is a commutative integral domain.

Primes. 1. $a|b$ $[a \neq 0, \exists q \text{ s.t. } aq = b]$ $(a|b \wedge b|a \Rightarrow a = ub)$ "a, b are associates"

2. $\gcd(a,b) = q$; $\gcd = q$ & $\gcd = q' \Rightarrow q' = uq$.
3. Primes: $p \neq 0$ non-unit $p | ab \Rightarrow p|a$ 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 $2 | (1-\sqrt{-5})(1+\sqrt{-5}) = 6$

UFDs. Def. Evry 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 $\Leftrightarrow$ ever $x \neq 0$ has a unique decomposition into irreducibles.

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

Thm. In a UFD gcd's always exist.

14-1100 Oct 30, hour 22: The isomorphism theorems for rings, "better rings"

October-10-14 1:09 PM

Reminders Ideal: $0\in I$, $I+I\subset I$, $-I\subset I$, $RI\subset I$, $IR\subset R$

R/I, Iso 1: Given $\varphi: R\to S$, $R/\ker\varphi \cong \operatorname{im}\varphi$

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

From this point, our goal is "modules over PID"

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 $\Longleftrightarrow$ 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. $S=\ell^\infty=\{\text{bndd seq's in }\mathbb{R}\}$ $A_n=\{(a_i): a_n=0\}$

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

Proof using Zorn's Lemma.

Example. $S=\{\text{bndd seq's in }\mathbb{R}\}$ $I=\{(a_n): a_n\to 0\}$ [$a_n=0$ a.e. is enough]

J - a maximal ideal containing I.

$\operatorname{Lim}: S\to S/J \underset{?}{=} \mathbb{R}$ [$\mathbb{R}\to S/J$ is obvious;

$\mathrm{Lim}: S \longrightarrow S/J \underset{!}{=} \mathbb{R}$ [$\mathbb{R} \longrightarrow S/J$ is obvious; the other direction is not]

Theorem Lim satisfies:

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.... $\square$.

done line

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 on, R is a commutative integral domain

target line

Primes. 1. $a|b$ $[a \neq 0, \exists q \text{ s.t. } aq=b]$ $(a|b \wedge b|a \Rightarrow a=ub)$ "a, b are associates"

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

3. Primes: $p \neq 0$ non-unit $p|ab \Rightarrow p|a$ 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 $2|(1-\sqrt{-5})(1+\sqrt{-5})=6$

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 $\Leftrightarrow$ ever $x \neq 0$ has a unique decomposition

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

Thm. In a UFD gcd's always exist.

14-1100 Nov 3, hours 23-24: "better rings", Euc -> PID -> UFD

October-10-14 1:09 PM

(141102) Assaf's riddle: ~~k~~ 5 kids share a loot of ~~n~~ 50 in-wrapping halloween candies. The first kid proposes a way to split the loot; if it is not accepted by a strict majority (her included), she~~'s left out~~ goes home and the second proposes a split, etc. How is the loot split?

Global goal: IT3CSW: M f.g. module over a PID $R \Rightarrow$ Uniquely

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

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"

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

Reminders R/I a field $\Leftrightarrow I$ is maximal.

R/I a domain $(ab=0 \Rightarrow (a=0)\vee(b=0))$ $\Leftrightarrow$ I is prime.

start line

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 on, R is a commutative integral domain.

Divisibility & Primes. 1. $a|b$ $[a\neq 0, \exists q \text{ s.t. } aq=b]$ $(a|b \wedge b|a \Rightarrow a=ub)$ "a, b are associates"

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

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

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

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

Claim. prime $\Rightarrow$ irreducible

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

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

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.

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 irrd & $x \mid ab$, 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.

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 $\dfrac{a = x^3 - 2x^2 - 5x + 12}{b = x^2 + 1}$

$\left.\begin{array}{l} \dots\ r = -6x + 14 \\ a(i) = 14 - 6i \end{array}\right\}$ 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, $I \subset J = \langle x \rangle \subset R \Rightarrow p = ax \Rightarrow$
$(a \in R^* \Rightarrow I = J) \vee (x \in R^* \Rightarrow J = R)$

done line

theorem. PID $\Rightarrow$ UFD.

Weak 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 $x_2 \in R^*$ $x_2 \in \langle x_3 \rangle \subset M_2$ maximal $M_2 = \langle p_2 \rangle$, $x_2 = p_2 x_3, \dots$ if process was infinite,

$M_2 = \langle P_2 \rangle$, $x_2 = P_2 x_3$, ... if process was infinite,

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

$\langle x_n \rangle \subset \langle x_{n+1} \rangle$ 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 $x = x_1 = P_1 x_2 = P_1 P_2 x_3 = \dots = P_1 P_2 \dots P_n u$

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

target line

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.

14-1100 Nov 6, hour 25: Finish rings, start modules

November-06-14 9:10 AM

HW. HW3 due, HW4 on web

Riddle along: A game: Player A writes the numbers 1-18 on the faces of three blank dice, to her liking. Player B takes one of the 3 dice. Player B takes one of the remaining two, and throws away the third. Player A and B then play 1,000 rounds of "dice war" with the dice they hold. Whom would you rather be, player A or player B?

Global goal: IT3C4W M f.g. module over a PID $R \Rightarrow$ Uniquely

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

Cor1. A f.g Abelian $\Rightarrow A \cong \mathbb{Z}^k \oplus \bigoplus \mathbb{Z}/p_i^{s_i}$

Cor2. $A \in M_{n\times n}(\mathbb{C})$ has a "Jordan form"

Today. Finish rings, start modules.

Reminders. Euc $\Rightarrow$ PID $\underset{6}{\not\Rightarrow}$ UFD

theorem. PID $\Rightarrow$ UFD.

