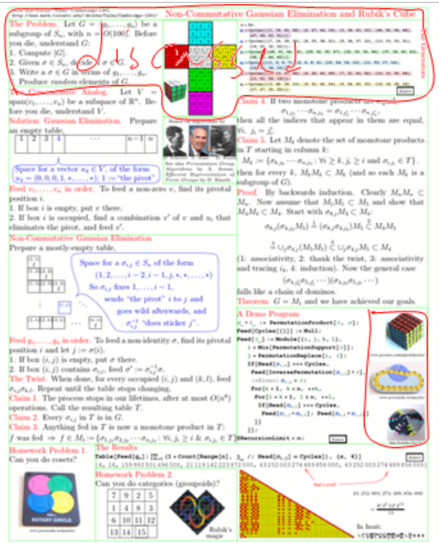
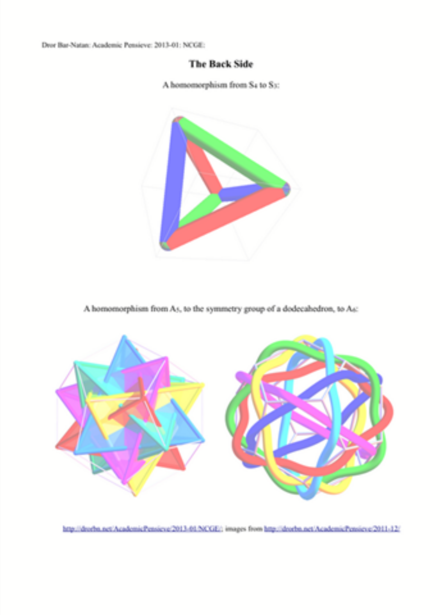
This is Dror Bar-Natan's 2025-26 MAT 347 personal notebook (A). It is publically available but it comes with no guarantees whatsoever. Its content may or may not be correlated with the actual class content.

Hours 1-2 on Wednesday September 3: The NCGE handout and the very basics of groups.



Non-Commutative Gaussian Elimination and Rubik's Cube

discussed



Dror Bar-Natan: Academic Pensieve: 2013-01: NCGE:

The Back Side

A homomorphism from S_4 to S_3:

A homomorphism from A_5, to the symmetry group of a dodecahedron, to A_5:

http://drorbn.net/AcademicPensieve/2013-01/NCGE/; images from http://drorbn.net/AcademicPensieve/2011-12/

+ Def of a group

uniqueness of e

Uniqueness of g^{-1}

Cancellation

$(ab)^{-1} = b^{-1}a^{-1}$

Examples $\mathbb{Z}, \mathbb{Q}, \mathbb{R}, \mathbb{C}, 2\mathbb{Z}, V$

$\mathbb{Q}^\times, \mathbb{R}^\times, \mathbb{C}^\times, F^\times$

The Rubik's cube

S_n, [ ] notation

$S($  $)$

$O(3)$

25-347 Hour 3 on Fri Sep 5: More NCGE.
Must check on Wed morning: http://drorbn.net/25-347 → It's a tough class!
The syllabus is still not public!
Say hello to Jacob, wish luck to Matt!
Permutation product is "usual" composition! → $\sigma \cdot \tau = \sigma \circ \tau$

Goal: within your lifetime, understand

$G = \langle g_1 \dots g_\alpha \rangle \subset S_n$:

1. $|G| = ?$ 2. $\sigma \in G$?

3. write $\sigma \in G$ in terms of $g_1 \dots g_\alpha$

4. Random σ.

on board!

Classical row reduction as in handout.

Describe the NCGE algorithm as in handout.

Claim 0. The process ends after at most n^6 steps. Call the resulting table T.

done line.

Claim 1 Every σ_{ij} in T is in G.

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

Claim 3 If two monotone products are equal,

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

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

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

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

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

$$\overset{3}{=} \cup_j \sigma_{4,j}(M_5M_5) \overset{4}{\subset} \cup_j \sigma_{4,j}M_5 \subset M_4$$

(1: associativity, 2: thank the twist, 3: associativity and tracing i_4, 4: induction). Now the general case

$$(\sigma_{4,j'_4}\sigma_{5,j'_5}\cdots)(\sigma_{4,j_4}\sigma_{5,j_5}\cdots)$$

falls like a chain of dominos.

Theorem. $G = M_1$ and we have achieved our goals.

