MAT 1100 Core Algebra. To do: 1. Print “About”

2. Print NCGE (4 sides)

3. Video tape?

I don’t know core algebra

Goal: Within your lifetime, understand $G = \langle g_1, \ldots, g_n \rangle \times S_n$:

1. $|G| = n^n$
2. $G/G_0$
3. $G = \langle g_1, \ldots, g_m \rangle$ random

Two prerequisites 1. Groups, $S_n$, silly uniquenesses,

cancellation, $(ab)^{-1} = b^{-1}a^{-1}$, subgroups, the

subgroup generated by $\{0, 2\}$.

2. Row reduction for real.

Algorithm as in handout.

Claim 1. Every $G_{ij}$ is in $G$.

Claim 2. Anything fed to $T$ is now a monoton product

Claim 3. If two monotone products are equal

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

Claim 4. Let $M_k = \{\text{monotone products} \}$, $\text{beginning with } k \}$, then for every $k_1, M_k \cdot M_k \subset M_k$ (and so each

$M_k$ is a subgroup of $S_n$.

Proof. Clearly $M_n \cdot M_n \subset M_n$. Now assume that $M_5 \cdot M_5 \subset M_5$

and show that $M_4 \cdot M_4 \subset M_4$. Start with $\sigma_8, M_4 \subset M_4$:
and show that $M_4 M_4 \subset M_4$. Start with $\sigma_{8, j} M_4 \subset M_4$:

$$\sigma_{8, j} (\sigma_{4, j4} M_5) \overset{1}{=} (\sigma_{8, j} \sigma_{4, j4}) M_6 \overset{2}{\subset} M_4 M_5$$
$$\overset{3}{=} \sigma_{4, j4} (M_3 M_5) \overset{4}{\subset} \sigma_{4, j4} M_5 \subset M_4$$

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

Then do goals 1, 2, 3, 4, and the 0: “in our lifetime.”

**Example** $\sigma^{-1} = (123)$, $\sigma_2 = (12)(34)$, in $S_4$

<table>
<thead>
<tr>
<th></th>
<th>11</th>
<th>12</th>
<th>13</th>
<th>14</th>
</tr>
</thead>
<tbody>
<tr>
<td>$\sigma_1$</td>
<td>$231,4$</td>
<td>$214,3$</td>
<td></td>
<td></td>
</tr>
<tr>
<td>$\sigma_2$</td>
<td>$231,4$</td>
<td>$214,3$</td>
<td></td>
<td></td>
</tr>
<tr>
<td>$\sigma_3$</td>
<td>$312,4$</td>
<td>$134,2$</td>
<td></td>
<td></td>
</tr>
<tr>
<td>$\sigma_4$</td>
<td>$312,4$</td>
<td>$134,2$</td>
<td></td>
<td></td>
</tr>
</tbody>
</table>

Feed $\sigma_1 = 231\,4$ ... Fed @ $\sigma_1$

Feed $\sigma_2 = 312\,4$ ... Fed @ $\sigma_2$

Feed $\sigma_3 = 214\,3$ ... Feed $\sigma_2^1 \sigma_3 = 134\,2$ ... Fed @ $\sigma_3$

Feed $\sigma_1 \sigma_2^3 = 214\,3$ ... Feed $\sigma_1^1 \sigma_1 \sigma_2^3 = \sigma_3$ ...

No point feeding $\sigma_{1, j}$ or if $j \neq 0$

Feed $\sigma_2^3 \sigma_{12} = 341\,2$ ... Feed $\sigma_{13}^{-1} \sigma_2^3 \sigma_{12} = 142\,3$ ... to $\sigma_{24}$

Feed $\sigma_2^3 \sigma_{13} = 413\,2$ ... to $\sigma_{24}$

Feed $\sigma_{24} \sigma_{12} = 421\,3$ ... Fed $\sigma_{24} \sigma_{12} \sigma_{12} = 142\,3$ ... drop

$16 \mid 143.1 \cdot 1 = 12$. It is $412\,3 \in G$.

Write $2431$ in terms of $\sigma_{1, 2}$.
* Go over the "about" handout.
1. Finish tracing the NCGE handout; along do the S₄ example.

2. Go over the "about" handout.

3. Group homomorphisms, the "category" of groups, images and kernels. Example: S₃ is an image of S₄, but not a kernel.

4. Normal subgroups, kernels are normal.

5. Question: Is there a normal subgroup of S₄ which is isomorphic to S₃?

---

**Example**

\[
\begin{array}{c|ccc}
1 & 2 & 3 & \hline
1 & 2 & 3 & 4 \\
2 & 3 & 4 & 1 \\
3 & 4 & 1 & 2 \\
4 & 1 & 2 & 3 \\
\end{array}
\]

\[
\sigma_1 = (1\ 2\ 3) \quad \sigma_2 = (1\ 2\ 3\ 4), \quad \text{in } S_4
\]

\[
\begin{array}{c|ccc}
1 & 2 & 3 & \hline
1 & 2 & 3 & 4 \\
2 & 3 & 4 & 1 \\
3 & 4 & 1 & 2 \\
4 & 1 & 2 & 3 \\
\end{array}
\]

\[
\sigma_1 = 2314 \quad \sigma_2 = 3124
\]

\[
\sigma_1 \sigma_2 = 1234 \quad \sigma_2 \sigma_1 = 1342
\]

\[
\sigma_1 \sigma_2 \sigma_1 \sigma_2 = 1432
\]

\[
\sigma_1 \sigma_2 \sigma_3 = 2143
\]

\[
\sigma_1 \sigma_2 \sigma_3 = \sigma_3
\]

\[
\text{No point feeding } \sigma_i \text{ if } i \neq k 
\]

\[
\sigma_2 \sigma_3 = 3412 \quad \text{Feed } \sigma_3 \sigma_2 \sigma_3 = 1423 \quad \text{to } \sigma_4
\]

\[
\sigma_2 \sigma_3 = 4132 \quad \text{to } \sigma_4
\]

\[
\sigma_2 \sigma_4 = 4213 \quad \text{Feed } \sigma_4 \sigma_2 \sigma_4 = 1423 \quad \text{drop}
\]

\[
16 = 4 \cdot 3 \cdot 1 \cdot 1 = 12, \quad \text{Is } 1123 \in S_6^2
\]

\[
\text{Write } 2431 \text{ in terms of } \sigma_{12}
\]
September 20 and 22, hours 4-6, Lectures by Selick

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

**Warnings.** For Dror,
1. \( x^g \cdot g^{-1} = x^g \) so that \( (x^g)^h = x^{gh} \)
2. If \( \sigma, \tau \in S_n \), then
   \( \sigma \cdot \tau = \tau \cdot \sigma \)

**Definitions.** Homomorphism, isomorphism, subgroup, cosets, normal subgroup, \( C_a(X) \), \( Z(G) \), \( N_G(X) \).

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

**The 3rd Isomorphism Thm.**
If \( K, H \leq G \) & \( K \triangleleft H \), then
\[
\frac{G/K}{H/K} \cong \frac{G}{H}
\]

**The 4th Isomorphism Thm.**
If \( N \triangleleft G \), then \( \pi: G \to G/N \), induces a “faithful” bijection between subgroups of \( G/N \) and \( \{ H : N \leq H \leq G \} : \)
* \( A \triangleleft B \iff \pi(A) \triangleleft \pi(B) \) & \( [B : A] = [\pi(B) : \pi(A)] \)
* \( A \triangleleft B \iff \pi(A) \triangleleft \pi(B) \)
* \( \pi(A \cap B) = \pi(A) \cap \pi(B) \).

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

**Claim.** For \( H, K \leq G \), \( HK \leq G \) iff \( HK = KH \).

**Claim.** If \( H, N_G(K) \) then \( HK = KH \), \( K \triangleleft HK \), & \( HK \triangleleft G \).

**The 2nd Isomorphism Theorem.**
If \( H \triangleleft N_G(K) \), then
\[
\frac{HK}{K} \cong \frac{H}{N_G(K) \cap H}
\]

**Permutation Groups.** \( S_n, |S_n| = n! \), \( \text{sign}: S_n \to \{ \pm 1 \} \) by
\[
\text{sign}(\sigma) = (-1)^{\frac{1}{2} \sum_{i < j} 1} \text{sign}(i-j)
\]
is a homomorphism, so \( A_n = \text{ker} (\text{sign}) \triangleleft S_n, |A_n| = \frac{n!}{2} \).

**Thm.** For \( n \# 4 \), \( A_n \) is “simple” - it has no normal subgroups except the trivial one and itself.

Thanks, Paul, for teaching for me, and Parker for the detailed notes!
On board.

1. Class photo at 10:55?

2. HW is on web.

3. \( x^g = g^{-1}xg \) so \((e^g)^h = e^{c_gh}(e^{c_gh} = x^{b(g)})\)

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


Go over the "Selick" handout.

Example: 1. \( \phi: S_4 \rightarrow S_3 \)

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

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

\[ G = G_0 \triangleright G_1 \triangleright G_2 \triangleright \ldots \triangleright G_n = \{ e \} \text{ s.t. } |H_i| = \frac{|G|}{|G_i|} \]

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

Example \( S_4 \triangleright A_4 \triangleright \frac{(12)(34)}{12} \triangleright \frac{(12)(34)}{2} \triangleright \frac{\{1\}}{2} \)

Proof: by induction on \( |G| \).

Existence: Let \( G_1 \) be a maximal normal...
Uniqueness: Use the "diamond principle":

\[ G = G_1 \triangleleft G_2 \quad \quad G = G_1' \triangleleft G_2' \quad \quad \]

Claim: \( G = G_1, G_1' \)

Proof: \( G_1, G_1' \) is normal in \( G \) yet

\( G_1 \trianglerighteq G_1' \) bigger than \( G_1, G_1' \).