Weak 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 $x_2 \in R^*$ $x_2 \in \langle x_3 \rangle \subset M_2$ maximal $M_2 = \langle p_2 \rangle$, $x_2 = p_2 x_3$, ... if process was infinite,

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

$\langle x_n \rangle \subset \langle x_{n+1} \rangle$ 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 $x = x_1 = p_1 x_2 = p_1 p_2 x_3 = \cdots = p_1 p_2 \cdots p_n u$

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.

skipped.

target line

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

done line

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

3. $A \subset B \subset M \Rightarrow {}^{M/A}\!/_{B/A} \cong M/B$

4. Also dull.

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

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

sum

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

product

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

differ for infinite families!

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

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

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

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

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

Debt

November-06-14 4:07 PM

The inclusions

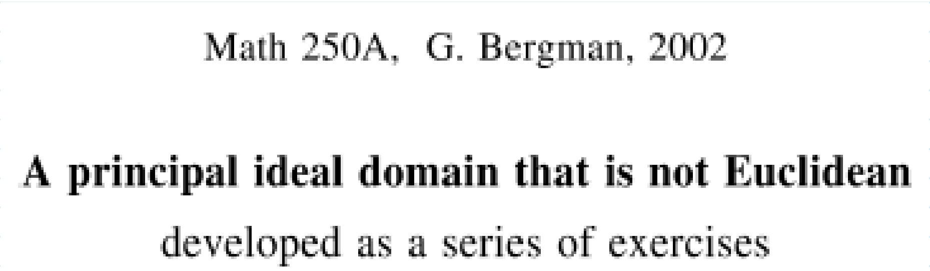
$$\text{UFD} \overset{1}{\supsetneq} \text{PID} \overset{2}{\supsetneq} \text{Euc}$$

are strict.

1. Many examples; especially polynomial rings in several variables and $\mathbb{Z}[x]$. (In general, R UFD $\Rightarrow$ $R[x]$ UFD).

2. Examples are hard. The easyest seems to be $\mathbb{Z}\left[\frac{1+\sqrt{-19}}{2}\right]$.

   A sequence of exercises leading to a proof is in eprints/Bergman:



Math 250A, G. Bergman, 2002

A principal ideal domain that is not Euclidean

developed as a series of exercises

14-1100 Nov 10, hours 26-27: Modules, Main Theorem - Existence

November-09-14 10:27 AM

Office Hour this week Wed $1^{30} - 2^{30}$ (not at 2^{30})

Global goal: IT3C4W: 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"

Today. Further dull technicalities, then proof of existence side of Thm.

Euc $\Rightarrow$ PID $\Rightarrow$ UFD.
Many UFD's are not PID's.

$\mathbb{Z}\left[\frac{1+\sqrt{-19}}{2}\right]$ is a PID but is not Euclidean.

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.

Reminder. Modules.

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. $A, B \subset M \Rightarrow \frac{A+B}{B} \cong \frac{A}{A\cap B}$

3 $A \subset B \subset M \Rightarrow {}^{M}\!/\!_{A} \big/ {}^{B}\!/\!_{A} \cong M/B$

4. Also dull.

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

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

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

differ for infinite families!

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

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

(!)

PM. I should have done $l = \operatorname{lcm}$
$\frac{R}{\langle a\rangle} \oplus \frac{R}{\langle b\rangle} \cong \frac{R}{\langle g\rangle} \oplus \frac{R}{\langle l\rangle}$ $g = \gcd$

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

$$\frac{R}{\langle a\rangle} \oplus \frac{R}{\langle b\rangle} \cong \frac{R}{\langle ab\rangle} \quad \text{via} \quad \begin{pmatrix} tb & sa \end{pmatrix} \quad \begin{pmatrix} 1 \\ 1 \end{pmatrix}$$

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

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

"the chinese remainder Theorem"

P.M. I should have done $l = \mathrm{lcm}$, $g = \gcd$

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

in a way compatible w/

$$\frac{R}{\langle ab\rangle} \longrightarrow \frac{R}{\langle a\rangle} \oplus \frac{R}{\langle b\rangle} \text{ by } \begin{pmatrix} 1 \\ 1 \end{pmatrix}$$

in the case of $\gcd = 1$.

Let R be a PID...

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

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

So we're back to Gaussian elimination!

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

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

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

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

P.M. I should have gone

1. $M_{n\times m} \longrightarrow$ modules w/ n gens & m rels.

2. $M_{n\times X} \longrightarrow$ f.g. modules

3. The above is surjective.

Examples. (1), (a), (0)

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

done line

Comment. May add/remove 0 columns.

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

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 $[\alpha]_{\operatorname{im} A} \longrightarrow [P\alpha]_{\operatorname{im} A'}$

P can be interpreted as $g\times g$ matrix

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

.... Can do arbitrary, invertible row operations on A,

and arbitrary invertible column ops, provided each column is touched finitely many times.

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; wlog, that entry is a_{11}.

<u>Claim</u> a_{11} divides all other entries in its row & column.

<u>pf 1</u> For a Euclidean domain.

<u>pf 2</u> In a PID, if $q = \gcd(a,b) = sa+tb$, then

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

$\Longrightarrow$ 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 $A \sim \left(\begin{array}{cc|c} a_{11} & & \\ & a_{22} & 0 \\ \hline & 0 & 0 \end{array}\right)$ $\begin{pmatrix} \text{w.l.o.g., } A \\ \text{is square} \end{pmatrix}$

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

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

14-1100 Nov 13, hour 28: Main Theorem - Existence

November-12-14 12:53 PM

Goal: M f.g. / PID $R \Longrightarrow$

$$M = R^k \oplus \bigoplus_{i=1}^{n} R/\langle p_i^{s_i}\rangle \qquad p_i \text{ prime} \quad s_i \in \mathbb{Z}_{>0}$$

There is a map from $n\times m$ matrices to f.g. modules:

$$A \longmapsto R^n \xrightarrow{A} R^n \longrightarrow R^n/\operatorname{im}A =: M_A$$

Equally well, $n\times X$ matrices to f.g. modules:

$$A \longmapsto R^X \xrightarrow{A} R^n \longrightarrow R^n/\operatorname{im}A =: M_A$$

$M_{n\times X}(R) \longrightarrow$ f.g. modules is surjective.