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

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

on board (minus fills)

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

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

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

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

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

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

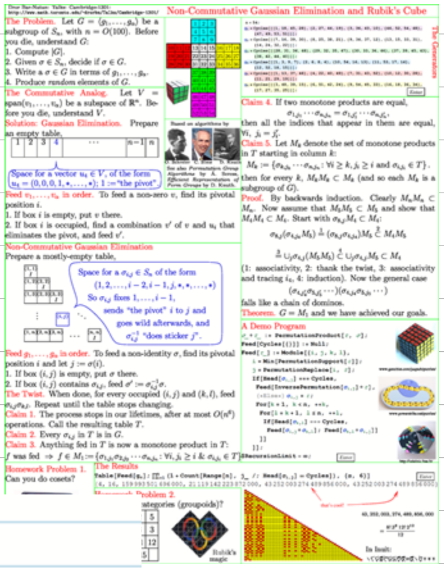
Feed $\sigma_{23}\sigma_{13} = 4132$ .. to σ_{14}

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

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

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

25-347 Hours 4-5 on Wed Sep 10: More NCGE.
Say hello to Matt!
A^{-1}^{-1}=a.



Dror Bar-Natan: Talks: Cambridge-1301:
http://www.math.toronto.edu/~drorbn/Talks/Cambridge-1301/

Non-Commutative Gaussian Elimination and Rubik's Cube

The Problem. Let $G = \langle g_1, \ldots, g_\alpha \rangle$ be a subgroup of S_n, with $n = O(100)$. Before you die, understand G:
1. Compute $|G|$.
2. Given $\sigma \in S_n$, decide if $\sigma \in G$.
3. Write a $\sigma \in G$ in terms of $g_1, \ldots, g_\alpha$.
4. Produce *random* elements of G.

The Commutative Analog. Let $V = \mathrm{span}(v_1, \ldots, v_\alpha)$ be a subspace of $\mathbb{R}^n$. Before you die, understand V.

Solution: Gaussian Elimination. Prepare an empty table.

1	2	3	4	⋯	n−1	n

Space for a vector $u_4 \in V$, of the form $u_4 = (0,0,0,1,*,\ldots,*)$; 1 :="the pivot".

Feed $v_1, \ldots, v_\alpha$ in order. To feed a non-zero v, find its pivotal position i.
1. If box i is empty, put v there.
2. If box i is occupied, find a combination v' of v and u_i that eliminates the pivot, and feed v'.

Non-Commutative Gaussian Elimination
Prepare a mostly-empty table,

Space for a $\sigma_{i,j} \in S_n$ of the form $(1, 2, \ldots, i-2, i-1, j, *, *, \ldots, *)$
So $\sigma_{i,j}$ fixes $1, \ldots, i-1$, sends "the pivot" i to j and goes wild afterwards, and $\sigma_{i,j}^{-1}$ "does sticker j".

Feed $g_1, \ldots, g_\alpha$ in order. To feed a non-identity σ, find its pivotal position i and let $j := \sigma(i)$.
1. If box (i,j) is empty, put σ there.
2. If box (i,j) contains $\sigma_{i,j}$, feed $\sigma' := \sigma_{i,j}^{-1}\sigma$.

The Twist. When done, for every occupied (i,j) and (k,l), feed $\sigma_{i,j}\sigma_{k,l}$. Repeat until the table stops changing.

Claim 1. The process stops in our lifetimes, after at most $O(n^6)$ operations. Call the resulting table T.

Claim 2. Every $\sigma_{i,j}$ in T is in G.

Claim 3. Anything fed in T is now a monotone product in T:
f was fed $\Rightarrow f \in M_1 := \{\sigma_{1,j_1}\sigma_{2,j_2}\cdots\sigma_{n,j_n} : \forall i, j_i \geq i \;\&\; \sigma_{i,j_i} \in T\}$

Based on algorithms by
C. Schreier C. Sims D. Knuth
See also *Permutation Group Algorithms* by A. Seress, *Efficient Representation of Perm Groups* by D. Knuth.

The Generators

Claim 4. If two monotone products are equal,
$$\sigma_{1,j_1}\cdots\sigma_{n,j_n} = \sigma_{1,j_1'}\cdots\sigma_{n,j_n'},$$
then all the indices that appear in them are equal, $\forall i,\ j_i = j_i'$.