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

**Cycle Decomposition.** \((12)(345) = [21453] = 2 \times 153\)

Claim: If \( \sigma = (a_1 \ldots a_k) \) and \( \tau = [T_1 T_2 \ldots T_n] \), then

\[ \sigma \tau = \tau^{-1} \sigma \tau = ([T^{-1} a_1], [T^{-1} a_2] \ldots ) \]

Corollary: \( \sigma \) is conjugate to \( \sigma' \) iff they have the same cycle lengths

Corollary: \( \#(\text{Conjugacy classes of } S_5) = P(4) \)

**Lemma 1.** Every element of \( A_n \) is a product of 3-cycles.

Proof: \((12)(23) = (123), (123)(234) = (12)(34) \ldots \)

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

Proof: WLOG, \((123) \in N\). Claim: For \( \tau \in S_5 \), \((123)^{\tau} \in N \) if \( \tau \in A_n \)

So \( N \) contains all 3-cycles... \( \square \)

Now take \( N \triangleleft A_n \) w/ \( N \neq A_1 \).
Case 1. $N$ contains an element with cycle of length $\geq 4$
\[ \sigma = (123456) \in N \quad \sigma^{-1}(123)(123)^{-1} = (136) \]

Case 2. $N$ contains an element $\sigma = (123)(456) \in N$
Consider $\sigma^{-1}(124)(124)^{-1} = (14263)$

Case 3. $N$ contains $\sigma = (123)$ (product of $\rho_n$)
Then $\sigma^2 = (132)$.

Case 4. Every element of $N$ is a product of disjoint 2-cycles
\[ \tau = (12)(34) \in N \quad \Rightarrow \quad \tau^{-1}(123)(123)^{-1} = (13)(24) \in N \]
\[ \Rightarrow \quad \tau^{-1}(125)(125)^{-1} = (13452) \in N \]
Jordan-Hölder:

\[ G \xrightarrow{H_1} G_1 \xrightarrow{H_1'} G_{1'} \quad \text{claim} \quad G = G_1 G_{1'} \]

\[ G \xrightarrow{G_1} G_{1'} \quad \text{is normal in } G \quad \text{yet} \]

\[ G_1 \triangleleft G_{1'} \quad \text{bigger than } G_1, G_{1'} \]
October 4, hours 9-10: Simplicity of $A_n$, Group Actions

* Agenda: Simplicity of $A_n$, group actions.

* Makeup class: Thursday at 9AM?

  Read Along?

* Go over handouts.

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

s.t. $(g_1g_2)x = g_1(g_2x)$, $eX = X$. Same as $f: G \rightarrow S(X)$.

$G$-sets are a category!


  2. Subgroups($G$), under conjugation.  \( \text{not} \) done.

Examples: 1. $G/H$ When $H$ is not necessarily normal

Sub-example: $S_n/S_{n-1}$, $S_{n-1} = O/S_{n-1}$ iff

$0 - (n) = 0 - (n)$. Let $T_i(n) = i$, then

$0 - T_i S_{n-1} = T_{n-1} S_{n-1}$. So $S_n/S_{n-1}$ is $\ldots$?

2. If $X_1, X_2$ are $G$-sets, then so is $X_1 \times X_2$.

3. $S^2 = SO(3)/SO(2)$ \( \text{done} \)

**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

$X \cong G/\text{stab}_X(x)$. (So $|X| = |G|$)

**Theorem.** If $X$ is a $G$-set and $x_i$ are representatives

of the orbits, then

$|X| = \sum \frac{|G|}{|\text{stab}_X(x_i)|}$
Example: If $G$ is a $p$-group, the Centre of $G$ is not empty.
The Class Photo

From Drorbn
Our class on September 27, 2011:

Class Photo: click to enlarge

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

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

The first option is more fun but less private.

Who We Are...

<table>
<thead>
<tr>
<th>First name</th>
<th>Last name</th>
<th>UserID</th>
<th>Email</th>
<th>In the photo</th>
<th>Comments</th>
</tr>
</thead>
<tbody>
<tr>
<td>Dror</td>
<td>Bar-Natan</td>
<td>Drorbn</td>
<td><a href="mailto:drorbn@math.toronto.edu">drorbn@math.toronto.edu</a></td>
<td>facing everybody, as the photographer</td>
<td>Take this entry as a model and leave it first. Otherwise alphabetize by last name. Feel free to leave some fields blank. For better line breaking, leave a space next to the &quot;@&quot; in email addresses.</td>
</tr>
<tr>
<td>Vanessa</td>
<td>Foster</td>
<td><a href="mailto:vanessa.foster@math.toronto.ca">vanessa.foster@math.toronto.ca</a></td>
<td>front row, 4th person from the left</td>
<td>Wearing a long sleeve T with stripes</td>
<td></td>
</tr>
<tr>
<td>Parker</td>
<td>Glynn-Adey</td>
<td>pgadley</td>
<td><a href="mailto:parker.glynn.adey@math.toronto.ca">parker.glynn.adey@math.toronto.ca</a></td>
<td>Fifth from the right in the back row</td>
<td>Glowing bald guy with yellow shirt.</td>
</tr>
<tr>
<td>Mary</td>
<td>He</td>
<td>ymhe</td>
<td><a href="mailto:yannmary.he@utoronto.ca">yannmary.he@utoronto.ca</a></td>
<td>Third from the left in the front row</td>
<td>Navy sweater</td>
</tr>
<tr>
<td>Daniel</td>
<td>Hirschmeier</td>
<td>Dhirschm</td>
<td><a href="mailto:daniel.hirschmeier@utoronto.ca">daniel.hirschmeier@utoronto.ca</a></td>
<td>Back row farthest to the right</td>
<td>Blonde guy, white t-shirt with a cowboy on it.</td>
</tr>
</tbody>
</table>
| Tyler      | Holden             | tholden | tholden@math.toronto.edu   | Roughly in the middle, under the $N \triangleleft G$ but obscuring the $
\triangleright$ | Wearing a black polo. |
| Philip     | Mar                | Pallenmar | pallenmar@gmail.com | 4th from right | White shirt among white shirts |
| James      | Mracok             | Irmarcek | jmracok@math.toronto.ed         | 7th from the right (or left) in the back row | Glasses with black and white t-shirt. |
| Jerrod     | Smith              | Smith36j | jerrod.smith(at)utoronto(dot)ca | Back row, 3rd from left | Brown t-shirt |
| Auben      | Tapia              | Auben  | aubertapia@gmail.com        | 5th from right | Dark brown shirt. |
| Louis-Philippe | Thibault   | Lp.thibault | lp.thibault@utoronto.ca | Back row, 2nd from left | Yellow and Blue t-shirt |
| Nan        | Wu                 | Wunan3 | n.wu@utoronto.ca            | 3rd from right, back row | Red shirt |
| Lei        | Zhang              | Zhanglei | leizhang@comm.utoronto.ca   | 4th from left, back row | Glasses, white shirt. |
The Simplicity of the Alternating Groups

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 $A_n \subset S_n$ is simple for $n \neq 4$.

**Remark.** Easy for $n \leq 3$, false for $n=4$ as there is $\phi : A_4 \to A_3$, 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 $\sigma = (12)\tau^{-1}$ w/ $\tau \in A_n$, and then as $(123)^{(12)} = (123)^2$, $(123)^\sigma = (123)^2$ in $N$. So $N$ contains all 3-cycles.

**Case 1.** $N$ contains an element w/ cycle of length $\geq 4$.

**Resolution.** $\sigma = (123456)^\sigma \in N \Rightarrow \sigma^{-1}(123)^\sigma(123)^{-1} = (134) \in N$.

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

**Resolution.** $\sigma = (123)(452)^\sigma \in N \Rightarrow \sigma^{-1}(124)^\sigma(124)^{-1} = (1423) \in N$.

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

**Resolution.** $\sigma = (123) \in N$.

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

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

$\Rightarrow \tau^{-1}(125) \tau(125)^{-1} = (13452) \in N$
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
   
   $$X \cong G/\text{stab}_x(x). \quad (\text{So } |X| = |G|/|\text{stab}_x(x)|)$$

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

$$|X| = \sum_{i} \frac{|G|}{|\text{stab}_x(x_i)|}$$

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

**THE SYLOW THEOREMS.**

Lecture notation: $p \nmid |G|$,

$$|G| = p^k \cdot m, \; \text{p prime, } p \nmid m.$$  

$\text{Syl}_p(G) := \{P \leq G : |P| = p^k\}$

are "Sylow $p$-subgroups of $G".$ A "$p$-subgroup" in general, is any subgroup of $G$ of order a power of $p.$

**Sylow I** $\text{Syl}_p(G) \neq \emptyset.$  

**Proof.** By induction on $|G|$, if $G$ has a normal subgroup of order $p$ (or $p^2$) or if $G$ has a subgroup of order divisible by $p^k$, we are done. The existence of one of the said types follows from the class equation:

The centre of $G$, the centralizer of $y_i$ in $G$.

Either both are divisible by $p$. 

\[ |G| = |\mathbb{Z}(G)| + \sum_i (G: G(y_i)) \] 
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" ODF pp 102

**Proof:** Enough to find an element of order divisible by \( p \). If \( Z \) is of order \( p \cdot n \), \( Z \) would be of order \( p \).

Pick \( x \in G \), \( x \neq 1 \). If \( p \nmid |x| \), we're done. Otherwise \( p \mid |G/<x>| \), so by induction, \( \exists y \in G \) s.t. \( |G/<y>| = p \) in \( G/<x> \). So \( y^p \in <x> \) i.e., \( y^p = x^k \) for some \( k \). Write \( |y| = pk + r \) with \( 0 \leq r < p \), get \( y^p = x^{pk + r} = y^r \) \( \in <x> \Rightarrow r = 0 \), as \( |G| = p \).

So the order of \( y \) is divisible by \( p \). \[ \square \]

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

**Claim:** if \( \phi : G \to H \) is a morphism \& \( y \in G \),

then \( |\phi(y)| \mid |y| \).