Examples. (1), (a), (0)

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

Comment. May add/remove 0 columns.

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

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 $[\alpha]_{\operatorname{im}A} \longrightarrow [P\alpha]_{\operatorname{im}A'}$

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; wlog, that entry is a_{11}.

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

pf1 for a Euclidean domain.

pf2 In a PID, if $q = \gcd(a,b) = sa+tb$, then

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

$\Longrightarrow$ 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 $A \sim \left(\begin{array}{c|c} a_{11} \ \ a_{22} & 0 \\ \hline 0 & 0 \end{array}\right)$ (w.l.o.g., A is square)

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

$a_1 | a_2 | \dots | a_n$

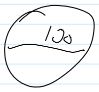
14-1100 Nov 20, hour 29: The JCF

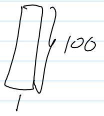
November-15-14 5:54 PM

Plan. JCF abstractly & in practice.

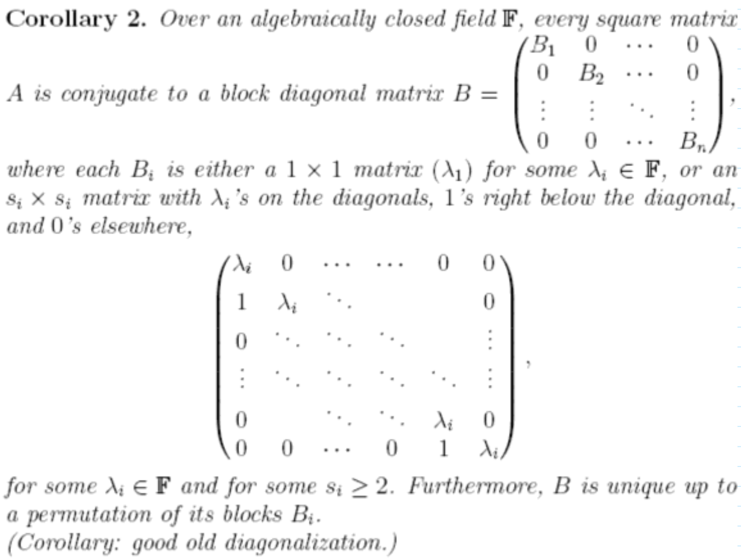
HW4 due, HW5 on web.

Riddle. 1. A spherical loaf of bread goes into a bread cutting machine which slice has the most crust?

2. Can you cover 

with 99 × 

?



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.)

on projector screen

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

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

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 $A \in M_{n \times n}(F)$. $\ker \pi = ?$

$r_i = xe_i - Ae_i \in \ker \pi$

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

pf Consider

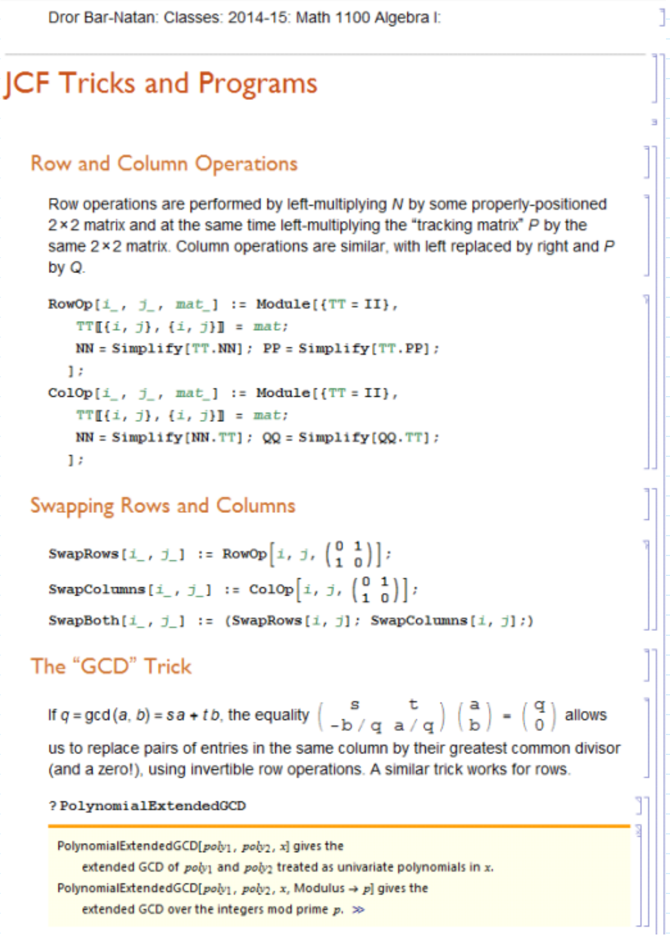
$$\begin{tikzcd} R^n \arrow[r, "xI-A"] & R^n \arrow[r, "\pi"] & F^n \\ & e_i \arrow[r] & e_i \\ & x^k e_i \arrow[r] & A^k e_i \end{tikzcd}$$

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

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_j's. Indeed,

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

Go over handout along with "run 1"



Dror Bar-Natan: Classes: 2014-15: Math 1100 Algebra I:

JCF Tricks and Programs

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

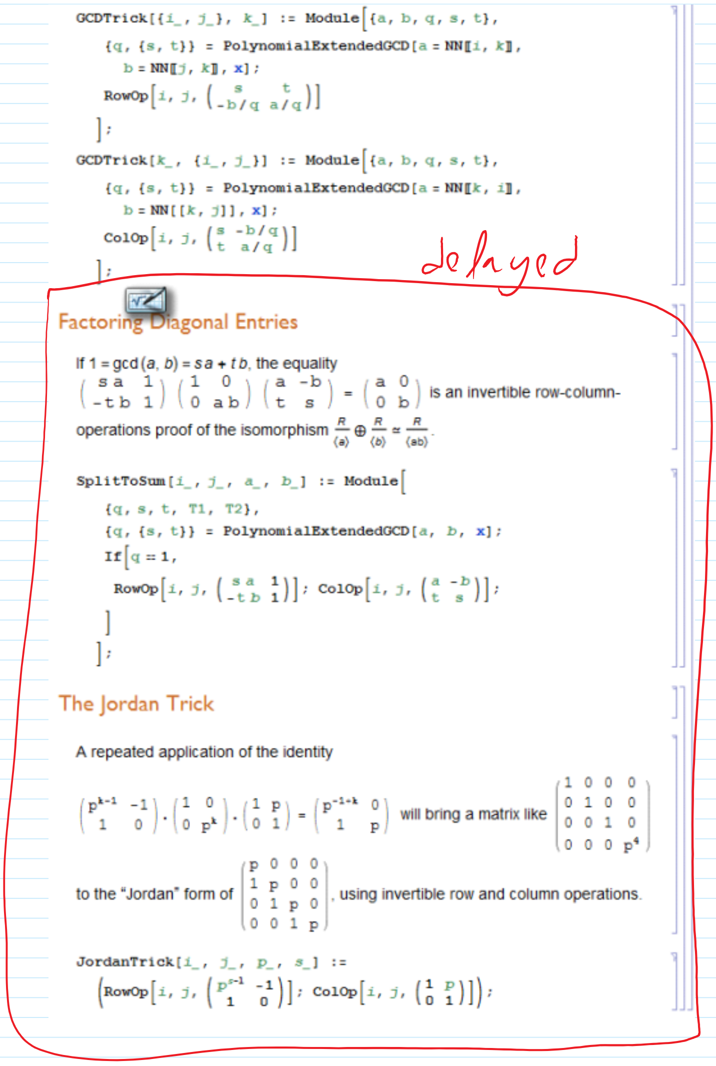
```
SwapRows[i_, j_] := RowOp[i, j, (0 1
                                 1 0)];
SwapColumns[i_, j_] := ColOp[i, j, (0 1
                                    1 0)];
SwapBoth[i_, j_] := (SwapRows[i, j]; SwapColumns[i, j];)
```

The "GCD" Trick

If $q = \gcd(a, b) = sa + tb$, 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.

```
?PolynomialExtendedGCD
```

PolynomialExtendedGCD[*poly*₁, *poly*₂, *x*] gives the extended GCD of *poly*₁ and *poly*₂ treated as univariate polynomials in *x*.
PolynomialExtendedGCD[*poly*₁, *poly*₂, *x*, Modulus → *p*] gives the extended GCD over the integers mod prime *p*. »



```
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)]
  ];
```

delayed

Factoring Diagonal Entries

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

```
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)];
   ]
  ];
```

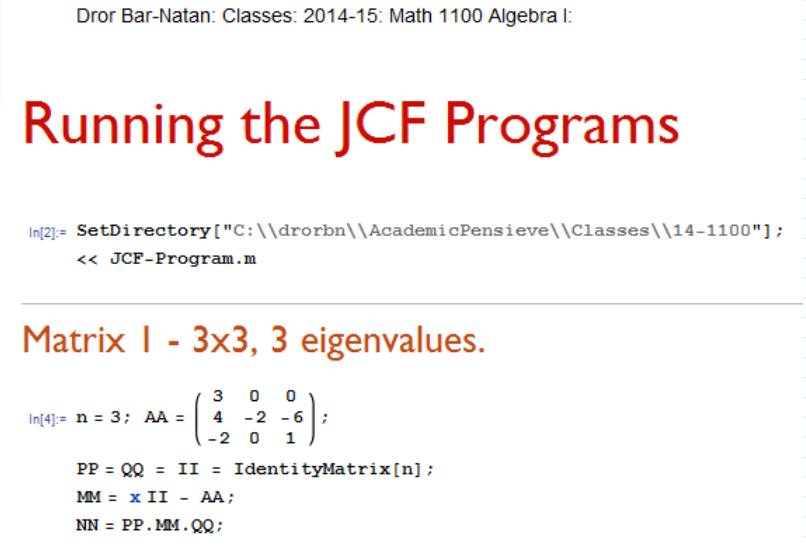
The Jordan Trick

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)]);
```

along with:



Running the JCF Programs

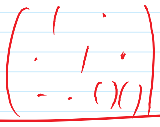
```
In[2]:= SetDirectory["C:\\drorbn\\AcademicPensieve\\Classes\\14-1100"];
        << JCF-Program.m
```

Matrix 1 - 3x3, 3 eigenvalues.

In[4]:= n = 3; AA = $\begin{pmatrix} 3 & 0 & 0 \\ 4 & -2 & -6 \\ -2 & 0 & 1 \end{pmatrix}$;