Claim 5. Let M_k denote the set of monotone products in T starting in column k:
$$M_k := \{\sigma_{k,j_k}\cdots\sigma_{n,j_n} : \forall i \geq k, j_i \geq i \text{ and } \sigma_{i,j_i} \in T\}.$$
then for every k, $M_kM_k \subset M_k$ (and so each M_k is a subgroup of G).

Proof. By backwards induction. Clearly $M_nM_n \subset M_n$. Now assume that $M_5M_5 \subset M_5$ and show that $M_4M_4 \subset M_4$. Start with $\sigma_{8,j}M_4 \subset M_4$:
$$\sigma_{8,j}(\sigma_{4,j_4}M_5) \overset{1}{=} (\sigma_{8,j}\sigma_{4,j_4})M_5 \overset{2}{\subset} M_4M_5$$
$$\overset{3}{=} \cup_j\sigma_{4,j}(M_5M_5) \overset{4}{\subset} \cup_j\sigma_{4,j}M_5 \subset M_4$$
(1: associativity, 2: thank the twist, 3: associativity and tracing i_4, 4: induction). Now the general case
$$(\sigma_{4,j_4'}\sigma_{5,j_5'}\cdots)(\sigma_{4,j_4}\sigma_{5,j_5}\cdots)$$
falls like a chain of dominos.

Theorem. $G = M_1$ and we have achieved our goals.

A Demo Program

```
σ_ * τ_ := PermutationProduct[τ, σ];
Feed[Cycles[{}]] := Null;
Feed[σ_] := Module[{i, j, k, l},
  i = Min[PermutationSupport[σ]];
  j = PermutationReplace[i, σ];
  If[Head[σ_{i,j}] =!= Cycles,
   Feed[InversePermutation[σ_{i,j}] * σ],
   (*Else*) σ_{i,j} = σ;
   For[k = 1, k ≤ n, ++k,
    For[l = k + 1, l ≤ n, ++l,
     If[Head[σ_{k,l}] === Cycles,
      Feed[σ_{i,j} * σ_{k,l}]; Feed[σ_{k,l} * σ_{i,j}]]
    ]];
  ]];
$RecursionLimit = ∞;
```

Homework Problem 1.
Can you do cosets?

The Results

```
Table[Feed[g_s]; ∏_{i=1}^{n} (1 + Count[Range[n], j_ /; Head[σ_{i,j}] == Cycles]), {s, 6}]
{4, 16, 159993501696000, 21119142223872000, 43252003274489856000, 43252003274489856000}
```

Homework Problem 2.
…ategories (groupoids)?

Rubik's magic

43,252,003,274,489,856,000

In bsuit:

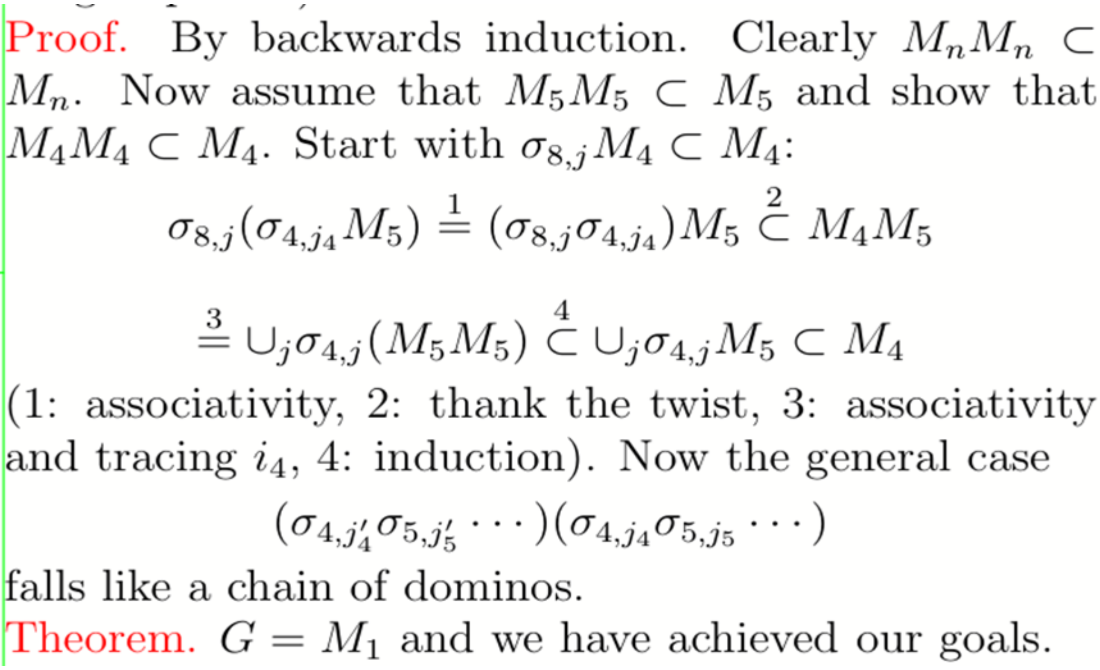
Go over home page and "About".
Review NCGE handout to the building of T.