**Proof.** If \( |\phi(y)| = n \), \( |y| = m \), \( m = nq + r \), then \( e = \phi(y^m) = \phi(y^n)^q \phi(y^r) = (\phi(y))^q \phi(y^r) = \phi(y)^r \).

So \( r = 0 \).

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

2. Every \( p \)-group is contained in a Sylow-\( p \) group.
3. All Sylow-$p$ subgroups of $G$ are conjugate, and

$$N_p(G) = |\text{Syl}_p(G)| = 1 \mod p \quad \& \quad N_p(G) \mid |G|$$

**Groups of order 15.**

$P_3$ is normal in $G$, $P_3$ is normal in $G$, Any $y \in P_3$ commutes

with $P_3$.

[Otherwise, $|y||\text{Aut}(P_3)| = y$.]

(Aside. $\text{Aut}(Q_4) = (Z/2)^*,$ so $|\text{Aut}(Q_4)| = 2 - 1$)

So $G = x^i y^j = y^j x^i$ for generators $x \in P_1, y \in P_3$.

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

$$G = G_1 \times G_2$$

**Aside.** $Z/p \times Z/q = Z/pq$  

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

This also works for order $pq$, $p, q$ primes, $pq \neq 1$.

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

$P_3$ may act on $P_7$. If $P_7 = \langle x \rangle$, $P_3 = \langle y \rangle$, we have $x^y = x$, or $x^2$, or $x^4$ [Aside. $\text{Aut}(Z/7)$ is cyclic]

Dell. What does this mean?

**Aside.** $\text{Aut}(Z/7) = \langle x^1, x^2, x^3, x^4 \rangle$  

This also works for order $pq$, $p, q$ primes, $pq \neq 1$.

Also did the "extension lemma.

**Lemma.** If $P \in \text{Syl}_p(G)$ & $H \triangleleft N_G(H)$ is a $p$-group, then $H \triangleleft P$.

2. If $P \in \text{Syl}_p(G)$, $|x| = p^b$, $x \in N_G(P)$, then $x \in P$.

Reformulation: $P \in \text{Syl}_p(G)$, $|H| = p^b \Rightarrow N_G(H) = H^P$.

**Stronger Sylow.** 1. If $p^b \mid |G|$, then $G$ has a subgroup of order $p^b$. 
Proof: Let \( X = \{ s \in G : |s| = p^k \} \), and write \( |G| = p^k \).

Let \( |G| = p^k \) be maximal \( k \). By counting binomial nonsense, \( p^k |\chi| \) yet \( p^{k+1} |\chi| \).

\( G \) acts on \( X \) by translations, so there must be \( s_0 \in X \) s.t. \( p^{k+1} |G : s_0| \), hence \( p^k |H| = \text{stab}_G(s_0) | \). Yet if \( x \in s_0 \), then \( g \to gx \) is an injection \( H \to s_0 \), so \( |H| \leq |s_0| = p^k \), so \( |H| = p^k \).
Theorem. 1. Sylow p-groups always exist: \( \text{Syl}_p(G) \neq \emptyset \).  
2. Every p-group is contained in a Sylow p-group. 
3. All Sylow p-subgroups of G are conjugate, and 
   \( n_p(G) = |\text{Syl}_p(G)| = 1 \mod p \) and \( n_p(G) | |G| \).

Lemma. If \( P \in \text{Syl}_p(G) \) and \( H < N_G(P) \) is a p-group, then \( H \leq P \).

Reformulation: If \( P \in \text{Syl}_p(G) \), \( |H| = p^k \Rightarrow N_H(P) = H \cap P \).

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

Claim. \( H \triangleleftHK, K \triangleleft HK, HK = \{e\} \), then \( HK \triangleleft HK \).

Proof. \( [h,k] = hkh^{-1}k^{-1} \in HK = \{e\} \).

Corollary. If \( |G| = 15 \), \( G = \mathbb{Z}_3 \rtimes \mathbb{Z}_5 = \mathbb{Z}_15 \).

Claim. If \( (a,b) = 1 \), then \( \mathbb{Z}_a \times \mathbb{Z}_b \cong \mathbb{Z}_{ab} \).

Proof. Find \( s, t \) s.t. \( as + bt = 1 \), and write:

\[
\begin{array}{ccc}
\mathbb{Z}_a & \times & \mathbb{Z}_b \\
\downarrow & & \downarrow \\
\mathbb{Z}_a b & \cong & \mathbb{Z}_{ab}
\end{array}
\]

Proposition. If \( P \in \text{Syl}_p(G) \), then \( |\text{conjugates of } P| = 1 \mod p \).

Proof. \( P \) acts on the set of its conjugates by conjugation. The orbit \( [P] \) is a singleton by lemma; the sizes of all other orbits are divisible by \( p \).

Proposition. If \( H \) is a p-subgroup \( \leq \text{Syl}_p(G) \), then \( \frac{|G|}{|H|} \) is divisible by \( p \).

In particular, all
Proposition. If $H$ is a $p$-subgroup of $\text{PcSym}(G)$, then $H$ is contained is a conjugate of $P$. [In particular, all $p$-subgroups are conjugate.]

Proof. $H$ acts on the set of conjugates of $P$ by conjugation. There must be a singleton orbit:

- A $P'$ s.t. $H < N_G(P')$.

Semidirect Products. If $N \leq G$, $H \leq G$, 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 $NH = \text{cay}$, injective 1st image might not be a group.

If $NH = \text{cay}$ & $N \not\leq G$ & $H \not\leq G$, then $[N, H] = \text{cay}$ & $NH \cong N \times H$.

The interesting case is when $NH = \text{cay}$, $N \not\leq G$, $H \not\leq G$.

Get $H \to \text{Aut}(N)$ by $h \mapsto (n \mapsto n^h = hnh^{-1})$ or $\varphi_h(n) = hnh^{-1}$.

$n_1h_1n_2h_2 = n_1h_1n_2h^{-1}_1h_1h_2 = n_1\varphi_{h_1}(n_2)h_1h_2$.

Definition. Given abstract $N, H$ & $\varphi : H \to \text{Aut}(N)$,

the semidirect product $N \rtimes H$.

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

2. $N \not\leq (N \times H)$ and $N \times H / N \cong H$. 
Claim. If \( K \triangleleft KH, \ H \triangleleft KH, \) then \( KH = K \times H. \)

\[
K \to KH \to KH/H \cong K
\]

\[
k h_1 = k_1 h_2 \Rightarrow k_2^{-1}k_1 = h_1 h_2^{-1} \Rightarrow k_1 = k_2 \cdot h_1 \cdot h_2^{-1}
\]

\[
h K = k h = k^h h \Rightarrow h^k = h \Rightarrow \Sigma h, k \in e.
\]

\[
h^{k h_1^{-1}} = k^{-1} k h^{-1} \Leftrightarrow k^{-1} h k h^{-1} \in H \cap K = e.
\]
October 13, hour 15: Semi-direct products

Semi-direct products.

**Given** $N$, $H$, and $\varnothing: H \rightarrow \text{Aut}(N)$,

$$N \rtimes_{\varnothing} H := \left\{ (n, h) \in N \times H \mid (n_1, h_1) \cdot (n_2, h_2) = (n_1 \varnothing h_1(n_2), h_1 h_2) \right\}$$

**Thm.** 1. $G = N \rtimes_{\varnothing} H$ is a group, $H \triangleleft G$, $N \vartriangleleft G$,

and $G/N \cong H$, and $G = NH$.

2. If $G = NH$, $N \vartriangleleft G$, $H \triangleleft G$, and $N \cap H = \varnothing$ then $G \cong N \rtimes_{\varnothing} H$.

**Small Examples.** 1. $D_{2n} = \mathbb{Z}_n \times \{ \pm 1 \}$

2. $\left\{ax + b \right\} = \mathbb{R}_b^+ \times \mathbb{R}_a^\times$

3. $\left\{ax + b : AEGL(V), b \in V \right\} = V_b \times \text{AGL}(V)$

4. "The Poincaré Relativity Group" $= \mathbb{R}^4 \times SO(3,1)

**Big Example.** $B_n = T_1 \left( (C^2 \otimes \text{sing}^0)/S_n \right) = \mathbb{R}^n$

$B_n = \langle e_1, \ldots, e_{n-1}, e_i \circ_{i+1} e_i, e_i \circ_{i-1} e_i, e_i \circ_{i+1} e_j, e_i \circ_{i-1} e_j \mid i, j > 1 \rangle$

$T: B_n \rightarrow S_n, PB_n = \ker T$

$PB_n \cap B_n$ yet $PB_n \neq B_n \times S_n$

Two reasons why I like this one:
Grains of order 21. $\mathbb{Z}/21$, $\mathbb{Z}/7 \times \mathbb{Z}/3 = \langle x \rangle \times \langle y \rangle$

$\text{Aut}(\mathbb{Z}/21) = \mathbb{Z}/6 = \langle \phi_3 \rangle$, $\phi_3(x) = x^3$, $y^7 = x$ or $x^2$ or $x^4$

(iso: if $xy = x^2$ & $y^7 = y^2$ then $x^5 = x^4$)

Grains of order 12. If $16/12$, $P_4 = \mathbb{Z}/4$ or $(\mathbb{Z}/2)^2$, $P_3 = \mathbb{Z}/3$, and at least one of these is normal for there is not enough room for $4 P_3$ & 3 $P_4$'s. So $G$ is a semi-direct product. $\mathbb{Z}_4 \times \mathbb{Z}_3$: must be $\mathbb{Z}_4 \times \mathbb{Z}_3 = \mathbb{Z}/12$

$(\mathbb{Z}/2 \times \mathbb{Z}_2) \times \mathbb{Z}_3$: Either direct or $\mathbb{Z}/2 \times \mathbb{Z}/6$

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

$\langle (123) \rangle$

$\text{Di}(\mathbb{Z}/2 \times \mathbb{Z}/2)$: Either direct or $\text{Di}(\mathbb{Z}/4) = \mathbb{Q}$

$\mathbb{Z}/3 \times \mathbb{Z}/4$: Either direct or $\mathbb{Z}/3 \times \mathbb{Z}/4$
Read Along: Schick 1.8, 1.10, 1.11, 2.1.