```
PP = QQ = II = IdentityMatrix[n];
MM = x II - AA;
NN = PP.MM.QQ;
```

done to



Recovering C from P?

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

$$Ce_i = \pi_B(Pe_i)$$
$$= \pi_B\left(\sum x^k P_k e_i\right)$$
$$= \sum x^k \pi_B(P_k e_i)$$
$$= \sum B^k P_k e_i$$

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

Go through run 2 until stuck, then

The "Jordan Trick": $R\langle p^s \rangle = \langle x \rangle / p^s x = 0$

$x_0 = x$

$x_1 = -px$

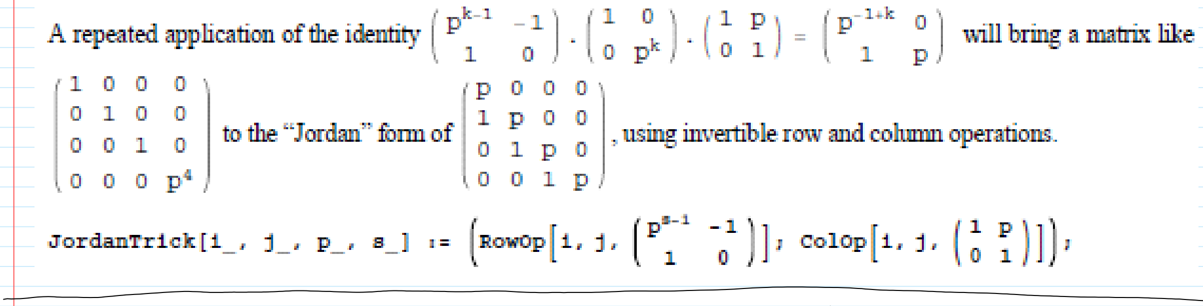
$x_2 = p^2 x$

$= \langle x_0 \ldots x_{s-1} \rangle \Big/ \begin{matrix} p x_i + x_{i+1} = 0 \\ p x_{s-1} = 0 \end{matrix}$

so $(p^s) \sim \begin{pmatrix} p & & & \\ 1 & p & & \\ & 1 & p & \\ & & 1 & p \end{pmatrix}$

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

Explicitly:



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_] := $\left(\text{RowOp}\left[i, j, \begin{pmatrix} p^{s-1} & -1 \\ 1 & 0 \end{pmatrix}\right]; \text{ColOp}\left[i, j, \begin{pmatrix} 1 & p \\ 0 & 1 \end{pmatrix}\right]\right)$;

Then go through the rest of run2 & through run 3 ....

The Jordan Trick

November-20-14 10:04 AM

$R/\langle p^s \rangle = \langle x \rangle / p^s x = 0$

$= \langle x_0 \ldots\ldots x_{s-1} \rangle \Big/ \begin{matrix} px_i + x_{i+1} = 0 \\ px_{s-1} = 0 \end{matrix}$

$x_0 = x$

$x_1 = -px$

$x_2 = p^2 x$

so $(p^s) \sim \begin{pmatrix} p &&& \\ 1 & p && \\ & 1 & p & \\ && 1 & p \end{pmatrix}$

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

14-1100 Nov 24, hours 30-31: More JCF, ...

November-20-14 12:14 PM

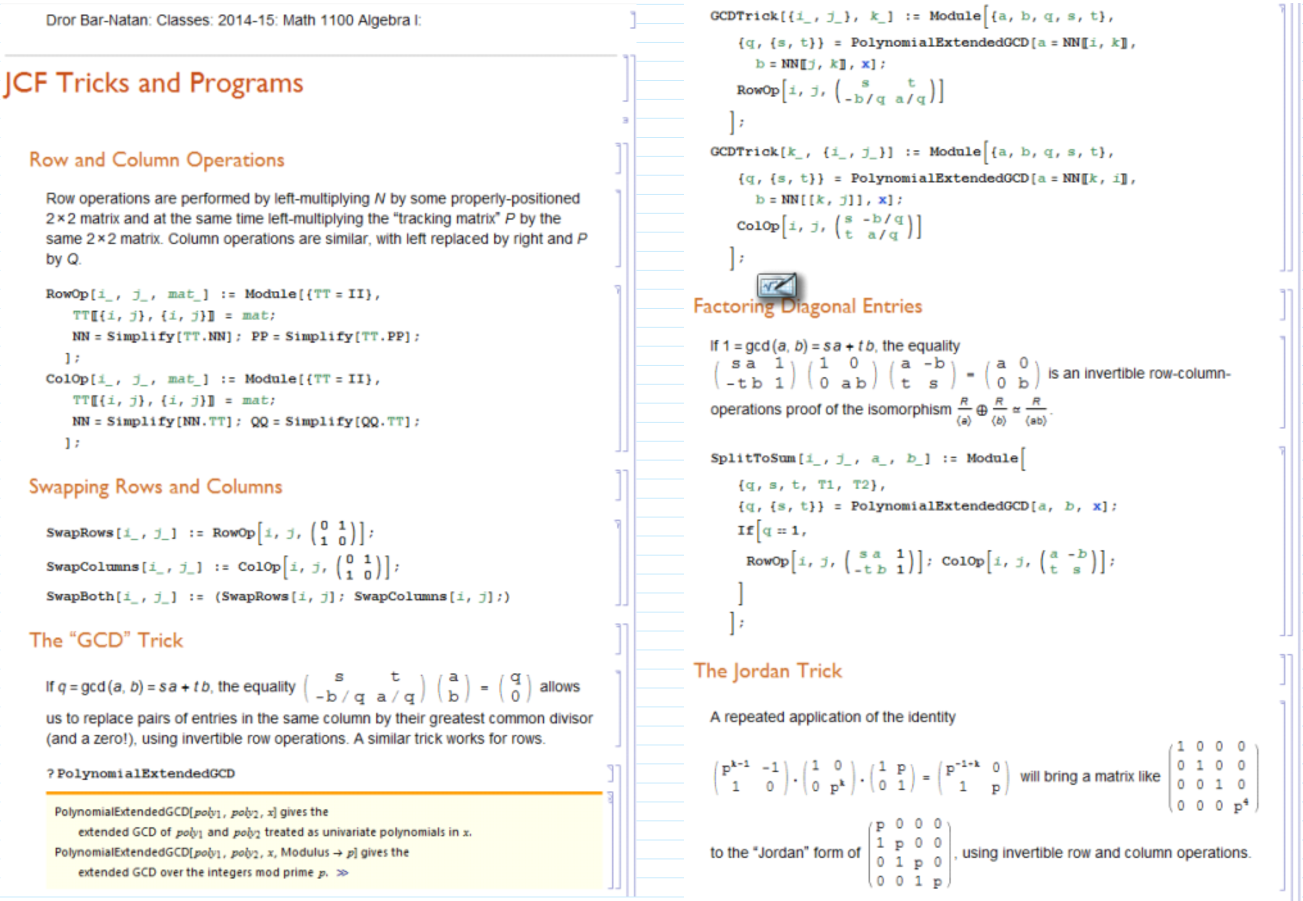
Course evals: 2/17

Riddles as in Nov24Riddles.nb

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

Finish last week's material:

Go over handout along with "run 1"



Dror Bar-Natan: Classes: 2014-15: Math 1100 Algebra I:

JCF Tricks and Programs

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