Claim 1 Every σ_{ij} in T is in G.

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

Claim 3 If two monotone products are equal, $\sigma_{1j_1}\cdots\sigma_{nj_n} = \sigma_{1j_1'}\cdots\sigma_{nj_n'}$ then all the indices are equal, $\forall i\ j_i = j_i'$.

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



Proof. By backwards induction. Clearly $M_nM_n \subset M_n$. Now assume that $M_5M_5 \subset M_5$ and show that $M_4M_4 \subset M_4$. Start with $\sigma_{8,j}M_4 \subset M_4$:
$$\sigma_{8,j}(\sigma_{4,j_4}M_5) \overset{1}{=} (\sigma_{8,j}\sigma_{4,j_4})M_5 \overset{2}{\subset} M_4M_5$$
$$\overset{3}{=} \cup_j\sigma_{4,j}(M_5M_5) \overset{4}{\subset} \cup_j\sigma_{4,j}M_5 \subset M_4$$
(1: associativity, 2: thank the twist, 3: associativity and tracing i_4, 4: induction). Now the general case
$$(\sigma_{4,j_4'}\sigma_{5,j_5'}\cdots)(\sigma_{4,j_4}\sigma_{5,j_5}\cdots)$$
falls like a chain of dominos.

Theorem. $G = M_1$ and we have achieved our goals.

Example $\sigma_1 = \underset{2314}{\underset{\shortparallel}{(123)}}$ $\sigma_2 = \underset{2143}{\underset{\shortparallel}{(12)(34)}}$, in S_4

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

on board (minus fills)

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.

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

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

25-347 Hour 6 on Fri Sep 12: More NCGE, homomorphisms.
HW01 is on Crowdmark. Do you see it? Can you submit it?
Tutorials today! 1-2 at WO30 with Jacob and 2-3 at FE213 with Matt

Alt. date for TT1:

	Tue	Thu	Mon	Tue	Wed	Thu
	Nov 4 (Kills reading week)	6	10	11	12	13
objections				27		

Show the animation!

1. $T \subset G$ Def $M_K = \{\sigma_{Kj_K}\sigma_{K+1,j_{K+1}}\cdots\sigma_{nj_n}\}$

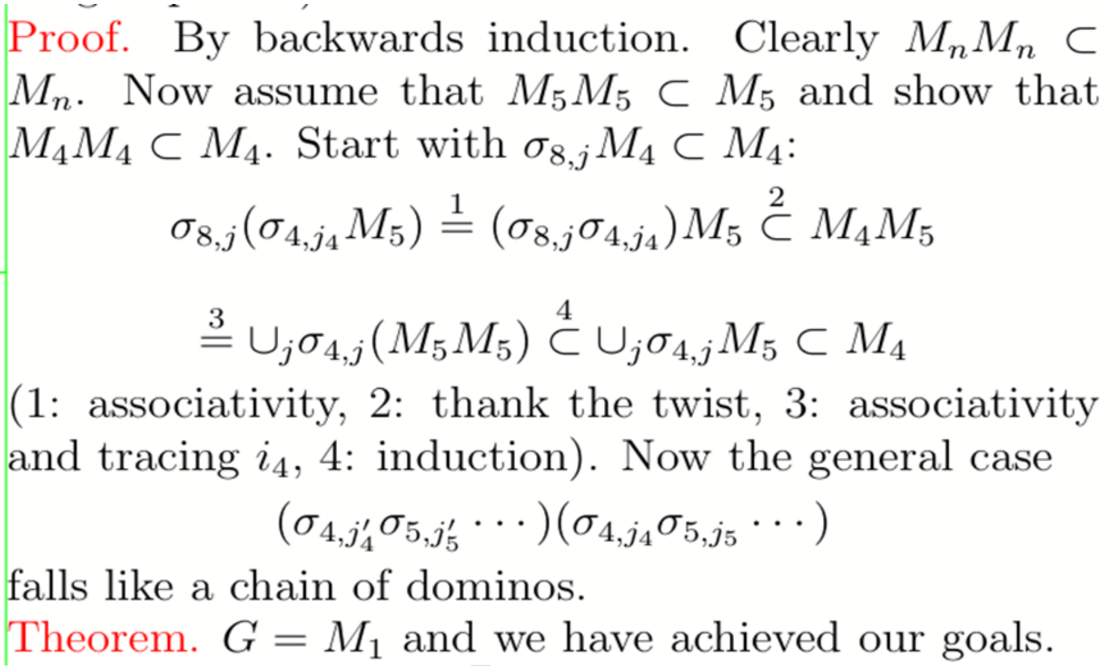
2. Anything fed is now a monotone product in M_1