Riddle Along: \( \sqrt{x^2+y^2} \) \( \begin{bmatrix} a \end{bmatrix} \) \( \bigwedge_{i=1}^{n} \) what do these solve?

Term Test. Material: everything; sample: see 2016.

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

**Semi-Direct Products.** Given \( N, H \) \& \( \phi: H \to \text{Aut}(N) \),

\[ N \rtimes H = \langle N \times H, (n_1, h_1), (n_2, h_2) = (n_1 \phi_h(n_2), h \cdot h_2) \rangle \]

**Big Example.** \( B_n = T(\langle (z^2-1)^{\infty} \rangle / \langle z \rangle ) = \frac{\mathbb{Z}}{\langle z \rangle} \)

\[ B_n = \langle 0, \ldots, 0, 1 \rangle \]

New class.

Some nice

\[ 1 \to B_n \to S_n \to \mathbb{Z}/n! \to 1 \]

\( PB_n = ke \mathbb{Z}/n! \)

\( PB_n \cap B_n \) yet not \( B_n = PB_n \times S_n \)

\( \rho: PB_n \to PB_{n-1} \)

Kepler: \( \rho = F_{n-1} \) and

\[ PB_n = F_{n-1} \times PB_{n-1} = F_{n-1} \times (F_{n-2} \times (\ldots \times (F_2 \times Z)) \ldots) \]

**Groups of order 21.** \( \mathbb{Z}/21, \mathbb{Z}/3 \times \mathbb{Z}/7 = \langle x, y \rangle \)

\[ \text{Aut}(\mathbb{Z}/21) = \mathbb{Z}/6 = \langle \phi_3 \rangle \]

\[ \phi_3(x) = x^3, \quad x^y = x \text{ or } x^3 \text{ or } x^9 \]

(iso: if \( x^3 = x^2 \) \& \( y = y^2 \) then \( x^5 = x^4 \)\)

**Groups of order 12.** If \( 16 = 12, \ p_1 = \mathbb{Z}/4 \) or \( (\mathbb{Z}/6) \)

and at least one of these is normal, for 4 \( Z_3 \) & 3 \( Z_4 \)’s. So \( G \) is a semi-direct product: \( \mathbb{Z}/4 \times \mathbb{Z}/3 \):

must be \( \mathbb{Z}/4 \times \mathbb{Z}/3 = \mathbb{Z}/12 \)

\[ (\mathbb{Z}/2 \times \mathbb{Z}/2) \times \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 \( A_4 \)

\[ 1, 2, 3, 4, 5, 6 \]

\[ (12)(34), (13)(24) \]

\[ \mathbb{Z}/3 \times (\mathbb{Z}/2 \times \mathbb{Z}/2): \text{ Either direct or } D_6 \times \mathbb{Z}/2 = D_6 \]

\[ \mathbb{Z}/3 \times \mathbb{Z}/4: \text{ Either direct or } D_3 \times \mathbb{Z}/4 \]

Done, but \( A_4 \) not yet.
Solvable Groups. Define a group $G$ to be solvable if all its quotients in its Jordan-Hölder series are Abelian.

**Theorem 1**. If $N \triangleleft G$, $G$ is solvable iff $N \triangleleft G/N$ are.

2. If $H \triangleleft G$ and $G$ is solvable, so is $H$.

\[ A \triangleright B \quad H \triangleright B \quad \forall \frac{H}{H \cap A} \rightarrow \frac{B}{A} \text{ by } [b]_{H \cap A} \rightarrow [b]_B \]

**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 $a \cdot 1 = 1 \cdot a = a \quad \forall a \in R$, and
4. $a \cdot (b + c) = a \cdot b + a \cdot c$ and $(a + b) \cdot c = a \cdot c + b \cdot c \quad \forall a, b, c \in R$.

**Examples.**

1. $\mathbb{Z}, R[X], M_{nn}(R)$
2. $\mathbb{Z} \rightarrow \mathbb{Z}/N$
3. $R \rightarrow M_{nn}(K)$ as $d_{xy}$
4. $(R, R[X]) \rightarrow R$ (if $R$ is commutative)
5. $M_{nn}(R[X]) \cong M_{nn}(R)[X]$
Solvable Groups. Def: G is solvable if all quotients in its Jordan-Holder series are Abelian.

Thm 1. IF N ⊆ G, G is solvable iff N \times G/N are.

2. IF H ⊆ G and G is solvable, so is H.

A \triangleleft B \Huge{\implies} A \triangleleft B 
\Huge{\implies} \frac{B}{A} \text{ by } [b]_{HA} \to [b]_A

is injective.

Cor. IF a group contains A_1, A_2, 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. Z, R[z], Mn(R)

More ISMs,

(Examples. 1. Z \rightarrow \mathbb{Z}/n
2. R \rightarrow R[z] + deg 0
3. R \rightarrow Mn(R) as deg
4. S, V a, R[z] \rightarrow k
   (if R is commutative)
\[ \text{(if } R \text{ is commutative)} \]
\[ \text{Let } \max(R[x]) = \max_n(R)[x] \]

im, subring, ker, ideal.

Q. Is every ideal a quotient.
Ans. Define \( R/I \).

Good luck w/ term test!
Subjects. 1. The NCCE story.

2. The isomorphism theorems.

3. Jordan Hölder, solvable groups.

4. Permutations, simplicity of $A_n$. $\checkmark$

5. $G$-sets.

6. The Sylow theorems, small examples $\checkmark$

7. Semi-direct products, braids. $\checkmark$

---

$(123)(245) = (12345)$ 1. Let $n$ be odd. Prove
$(123)(234) = (12)(34)$ that a subgroup of $S_n$,
$(12)(34)(12) = (1)(243)$ which contains $S_{4n}$
$(12)(34)(23)(45) = (12453)$ $(123) \not\sim (123... n)$ is
$(123)(345) \sim (124)$ An.

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

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

$H_1 \overset{\sigma}{\rightarrow} G/H_2$

$H_1 H_2 \rightarrow H_2 \in G/H_2$

$gH_2 \rightarrow H_1$
\[
\begin{align*}
\gamma_2 : & \longrightarrow H_1 \\
\gamma_1 : & \longrightarrow \bar{H}_1
\end{align*}
\]

3. Prove that the semi-direct product of two torsion-free groups is torsion-free.
2. Prove that there is no brand \( \beta \) s.t. \( \beta^n = e \).


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

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

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

1. Prove that there is a subgroup $P$ of $G$ whose order is $p^\alpha$. (You are not allowed to use the Sylow theorems, of course).

2. Suppose that $x \in G$ is an element whose order is a power of $p$, and suppose that $x$ normalizes $P$. Show that $x \in P$.

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

1. Prove that a semi-direct of two torsion free groups is again torsion free.

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

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

Problem 4.

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

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

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

Good Luck!
Further Thoughts

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

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

Marking up is always possible, but it is better done before the grades are first published, not after.

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

Problem 3:

\[ \Rightarrow \text{If } H_2 = \text{g}^{-1} H_1 g \]

\[ \Rightarrow \text{If } \phi : G/H_1 \rightarrow G/H_2 \text{ by } \psi(xH_1) = xgH_2 \]

1. Check well-defined: \( xh_1 H_1 \psi \rightarrow xh_1 g H_2 = xg h_1^g H_2 = xg H_2 \)
2. Check injectivity \( \text{1-set morphism} \).
3. Check surjectivity.

\[ \Rightarrow \text{IF } \phi : G/H_1 \rightarrow G/H_2 \text{ is an isomorphism,} \]

\[ \Rightarrow \phi(H_1) = g H_2 \text{ for some } g \]

\[ g H_2 = \phi(h_1 H_1) = h_1 g H_2 \Rightarrow g^{-1} h_1 g H_2 = g^{-1} H_2 \]

3. But also \( \phi^{-1}(g H_2) = H_1 \) so

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

So by analogy, \( g H_2 g^{-1} \subseteq H_1 \)

\[ \Rightarrow g^{-1} H_1 g = H_2 \]

\[ gx = y \Rightarrow x = g^{-1} y \]
People who haven't tried don't realize how hard learning may be, forcing you to confront your fears and insecurities (yet it is well worth it!). Try teaching (recommended!) and you'll see it's hard too. After more than 20 years I still make mistakes.

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

Goal. 1. Rings, ideals, isomorphisms.

2. Prime & maximal ideals, domains and fields.

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

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

Examples. $\mathbb{Z}, R[x], \text{Mat}_n(R)$

Morphisms,

- $\mathbb{Z} \to \mathbb{Z}/n$
- $R \to R[x]$, $\text{deg } 0$
- $\text{if } R \text{ is commutative}$
- $\text{Mat}_n(R)[x] \cong \text{Mat}_n(R)[x]$.

Im, subring, ker, ideal.

Q. Is every ideal a quotient?

Ans. Define $R/I$.

The Isomorphism Theorems. 1. $f : R \to S = R/\ker(f) \cong \text{im } f$.

2. $A + I \cong A/I$, $A \subset R$ subring, $I \subset R$ ideal.

3. $I \cap R/I$ ideals $\cong R/I \cong R/J$

4. Given an ideal $I$ of $R$, there's a bijection between ideals $I \subset J \subset R$ and ideals of $R/I$. 
November 1, hours 22-23: Ideals, isomorphism theorems, prime and maximal ideals

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

Read Along. Select 2.1-2.3.

HW3 on web.

Def. \( I \subset R \) is an ideal.

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

Q. Is every ideal a quotient?

Ans. Define \( R/I \).

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

The Isomorphism theorems.

1. \( F: R \to S \Rightarrow R/\ker F \cong \text{im } F. \)

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

2. \( A + I \cong \frac{A}{A + I} \). \( A \subset R \) subring, \( I \subset R \) ideal.