```
                                (0 1)
SwapRows[i_, j_] := RowOp[i, j, (1 0)];

                                   (0 1)
SwapColumns[i_, j_] := ColOp[i, j, (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 divisor (and a zero!), using invertible row operations. A similar trick works for rows.

```
? PolynomialExtendedGCD
```

PolynomialExtendedGCD[*poly*₁, *poly*₂, *x*] gives the extended GCD of *poly*₁ and *poly*₂ treated as univariate polynomials in *x*.
PolynomialExtendedGCD[*poly*₁, *poly*₂, *x*, Modulus → *p*] gives the extended GCD over the integers mod prime *p*. >>

```
GCDTrick[{i_, j_}, k_] := Module[{a, b, q, s, t},
   {q, {s, t}} = PolynomialExtendedGCD[a = NN[[i, k]],
     b = NN[[j, k]], x];
                     (  s     t  )
   RowOp[i, j, (-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];
                     (s -b/q)
   ColOp[i, j, (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,
                   ( s a  1)                (a -b)
    RowOp[i, j, (-t b  1)]; ColOp[i, j, (t  s)];
   ]
  ];
```

The Jordan Trick

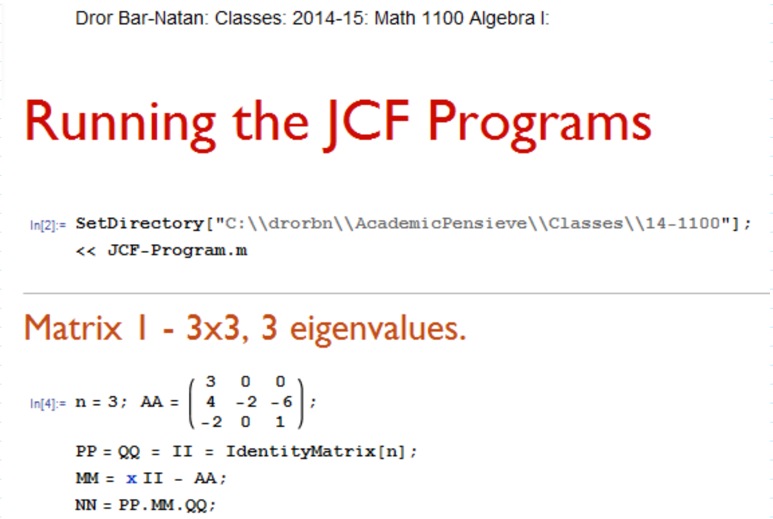
A repeated application of the identity

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

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_] :=
                    (p^(s-1) -1)                (1 p)
  (RowOp[i, j, (  1      0)]; ColOp[i, j, (0 1)]);
```

along with:



Dror Bar-Natan: Classes: 2014-15: Math 1100 Algebra I:

Running the JCF Programs

```
In[2]:= SetDirectory["C:\\drorbn\\AcademicPensieve\\Classes\\14-1100"];
        << JCF-Program.m
```

Matrix 1 - 3x3, 3 eigenvalues.

```
In[4]:= n = 3; AA = ( 3   0   0
                      4  -2  -6
                     -2   0   1 );
        PP = QQ = II = IdentityMatrix[n];
        MM = x II - AA;
        NN = PP.MM.QQ;
```

Recovering C from P?

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

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

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

Go through run 2 until stuck, then

The "Jordan Trick": $R/\langle p^s\rangle = \langle x\rangle / p^s x = 0$

$x_0 = x$

$x_1 = -px$

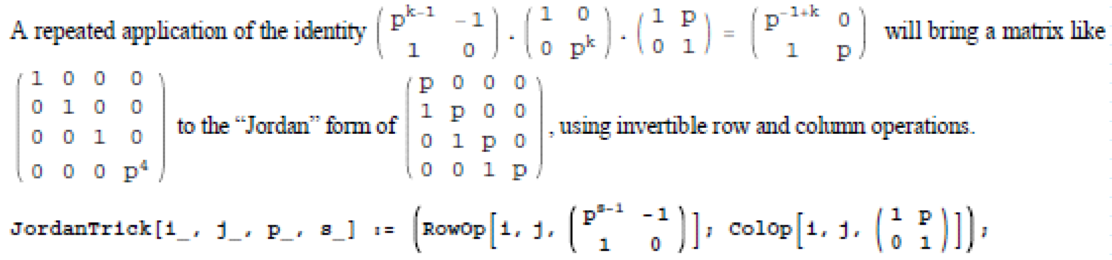
$x_2 = p^2 x$

$= \langle x_0 \ldots x_{s-1}\rangle \Big/ \begin{matrix} px_i + x_{i+1} = 0 \\ px_{s-1} = 0 \end{matrix}$

so $(p^s) \sim \begin{pmatrix} p &&& \\ 1 & p && \\ & 1 & p & \\ && 1 & p \end{pmatrix}$

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

Explicitly:



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 )]);
```

Then go through the rest of run 2 & through run 3 .....

Goal: The "ring" of modules.

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

Tensor Products. Given M, N

Definition A "tensor product" $M \otimes N$ is a module $M \otimes N$ along with a bilinear $\iota : M \times N \longrightarrow M \otimes N$ s.t.