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

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

Better rings. 1. The ultimate:

- Field [commutative, for a group, almost all of high-school & freshman algebra carries through]

- "Division ring", if not commutative

  (Example: \( \mathbb{H} = \{ a + b i + c j + d k : i^2 = j^2 = k^2 = -1, ij = k \} \) useful for 3D rotations, etc...)
2. (Integral) domains: commutative, has no 0-divisors.

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

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

Maximal Ideals. 1. Definition.

2. J ⊆ R is maximal ⇔ R/I is a field.

Fishy proof: Use the 4th isomorphism theorem.

Honest proof: ⇒: xJ ∩ I = Rx + I = R ⇒ ∃y ∈ R xy + I = 1 + I

⇐ J ⊆ I , x ∈ J \ I ⇒ ∃y ∈ R xy - 1 ∈ I ⇒ 1 ∈ J

Examples. 1. pZ is a maximal ideal in Z.

2. $S = \{ \sum (a_i) : a_i \in \mathbb{R} \}$

Theorem. Every ideal is contained in a maximal ideal.

Proof using Zorn’s Lemma.

Theorem. There exists a function

$L_{\text{in}} : \{ \text{bndd seqs} \} \rightarrow \mathbb{R}$ s.t.

1. If $(a_n)$ is convergent, $\lim_{n \to \infty} a_n = L_{\text{in}}(a_n)$.

2. $\lim_{n \to \infty} (a_n + b_n) = \lim_{n \to \infty} (a_n) + \lim_{n \to \infty} (b_n)$ + more...

3. $\lim_{n \to \infty} (a_n b_n) = \lim_{n \to \infty} (a_n) \cdot \lim_{n \to \infty} (b_n)$

Proof.

$S = \{ \text{bndd seqs in } \mathbb{R} \}$
$I = \{ (a_n) : \text{finitely many } a_n \neq 0 \}

J - a \text{ maximal ideal containing } I.

$L_{\text{in}} : S \rightarrow S/J \cong \mathbb{R}$
Prime Ideals. 1. Definition \( \mathfrak{p} \subseteq R \) is prime if \( ab \in \mathfrak{p} \implies a \in \mathfrak{p} \ or \ b \in \mathfrak{p} \).

2. Theorem. \( R/\mathfrak{p} \) is a domain iff \( \mathfrak{p} \) is prime.

Proof: \( \implies \) \( ab \in \mathfrak{p} \implies [ab] = 0 \implies [a][b] = 0 \implies \mathfrak{p}/\mathfrak{p} = 0 \implies a + \mathfrak{p} \in \mathfrak{p} \).

\( \leq \) \( [a][b] = 0 \implies [ab] = 0 \implies ab \in \mathfrak{p} \implies a + \mathfrak{p} \in \mathfrak{p} \implies [a] = 0 \implies b + \mathfrak{p} \in \mathfrak{p} \implies [b] = 0 \).

Theorem. A maximal ideal is prime.
November 3, hour 24: Prime and maximal ideals

1. Next class on Tuesday. Read Along: Selick 2.1-2.3

Riddle Along: $g(x) = x$

Agenda: “better ideals.”

... from now on, $R$ is commutative.

Maximal Ideals.

1. Definition.

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

Example. $S = \{ f(x) \in \mathbb{R}[x] \mid a_n = 0 \}$

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

Proof using Zorn’s Lemma.

Theorem. There exists a function $\lim : \{ \text{bounded seqs in } \mathbb{R} \} \rightarrow \mathbb{R}$ s.t.

1. If $(a_n)$ is convergent, $\lim a_n = \lim a_n$.

2. $\lim (a_n + b_n) = \lim (a_n) + \lim (b_n)$ + more...

3. $\lim (a_n b_n) = \lim (a_n) \cdot \lim (b_n)$

Proof. $S = \{ \text{bounded seqs in } \mathbb{R} \mid I = \{ (a_n) \mid a_n \text{ converges} \}$

$J$ - a maximal ideal containing $I$.

$\lim : S \rightarrow S/J = \mathbb{R}$
Prime Ideals. 1. Definition $P \in R$ 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. $\Rightarrow$: $ab \in P \Rightarrow [ab] = 0 \Rightarrow [a][b] = 0 \Rightarrow a \not\in P$ or $b \not\in P$.

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

Theorem. A maximal ideal is prime.

From this point, $R$ is a domain (no zero-divisors).

Primes. 1. $a \mid b \Rightarrow (a, b) = (a) \Rightarrow a = u_b$.

2. $\gcd(a, b) = 1 \Rightarrow \gcd(a) = 1$ and $\gcd(b) = 1 \Rightarrow 1 = u_a u_b$.

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

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

4. Irreducible $x = a \mid b \Rightarrow a \in R^* \lor b \in R^*$.

Claim. prime $\Rightarrow$ irreducible

   Counterexample: in $\mathbb{Z}[\sqrt{-5}]$, $2$ is irreducible (no norm reasons) but not prime, as $2 \mid (1 + \sqrt{-5})(1 - \sqrt{-5}) = 6$.
\[ S = \{ \text{bounded seqs in } \mathbb{R} \}, \quad \mathbb{I} = \{ (a_n) : \text{finite, very nice} \} \]

Let \( J \) be a maximal ideal containing \( \mathbb{I} \).

**Theorem:** \( S \to S/J \to \mathbb{R} \) extends \( \lim \).

**Definition:** Say that \( A \in \mathbb{N} \) is "essential" if \( 1_A \notin J \).

**Claim:** \( \{ A : A \text{ is essential} \} = \mu \) is a non-principal ultrafilter on \( \mathbb{N} \).

**Proof:** \( J \) is prime \( \implies (A, B, EM \implies A \lor B, EM) \)

\( N, E, M \) because \( 1_S = 1_N \) is not in \( J \).

\( A \in N \supseteq 1_A \notin J \iff (1_N - 1_A) \in J \iff 1_A \in E, 1_A \in F \iff A \in F \).  

Monotonically because \( J \) is an ideal: \( A \subseteq B \Rightarrow B \in E \Rightarrow 1_A = 1_B \cdot 1_A \in J \Rightarrow A \notin \mu \).

Principality from the definition of \( J \).

**Definition:** \( J = \{ (a_n) : \forall E > 0, \{ n : |a_n| < E \} \text{ is essential} \} \)

**Claim:** \( J = J \)

**Proof:** Suppose \( (a_n) \in J \) and \( E > 0 \) is such that \( \{ n : |a_n| < E \} \) is essential.

Let \( b_n = \begin{cases} \frac{1}{n} & \text{if } |a_n| < E, \\ 0 & \text{otherwise}. \end{cases} \)
Then $a_n b_n = 1$ on an essential set,
so $\overline{a_n} \neq 0$, so $\overline{a_n} \neq 0$ so $a_n \not\in J = \mathbb{F}$.

Now by the maximality of $J$, $J = \mathbb{F}$.

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

(follows from convergence on ultrafilters)

$\Rightarrow \lim (a_n) = \lim (\alpha \mathbb{F})$

**Claim.** The map $\mathbb{R} \to S/\mathbb{F}$ via $x \mapsto x \mathbb{F}$

is injective and surjective.

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

$\Rightarrow$ using $x \mapsto x \mathbb{F}$ to identify $S/\mathbb{F}$ with $\mathbb{R}$, the resulting $\lim$ has all the required properties. $\square$
November 10, hour 25: Primes, UFDs, One Theorem Two
Corollaries Four Weeks

Local goal. Prime Ideals & Primes

1T2CYW: \( M \) f.g. over a PID \( R \) \( \Rightarrow \) uniquely

\[ M \cong R^k \oplus \bigoplus_{i} R/\langle p_i \rangle \quad p_i \text{ prime} \quad s_i > 1 \]

Euclidean \( \Rightarrow \) PID \( \Rightarrow \) UFD

Conclusion

Cor 1. A f.g. Abelian \( \Rightarrow \)

Cor 2. A \& \text{Man}(C) has a "Jordan Form"

Read Also. Click 2.2, 2.7, (2.8, 2.9)

Battfish link or push

Did: Maximal & prime ideals, fields & domains.

\( R \) is a commutative integral domain. "\( a,b \) are associates"

Primes 1. \( a|b \quad (a|b \land b|a \Rightarrow a=b) \)

2. \( \gcd(a, b) = 1 \quad \text{gcd} = q \land \gcd = q' \Rightarrow q = uq' \)

3. Primes: \( p \neq 0 \text{ non-units} \quad p | a \cdot b \Rightarrow p | a \text{ or } p | b \)

\( p \) is prime iff \( \langle p \rangle \) is prime ideal.

4. Irreducible \( X = \alpha \cdot b \Rightarrow \alpha \in \text{nil}_X \lor b \in \text{nil}_X \)

Claim. prime \( \Rightarrow \) irreducible

\( p = \alpha \cdot b \Rightarrow p | \alpha = \Rightarrow \alpha = p \cdot c \)

\( = \Rightarrow p = p \cdot c \Rightarrow c = 1 \Rightarrow b \in \text{nil}_X \)

counterexample: in \( \mathbb{Z}[\sqrt{-5}] \)

2 is irreducible (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.

Pr: In a UFD, prime \( \Leftrightarrow \) irreducible.

pr: If an irreducible is decomposed, the decomposition must have length 1.

Thm. UFD \( \Leftrightarrow \) over \( x \neq 0 \) y has a unique decomposition.
into irreducibles. If x is irreducible, then x = \prod_{i=1}^{n} p_i is prime. If x is irreducible, then x = \prod_{i=1}^{n} p_i is prime.

Thm. In a UFD gcd's always exist.
HW3 due, HW4 on Web soon.

Child goal: $M$ fg. module over a PID $R \Rightarrow$ uniquely

$M \cong R^k \oplus \bigoplus R/p_{i1}^{s1}$

Cor. 1. A fg. Abelian $\Rightarrow A \cong \mathbb{Z}^k \oplus \bigoplus \mathbb{Z}/p_{i1}^{s1}$

Cor. 2. $A \in \text{Mat}(n, C)$ has a "Jordan Form"

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

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

Thm. Uniqueness up to units b a permutation.

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

PE If an irreducible is decomposed, the decomposition must have length 1.

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

Def. In a UFD, $x = x_1 \cdots x_k$ $\Rightarrow x_{i1} \cdots x_{ik} = x_{i1} \cdots x_{ik}$

Thm. In a UFD gcd's always exist.

How show UFD? $\forall m \Rightarrow \text{Norm} \Rightarrow \text{PID} \Rightarrow$ UFD.

Def. Euclidean domain: has a "norm" $\epsilon: R \setminus \{0\} \rightarrow \mathbb{N}$ s.t.

1. $\epsilon(ab) \geq \epsilon(a)$
2. $\forall a, b \in R$ s.t. $a = qb + r$ $\Rightarrow r = 0$ or $\epsilon(r) < \epsilon(b)$

Example: 1. $\mathbb{Z}$

Example $\frac{a}{b} = \frac{x^3 - 2x^2 - 5x + 12}{x^2 + 1}$ $\Rightarrow a(i) = 14 - 6i$

Thm. A Euclidean domain is a "PID" (UFD).

(Thm: a PID is a UFD, btw.)

Theorem. A Euclidean domain is a "PID" (UFD).

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

PF. $I = \langle p \rangle$ prime, $I \subset J \subset R \Rightarrow p = a \in J$ $\Rightarrow (a \in R^* \Rightarrow I = J) \lor (x \in R^* \Rightarrow J = R)$
Take $x = x_1$, unless $x_1 \neq R^*$, $x_1 \in M_1$, where $M_1$ is a maximal ideal containing $<x_1>$. $M_1 = <p>$.

$x_1$ prime. So $x_1 = p_1 x_2$; unless $x_2 \neq R^*$, $x_2 \in M_2$, maximal $M_2 = <p_2>$, $x_2 = p_2 x_3, \ldots$ if process was infinite,

$<x_1> \not= <x_2> \not= <x_3> \not= \ldots$

Put a PID is “Noetherian”,

So the process must terminate.

So $x = x_1 = p_1 x_2 = p_1 p_2 x_3 = \ldots = p_1 p_2 \ldots p_n \in$ R.

Theorem. In a PID $<a, b> = <gcd(a, b)>$. (so gcd($h, b$) = $a + bh$)

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

If $<a, b> = <b>$, take $(s, t) = (0, 1)$. Otherwise

$a = bq + r$, $e(r) < e(b)$,

$<a, b> = <b, r>$ so if $g = s' b + t' r$, then

$g = s' b + t' (a - bq) = t' a + (s' - t' q) b$

Theorem. R is a PID iff it has a “Dedekind-Hasse” norm: $d: R \{-0\} \to \mathbb{N}_{\geq 0}$ [or add $d(0) = 0$]

s.t. if $a, b$ to either $a < b$ or $\exists 0 \neq x \in a < b$

w/ $d(a) < d(b)$.

Pf. $\in$ as before, $\Rightarrow$ replace every prime by 2, get

even a “multiplicative” D-H norm.

If time: Modules, $Z, \mathbb{V}, T: \mathbb{V} \to \mathbb{V}$.
The ring of modules

Let $M \in \mathbb{R}^k \oplus \mathbb{R}^{p,\mathbb{R}}$.

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

Today, the "ring" of modules.

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

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

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


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

5. Column vectors $R^n$ over $M_{nm}$ (left module $R$-mod),
row vectors $(R^n)^\text{T}$ over $M_{nm}$ (right module $m\text{od}-R$).

Def/Claim. $R$-mod & $m\text{od}-R$ are categories.

Def/Claim. Submodules, $\ker \phi, \text{Im } \phi, M/N$.

Boring Theorems.
1. $\phi: M \rightarrow N$ $\Rightarrow$ $M/\ker \phi \cong \text{Im } \phi$

2. $A, B \subseteq M$ $\Rightarrow$ $A + B \cong A/\mathcal{E} B$

3. $A \mathcal{E} B \subseteq M$ $\Rightarrow$ $M/A \mathcal{E} B \cong M/B$

4. Also dull.

Direct sums. $M \oplus N$.

\[ M \quad \oplus \quad N \]

\[ M \quad \oplus \quad N \quad \oplus \quad \ldots \]

\[ M \quad \oplus \quad N \quad \oplus \quad \ldots \]

\[ M \quad \oplus \quad N \quad \oplus \quad \ldots \]
\[
\left( \begin{array}{ccc}
M & \otimes & N \\
\oplus & \oplus & \oplus \\
\text{sum} & \text{sum} & \text{sum}
\end{array} \right) \rightarrow \left( \begin{array}{c}
M \otimes N \\
\rightarrow & \rightarrow \\
\text{N product} & \text{N product}
\end{array} \right) \rightarrow \prod_{i \in I} \text{N product}
\]

Differ for infinite families!

\[
\text{Hom}(\bigoplus N_i, \bigoplus M_i) = \left\{ (a_{ij})_{i \in I} : a_{ij} \in \text{Hom}(M_i, N_j) \right\}
\]

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

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

\[
\frac{\mathbb{R}}{\langle a \rangle} \oplus \frac{\mathbb{R}}{\langle b \rangle} \cong \frac{\mathbb{R}}{\langle ab \rangle} \text{ via } \frac{R}{\langle a \rangle} \oplus \frac{\mathbb{R}}{\langle b \rangle} \cong \frac{R}{\langle ab \rangle} \cong \left( \begin{array}{c}
\mathbb{R} \\
\mathbb{R} \\
\mathbb{R}
\end{array} \right) \cong \mathbb{R}^3
\]

\( \mathbb{Z} \oplus \mathbb{Z} \oplus \mathbb{Z} \cong \mathbb{Z}^3 \oplus \mathbb{Z} \cong \mathbb{Z} \mathbb{Z}^3 \cong \mathbb{Z} \) \text{ “the chinese remainder theorem.”}

\text{...}
November 22, hours 29-30: Proof of the Structure Theorem - Existence

**Goal:** The existence part, $\mathbb{R}^n$ "ring" of modules.

**Read Along:** You tell me.

Let $R$ be a PID...

**Sketch**

$\text{Matrices} \xrightarrow{\text{row}} \text{modules}$

*Proof by induction* & more

*But the induction is just a nuisance.*

So we're back to Gaussian elimination.

**Def** $M$ is "finitely generated" if $\exists j_1, ..., j_r \in M$ s.t.

\[ M = \left\{ \sum a_i \mathbf{e}_{j_i} : a_i \in R \right\} \]

\[ R^X \xrightarrow{\text{A}} R^9 \xrightarrow{\text{T}} M \]

**Claim:** If $A, Q$ are invertible on the left, then

\[ M = R^9 / \text{im} A \]

\[ M' = R^9 / \text{im} A \]

are isomorphic.
If $\Phi: \mathbf{M} \rightarrow \mathbf{M}'$ by $[x]_{\text{im} A} \rightarrow [x]_{\text{im} A'}$, then $A'$ can be interpreted as a $g \times g$ matrix $Q$ can be interpreted as an $X \times X$ column-finite matrix: $A' = PAQ$

... can do arbitrary 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 $a_{ii}$.

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

(1) for a Euclidean domain.

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

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

$\Rightarrow$ w.l.o.g., the row & column of $a_{ii}$ are $0$ (except for $a_{ii}$)

$\Rightarrow$ all entries of $A$ are divisible by $a_{ii}$.

\[ A = \begin{pmatrix} a_{ii} & \scriptstyle{\text{divisible}} \\ \text{0} & \scriptstyle{\text{all entries}} \end{pmatrix} \]

Continue to get $A^n$ \[ \begin{pmatrix} a_{ii} & \text{divisible} \\ 0 & \text{divisible} \end{pmatrix} \] (wlog, $A$ is square)
Continue to get $M = \left( \begin{array}{c} \cdot \\ \cdot \\ 0 \end{array} \right)$ (is square)

So $M = \bigoplus_{i=1}^{g} R/a_i \cong R^g \oplus R/a_1$

$\alpha_1, \alpha_2, \ldots, \alpha_n$

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

Then $R/a \oplus R/b \cong R/a \oplus R/b$. Aside: $R/67 \oplus R/97 \cong R/67 \oplus R/97 \cong \mathbb{Z}_{1,001}$

Proof 1. as before, use the Chinese Remainder Theorem.

Proof 2. Using the techniques above, $(a, b) \sim (9, 69) \Box$

Recall that $(R, +, \cdot)$ is an "Abelian group" (really, an additive semigroup, and even a semi-group, and even a group, and even a ring)

Tensor Products. Given $M, N$

$M \otimes R : N = \sum_{i=1}^{n} a_i (n_1 \otimes n_2) : n_1, n_2 \in R$ \,(bilinear)

$M \times N$

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

Example. If $q \equiv g \equiv (a, b)$, $R/a \oplus R/b \cong R/<q>$

PF. $[r]_a \oplus [r]_b \rightarrow [r] \cdot [r]_b$ \,$[a] \oplus [b] = [4 + 2c] \oplus [4] = 0$

$[c]_a \rightarrow [c]_a \otimes [c]_b$ \,$[c]_a \otimes [c]_a = [c]_a [c]_a$

Theorem. $(R, \cdot, \oplus, \otimes)$ is a "Ring".