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

Thm $M \otimes N$ exists & is unique up to isomorphism.

Pf First uniqueness, Then

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

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

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

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

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

example. $\iota : F(X) \otimes F(Y) \to F(X \times Y)$

1. Always injective! [not so easy!]
2. Isomorphism if X or Y are finite.
3. Not surjective if $R = \mathbb{Z}$, X, Y are infinite. [not at all obvious!]

---

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

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

14-1100 Nov 27, hour 32: The "ring" of modules

November-26-14 3:39 PM

Return HW4!

Course evals: 2/17. Vote and warn others!

Definition A "tensor product" $M\otimes N$ is a module $M\otimes N$ along with a bilinear $\iota : M\times N \longrightarrow M\otimes N$ s.t.

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

Thm $M\otimes N$ exists ✓ & is unique up to isomorphism.
today

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

Proof of uniqueness.

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

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

$[r]_q \longrightarrow [r]_a\otimes[1]_b$ $\quad [r_1r_2]\otimes[1] = [r_1][r_2]$

Example. $\iota : F(X)\otimes F(Y) \to F(X\times Y)$

1. Always injective! [not so easy!]
2. Isomorphism if X or Y are finite.
3. Not surjective if $R=\mathbb{Z}$, X, Y are infinite. [not at all obvious!]

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

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

done line

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

line

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

<u>Claim</u> If M is torsion $\left[\begin{matrix}\forall m \in M\ \exists r \in R \setminus \{0\} \\ rm = 0\end{matrix}\right]$ 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. $\dim_{R/\langle p \rangle} \operatorname{im}(m \mapsto p^s m)_{R/\langle p \rangle} = k + |\{i : p_i \sim p \text{ \& } s < s_i\}|$

$R/\langle p \rangle$ is a field because in a PID $\langle p \rangle$ is maximal

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!

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 $a \neq 0$.

Definition $S^{-1}R = \left\{\frac{r}{s}\right\} /$

$\frac{r_1}{s_1} \sim \frac{r_2}{s_2}$ if $r_1 s_2 = r_2 s_1$

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

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

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

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

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

$R \setminus P$ — "localization at P"

$\{2^n\}$ — "dyadic rationals".

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

14-1100 Dec 1, hours 33-34: Uniqueness in the structure theorem

November-29-14 7:29 PM

Next class: Wed 1-3 OH 3-4.

Course evals: 4/17 Vote and warn others!

Goal. Uniqueness in the structure thm.

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

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

start line

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 $Q(R)$ "the field of fractions"

s.t.

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

proof: later.

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

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

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

$R/\langle p\rangle$ is a field because in a PID $\langle p\rangle$ is maximal

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

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

on $R/\langle p^t\rangle$ $s \geq t$

$R/\langle p^{t-s}\rangle$ on $R/\langle p^t\rangle$ $s<t$

$R/\langle p^t\rangle$ on $R/\langle p^s\rangle$ $s \geq t$

$R/\langle p^s\rangle$ on $R/\langle p^t\rangle$ $s<t$

$R/\langle p^s\rangle \hookrightarrow \ker$ 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 $r_1 s_2 = r_2 s_1$

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

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

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

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

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

$R\setminus P$ — "localization at P"

$\{2^n\}$ — "dyadic rationals".

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

all done

14-1100 Dec 1, hours 35-36: Topological insolubility of the quintic, more on the JCF

September-03-14 12:34 PM

Pam needs voluntеers to mark olympiad questions!

Course evals: 5/17

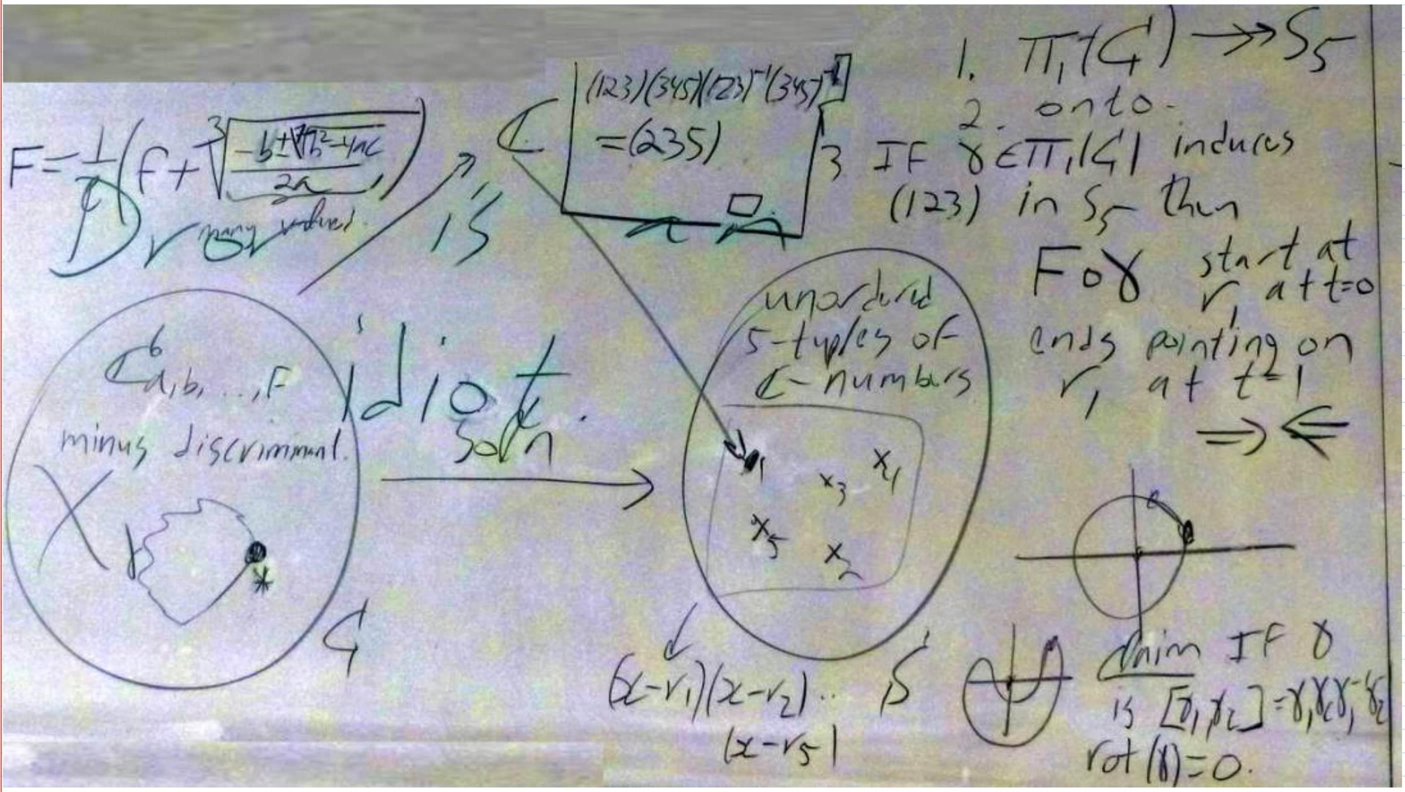
The Final: All is included, same style as term test & as previous years.