Theorem. $(M, N) \rightarrow M \otimes N$ is a "bifunctor".
November 24, hour 31: The "ring" of modules

1. Tensor Products. Given $M, N$

$$M \otimes_{k} N = \{ \sum_{i} a_i (n_i, \alpha_i) : \text{new}, \alpha_i \in k^2 \} / \sim$$

where

- $(\alpha \cdot m, n \cdot \beta) = m \otimes n \cdot (\alpha, \beta)$
- $m \otimes n = n \otimes m$
- $(m_1 + m_2) \otimes n = m_1 \otimes n + m_2 \otimes n$
- $m \otimes (n_1 + n_2) = m \otimes n_1 + m \otimes n_2$

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

Example. If $q \in \mathbb{Q}, \langle a, b \rangle, \frac{R}{q} \otimes \frac{R}{q} \cong \frac{R}{q^2}$

Proof.

- $[r] \otimes [s] \rightarrow [r \cdot s]$ where $[s] = [a + b \cdot q, b]$
- $[r, s] = [a + b \cdot q, b]$
- $[r] \otimes [s] = [a + b \cdot q, b]$
- $[r, s] = [a + b \cdot q, b]$

Theorem. $(R, +, 0, \cdot, \otimes, 0, R)$ is a "ring".

Theorem. $(M, N) \rightarrow \text{Hom}(M \otimes N)$ is a "bifunctor".

Theorem. The universal property.

$$\text{bilin} : M \otimes N \rightarrow \text{Hom}(M \otimes N)$$
November 29, hours 32-33: Uniqueness

\( \frac{\text{Uniqueness}}{\text{Goal}} \)

HW 4 due, HW 5 & last week's schedule on web.

Riddle solutions. \( \infty \), Möbius. Nov29Riddles.png:

Tensor Products. Given \( M, N \):

\[
M \otimes_k N := \left\{ \sum_{i=1}^{n} a_i (m_i \otimes n_i) : m_i \in M, n_i \in N, a_i \in k \right\}
\]

Example. If \( q = gcd(a, b) \),

\[
\frac{\mathbb{R}}{\langle a \rangle} \otimes \frac{\mathbb{R}}{\langle b \rangle} \sim \frac{\mathbb{R}}{\langle q \rangle}
\]

Proof. \([r]_a \otimes [r]_b \rightarrow [r \cdot r]_q \) well-def.: \([q]_q [l]_q = [l]_q \cdot [l]_q = 0\)

\([r]_a \otimes [l]_b \leftarrow [r]_q \) Inverseness:

\([r]_q \otimes [l]_q = [l]_q \cdot [r]_q\)

Theorem. \((R, \cdot, 0, 1, R)\) is a "ring".

Theorem. The universal property.

\[
M \times N \xrightarrow{\text{bilinear}} M \otimes N \\
\text{bilinear} \downarrow \rho \in \mathcal{F}(G)
\]

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

Example. \( \mathbb{Q} \otimes \mathbb{Z} \mathbb{N} \equiv \mathbb{Q} \mathbb{N} \), "Extension of scalars".

In general, given \( \phi: R \rightarrow S\) a ring morphism, \( S\) is an \( R\) module by set \( M_S := S \otimes_R M\). Then \( M_S\) is an \( S\) module and \( R_S = S^\mathbb{N} \).
Prop. For any domain \( R \) there is a unique field \( Q(R) \) s.t. \( R \rightarrow Q(R) \) “The field of fractions”

Proof later.

Claim: If \( M \) is torsion \( \forall m \in M \exists r \in R \text{ such that } rm = 0 \) then \( M \text{ is torsion} = 0 \).

Prop. If \( M \cong R^k \oplus \prod R/<p_i> \), then

1. \( \dim_{Q(R)} M_{Q(R)} = k \)
2. \( \dim_{R/<p>} M_{R/<p>} = k + \left| \{ i : p_i \nmid p \} \right| \)
3. \( \dim_{R/<p>} \text{im}(m \mapsto p^s m)_{R/<p>} = k + \left| \{ i : p_i \nmid p \text{ and } s \leq s_i \} \right| \)

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: \( R \setminus \{0\} \), \( R \setminus \{p\} \) (\( p \text{ prime}) \), Powers of \( a \neq 0 \).

Definition: \( S^{-1}R = \left\{ \frac{r}{s} \right\} \) such that \( r,s \in S \) if \( r_1s_1 = r_2s_2 \)

\[
\frac{r_1}{s_1} = \frac{r_2}{s_2} \Rightarrow \frac{r_1s_2}{s_1} = \frac{r_2s_1}{s_2} \Rightarrow \frac{\frac{r_1}{s_1}}{\frac{s_2}{s_1}} = \frac{\frac{r_2}{s_2}}{\frac{s_1}{s_2}} \Rightarrow \frac{r_1s_2}{s_1} = \frac{r_2s_1}{s_2} = \frac{r_2}{s_2} \Rightarrow \frac{r_1}{s_1} = \frac{r_2}{s_2} \Rightarrow \frac{r_1s_2}{s_1} = \frac{r_2s_1}{s_2} \Rightarrow R \setminus \{0\} = \text{ “field of fractions } Q(R) \text{”} \]

\( R \setminus \{p\} \text{ “localization at } p \text{”} \)

\( R \rightarrow S^{-1}R \) is injective.
Abelian groups & the mult. groups of finite fields

\[ A \cong \mathbb{Z}^k \oplus \mathbb{Z}_{\beta_1} \oplus \mathbb{Z}_{\beta_2} \oplus \ldots \]
\[ \frac{\alpha_1}{\alpha_2/\alpha_3} \ldots \]

Theorem: If \( F \) is finite, \( F^* \) is cyclic.

Proof: Otherwise, \( x^{\text{deg}(f)} - 1 \) has too many roots.

(Aside: \( \lambda \) is a root of \( f \in F[x] \Rightarrow x-\lambda \mid f \), so \( f \) may have at most \( \deg(f) \) roots)
**Theorem.** \((R_{-\text{mod}}, \oplus, \otimes, 0, R)\) is a "ring." \(\checkmark\)

**Theorem.** \(M_1 \rightarrow \otimes N\) is a "bifunctor." \(\checkmark\)

**Theorem.** The universal property.

\[
\begin{align*}
M \times N &\xrightarrow{\text{lilin}} M \otimes N \\
&\text{bilin} \\
&\bullet \\
&\rightarrow P \subset \mathcal{F}
\end{align*}
\]

**Example.** \(\mathbb{Q} \otimes \mathbb{Z} \cong \mathbb{Q}\) as an \(R\)-module.

"Extension of scalars." \(\checkmark\)

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

---

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

\[
\begin{align*}
\mathbb{R} &\rightarrow Q(R) \\
\text{a field} &\rightarrow F
\end{align*}
\]

"The field of fractions" Proof later.

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

\[
\forall m \in M, \exists r \in R, rm = 0 \implies 0 = 0
\]

Prop. If \(M = R^k \oplus \left< R/\langle p_1, \ldots, p_i \rangle \right>\), then

1. \(\dim_{Q(R)} M_{Q(R)} = k\) \(\checkmark\)

2. \(\dim_{R/p} M_{R/p} = k + \left| \{i : p_i \nmid p_j\} \right| \) \(\checkmark\)

3. \(\dim_{R/\langle p \rangle} \operatorname{im}(m_{R/p} \rightarrow p^m)_{R/K} = k + \left| \{i : p_i \nmid p \text{ & } s = s_i\} \right|\) \(\checkmark\)
Localization & Fields of Fractions. Let \( R \) be a commutative domain.

Define a multiplicative subset \( S \) of \( R \setminus \{0\} \) (contains 1, closed under \( \times \)).

Examples: \( R \setminus \{0\} \), \( R \setminus \{0\} \) (if prime), powers of \( a \neq 0 \).

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

\[ \frac{r_1}{s_1} \sim \frac{r_2}{s_2} \text{ if } r_1s_2 = r_2s_1 \]

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

\( R \setminus \{0\} \) — "localization at \( \mathbb{Z} \)"

\([2^n]\) — "dyadic rationals".

Abelian groups & The mult. groups of finite fields

\[ A \cong \mathbb{Z}^k \oplus \bigoplus_{i=1}^n \mathbb{Z}_{a_i} \oplus \mathbb{Z}_{a_i}^\times \oplus \mathbb{Z}_{a_i}^\times \]

\[ a_1 \mid a_2 \mid a_3 \]

Theorem: If \( F \) is finite, \( F^* \) is cyclic.

Proof: Otherwise, \( x^{a_1} - 1 \) has too many roots.
Discuss the Find!

Goal. \( M = R^k \oplus \frac{R}{<p_i>}, \) Uniqueness & Corollaries.

Reminder. In a PID, \( \frac{R<x> \oplus \frac{R}{<b>}}{<gcd(x,b)>} \)

Prop. If \( M \cong R^k \oplus \frac{R}{<p_i>}, \) then

1. \( \dim_{R(x)} M_{R(x)} = k \)
2. \( \dim_{R<\alpha, \beta>} M_{R<\alpha, \beta>} = k + \left\lfloor \frac{1}{|i : \alpha \mid \beta \mid} \right\rfloor \)
3. \( \dim_{R<\alpha, \beta>} M_{R<\alpha, \beta>} = k + \left\lfloor \frac{1}{|i : \alpha \mid \beta \mid S \leq S_i} \right\rfloor \)

So such a decomposition is unique! \( \square \) [Though not “canonical”]

\( F[x] \) and the J.C.F. \( T:V \rightarrow V \) makes \( V \) an \( F[x]-R \)

module, so \( \sqrt{S} = R^k \oplus \frac{R}{<p_i>}. \) As \( f(T) = 0 \)

for some \( F, k=0. \) IF \( F \) is alg. close, \( P_i = x-\lambda_i \)

Q. What does \( F[x] \)

\[ \frac{1}{x-\lambda} \cdot (x-\lambda)^2 \cdot \cdots (x-\lambda)^s \]

look like as a vector space?

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

\( T-\lambda \) acts by “shift to the right” \( \begin{pmatrix} 0 & 0 \\ 1 & 0 \end{pmatrix} \)

So \( T \) acts by \( \begin{pmatrix} 1 & a \\ 0 & 1 \end{pmatrix} \)
Corollary 2. Over an algebraically closed field $\mathbb{F}$, every square matrix $A$ is conjugate to a block diagonal matrix $B = \begin{pmatrix} B_1 & 0 & \cdots & 0 \\ 0 & B_2 & \cdots & 0 \\ \vdots & \vdots & \ddots & \vdots \\ 0 & 0 & \cdots & B_n \end{pmatrix}$, where each $B_i$ is either a $1 \times 1$ matrix $(\lambda_i)$ for some $\lambda_i \in \mathbb{F}$, or an $s_i \times s_i$ matrix with $\lambda_i$'s on the diagonals, 1's right below the diagonal, and 0's elsewhere.

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

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

(Corollary: good old diagonalization.)

Challenge.

Open all the boxes!

Find an algorithm to find $B_j$ if the same.

At least when all $\lambda_i$'s are different as the one you learned in junior high?
Plan. UFO blender; JCF abstractly & in practice.

I said “I think in a UFO every prime ideal is maximal.”

JCF. \( V \) a f.d. v.s.; \( A : V \to V \) linear, makes \( V \) a module over \( \mathbb{F}[x] \) via \( xu = Au \). Then

\[
V \cong \bigoplus \mathbb{F}[x]/(x-\lambda_i) \langle v_i \rangle.
\]

UFO blender. The above statement is nonsense.

In \( \mathbb{Q}[x, y] = \mathbb{Q}[x][y] \), \( \langle x \rangle \) is prime

but not maximal.

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

\( x-\lambda \) acts by “shift to the right \( \begin{pmatrix} 0 & 0 & \cdots & 0 \\ 1 & 0 & \cdots & 0 \\ \vdots & \ddots & \ddots & \vdots \\ 0 & \cdots & 1 & 0 \end{pmatrix} \)"

so \( A \) acts by \( \begin{pmatrix} \lambda_i & \cdots & 0 \\ 1 & \lambda_i & \cdots \\ \vdots & \ddots & \ddots \\ 0 & \cdots & 1 & \lambda_i \end{pmatrix} \)

Now let’s do that in practice...

Step 1. Find a presentation matrix for \( V \in \mathbb{R}^{\text{mod}} \).

w.l.o.g. \( V = \mathbb{F}^n \) and \( A \in \text{Mat}_n(\mathbb{F}) \).

Corollary 2. Over an algebraically closed field \( \mathbb{F} \), every square matrix \( A \) is conjugate to a block diagonal matrix \( B = \begin{pmatrix} B_1 & 0 & \cdots & 0 \\ 0 & B_2 & \cdots & 0 \\ \vdots & \ddots & \ddots & \vdots \\ 0 & \cdots & 0 & B_s \end{pmatrix} \)

where each \( B_i \) is either a \( 1 \times 1 \) matrix \( (\lambda_i) \) for some \( \lambda_i \in \mathbb{F} \), or an \( s_i \times s_i \) matrix with \( \lambda_i \)'s on the diagonals, \( 1 \)'s right below the diagonal, and \( 0 \)'s elsewhere,

\[
\begin{pmatrix}
\lambda_i & 0 & \cdots & 0 \\
1 & \lambda_i & \cdots & 0 \\
0 & \cdots & 1 & \lambda_i \\
0 & \cdots & 0 & 1 & \lambda_i
\end{pmatrix}
\]

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.)

We want to know if \( \langle x \rangle \) is 1-1; it is enough to show that \( \beta \) is onto \( x \) i.e., that any \( x^k e_i \) can be written, modulo \( \langle x \rangle \),
As a combination of \( \mathbf{e}_i \)'s. Indeed,

\[
x^{k-1} \mathbf{e}_i = x^{k-1} (x \mathbf{e}_i) = x^{k-1} \mathbf{A} \mathbf{e}_i = \ldots = \mathbf{A}^{k-1} \mathbf{e}_i
\]

Go over handout, first in the distinct-eigenvals case.

Row and Column Operations

Row operations are performed by left multiplying \( N \times N \) by some properly-positioned \( 1 \times 2 \) matrix and at the same time left multiplying the \( (N+1) \times (N+1) \) matrix. Column operations are similar, with left replaced by right and \( P \) by \( Q \).

Swapping Rows and Columns

\[
\begin{align*}
\text{SwapRows} & : \text{Row}[1, 1] \rightarrow \text{Row}[1, 1] \oplus \text{Row}[2, 1] \\
\text{SwapColumns} & : \text{Col}[1, 1] \rightarrow \text{Col}[1, 1] \oplus \text{Col}[2, 1] \\
\text{SwapPlaces} & : (\text{Row}[1, 1], \text{Col}[1, 2]) \rightarrow (\text{Row}[1, 1], \text{Col}[1, 2])
\end{align*}
\]

Recovering \( C \) from \( \mathbf{P} \)

\[
\begin{align*}
\mathbf{M} & \xrightarrow{J} \mathbf{X} \xrightarrow{A} \mathbf{F} \\
\mathbf{Q} & \xrightarrow{J} \mathbf{X} \xrightarrow{B} \mathbf{F} \xrightarrow{T_J(B)} \mathbf{F} \\
\mathbf{C} & = \mathbf{Z} \mathbf{B}^k \mathbf{P} \mathbf{e}_i \quad \text{complete run!}
\end{align*}
\]

The "Jordan Trick":

Then go through run 2

\( \ldots \) done line

Theorem. The universal property for tensor products.

1. Holds 2. Determines \( \mathbf{M} \otimes \mathbf{N} \)

up to a unique isomorphism.
Debits.

Polynomials over a UFO make a UFO.

Lang page 180-193 — mostly a discussion of contents.

Unboxing.

1. Fix the UFO blunder

2. Complete the "abstract" JCF story.

3. Do the computational JCF story following the handout.

   a. The presentation matrix.

   b. Reductions. (handout really only does this part.

   c. Reading off the end result.
Abelian groups & The multi. groups of finite fields

\[ A \cong \mathbb{Z}^k \oplus \mathbb{Z} \oplus \mathbb{Z}^\infty \cong \mathbb{Z} \oplus \mathbb{Z} \oplus \mathbb{Z} \oplus \mathbb{Z} \oplus \ldots \]

\[ a_1 \oplus a_2 \oplus a_3 \oplus \ldots \]

**Theorem.** If \( F \) is finite, \( F^* \) is cyclic.

**Proof.** Otherwise, \( x^{a_1} - 1 \) has too many roots.

(Aside: \( \lambda \) is a root of \( f \in F[x] \iff \lambda \in \mathbb{F}, \) so \( f \) may have at most \( \deg(f) \) roots)

---

Theorem. The universal property for tensor products.

\[ \begin{array}{c}
M \times N \\
\text{bilinear} \rightarrow \\
\text{bilinear} \rightarrow \end{array} \leftarrow \begin{array}{c}
M \otimes N \\
F \end{array} \]

---

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

**Proof I.** Substitute \( t = A \), so \[ t(tI - A) = nt - tA \]

So \[ nA - tA_1 = 0 \]

So all matrices are diagonal.

**Proof II.** Recall that any matrix \( B \) has an "adjoint" \( B^* \) such that \( B^*B = BB^* = \det(B)I \). Then

\[ (tI - A)^* (tI - A) = X_A(t)I \]

as \( \det \) of \( M_{m \times n}(R) \) & \( \sum B_k t^k \)
There is a well-defined \( \chi_A : C_A[t] \to C_A[t] \) applying to both sides, get

\[
(\sum B_k A^k) \cdot (A - A) = \chi_A(A) I
\]
\[
\begin{pmatrix}
1 & 0 \\
0 & \rho^2
\end{pmatrix}
\sim
\begin{pmatrix}
\rho & 0 \\
1 & \rho
\end{pmatrix}
\Rightarrow
\begin{pmatrix}
1 & 0 \\
\rho & -\rho^2
\end{pmatrix}
\Rightarrow
\begin{pmatrix}
1 & 0 \\
0 & \rho^2
\end{pmatrix}
\]
\[
\begin{pmatrix}
\rho & 0 \\
1 & \rho^2
\end{pmatrix}
\rightarrow
\begin{pmatrix}
0 & -\rho^n \\
1 & \rho^{n-1}
\end{pmatrix}
\rightarrow
\begin{pmatrix}
0 & -\rho \\
1 & 0
\end{pmatrix}
\rightarrow
\begin{pmatrix}
1 & 0 \\
0 & \rho^n
\end{pmatrix}
\]
\[
\begin{pmatrix}
\rho^{n-1} & 0 \\
1 & \rho
\end{pmatrix}
\rightarrow
\begin{pmatrix}
\rho^{n-1} & -\rho \\
1 & 0
\end{pmatrix}
\rightarrow
\begin{pmatrix}
0 & -\rho \\
1 & 0
\end{pmatrix}
\rightarrow
\begin{pmatrix}
1 & 0 \\
0 & \rho
\end{pmatrix}
\]
\[
\mathbb{Q}
\begin{pmatrix}
1 & 0 \\
0 & 1
\end{pmatrix}
\rightarrow
\begin{pmatrix}
1 & -\rho \\
0 & 1
\end{pmatrix}
\]
\[
\text{row:}
\begin{pmatrix}
1 & 0 \\
0 & 1
\end{pmatrix}
\rightarrow
\begin{pmatrix}
1 - \rho^{n-1} \\
0 & 1
\end{pmatrix}
\rightarrow
\begin{pmatrix}
0 & 1 \\
1 + \rho^{n-1}
\end{pmatrix}
\]
\[
\Rightarrow
\begin{pmatrix}
1 & 0 \\
0 & \rho^n
\end{pmatrix}
= \begin{pmatrix}
0 & 1 \\
-1 & \rho^{n-1}
\end{pmatrix}
\begin{pmatrix}
0 & 1 \\
\rho^n & 0
\end{pmatrix}
\begin{pmatrix}
1 & 0 \\
0 & 1
\end{pmatrix}
\]