The key: Understand EVERYTHING.

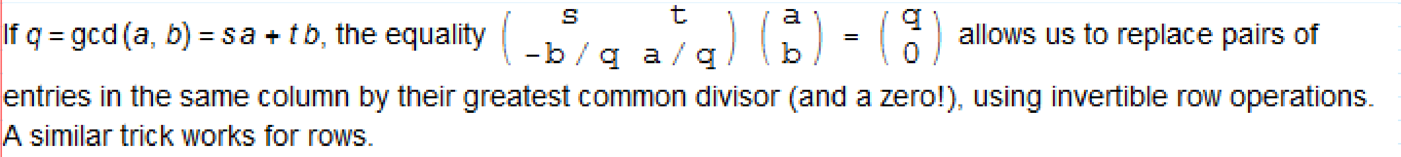
Today: Not solving the quintic, more on JCF.

Tomorrow: Riddles session! Bahen 6183, 10 AM.

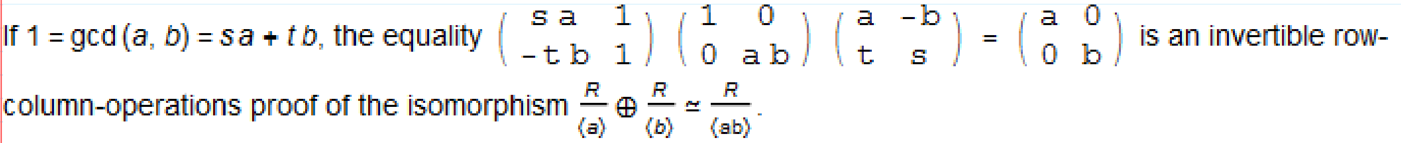
Following http://drorbn.net/dbnvp/AKT-140314.php:


$F=\frac{1}{f}\left(f+\sqrt[3]{\frac{-b\pm\sqrt{b^2-4ac}}{2a}}\right)$
many valued
is
$\mathbb{C}$
$(123)(345)(123)^{-1}(345)^{-1}$
$=(235)$
1. $\pi_1(G)\twoheadrightarrow S_5$
2. onto.
3 If $\gamma\in\pi_1(G)$ induces (123) in S_5 then
For γ start at r_1 at t=0
ends pointing on r_1 at t=1
$\mathbb{C}^6_{a,b,\dots,F}$
minus discriminant
X
γ
G
idiot.
soln
unordered 5-tuples of $\mathbb{C}$-numbers
x_1 x_3 x_4 x_5 x_2
$(x-r_1)(x-r_2)\cdots(x-r_5)$
is
claim If γ is $[\gamma_1,\gamma_2]=\gamma_1\gamma_2\gamma_1^{-1}\gamma_2^{-1}$
rot$(\gamma)=0$.

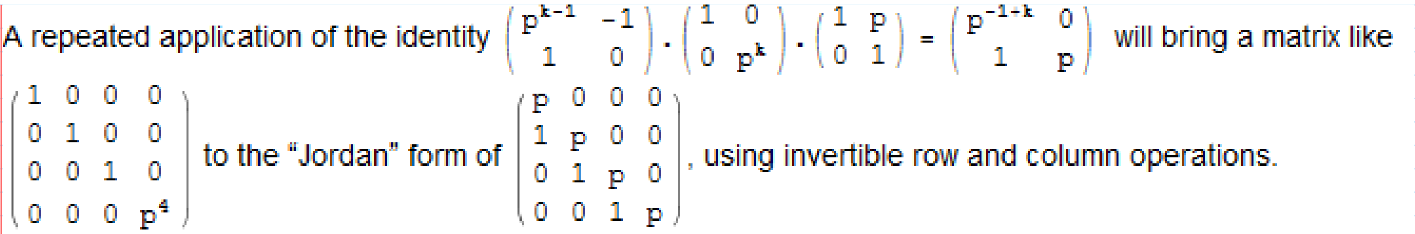
Some JCF tricks



If $q=\gcd(a,b)=sa+tb$, 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.



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



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.

$$\langle x, y\rangle \Big/ \begin{matrix} y=0 \\ p^k x = 0 \end{matrix} \quad \cong \quad \langle x, z\rangle \Big/ \begin{matrix} p^{k-1}x + z = 0 \\ pz = 0 \end{matrix}$$

$$y \longmapsto p^{k-1}x + z$$

$$x \longmapsto -x$$

$$-x \longleftarrow\!\shortmid\ x$$

$$y + p^{k-1}x \longleftarrow\!\shortmid\ z$$