3. Monotone products are unique.

Thm $M_K \circ M_K \subset M_K$, so M_K is a subgroup of S_n.

Cor $M_1 = G$ and our work is done.   bend line.

Pf of Thm


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

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

$$\overset{3}{=} \cup_j \sigma_{4,j}(M_5M_5) \overset{4}{\subset} \cup_j \sigma_{4,j}M_5 \subset M_4$$

(1: associativity, 2: thank the twist, 3: associativity and tracing i_4, 4: induction). Now the general case

$$(\sigma_{4,j_4'}\sigma_{5,j_5'}\cdots)(\sigma_{4,j_4}\sigma_{5,j_5}\cdots)$$

falls like a chain of dominos.

Theorem. $G = M_1$ and we have achieved our goals.

If time: 1. homomorphisms

Examples: $\mathbb{Z} \to \mathbb{R}$! exp, esp. $e^{2\pi i t}$; $S_4 \to S_3$.

2. "groups make a category"

3. isomorphisms, ker, im both are subgroups.

25-347 Hours 7-8 on Wed Sep 17: Homomorphisms, quotients, isomorphism theorems.
We need a blackboard shots volunteer!
HW01 is due on Friday!

Def $\varphi: G \to H$ is a homomorphism means board line

1. $\varphi(x \cdot y) = \varphi(x)\varphi(y)$
2. $\varphi(e_G) = \varphi(e_H)$
3. $\varphi(x^{-1}) = \varphi(x^{-1})$

$\iff \varphi(xy^{-1}) = \varphi(x)\varphi(y)^{-1}$

Examples: $\mathbb{Z} \to \mathbb{R}$! exp, esp. $e^{2\pi i t}$; $S_4 \to S_3$.

2. "groups make a category"

3. isomorphisms, $\mathrm{Aut}(G)$

$(g_1 g_2)^h = g_1^h g_2^h$

4. Conjugation $g^h = h^{-1} g h = C_h(g)$ $g^{h_1 h_2} = (g^{h_1})^{h_2}$

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

5. ker, im both are subgroups. $\ker < G$ $\mathrm{im} < H$

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

Normal Subgroups $N \triangleleft G$, Kernels are normal.

Q Is every normal subgroup the kernel of a morphism?

Given $N \triangleleft G$, can we find a surjective morphism $\phi: G \to H$ with $\ker \phi = N$?

Set theoretic aside: surjections are the same as equivalence relations. [define, explain]

done line

wishful thinking

Sol'n: $g_1 \sim g_2$ [$\iff \phi(g_1) = \phi(g_2) \iff \phi(g_1^{-1} g_2) = e$]

$\iff g_1^{-1} g_2 \in N \iff g_2 \in g_1 N \iff g_1 N = g_2 N$

Let $H = G/N = \{[g]\}$ where $[g] = gN \underset{\substack{\uparrow \\ !}}{=} Ng$

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

Define $[g_1][g_2] = [g_1 g_2]$

$[g]^{-1} = [g^{-1}]$ well defined ?

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

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

Proof Construct

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

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

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

25-347 Hours 9 on Fri Sep 19: Quotients, isomorphism theorems.
TT1 moves to Nov 4! HW02 is online HW01 is due at 11:59pm!

Can you do it with 4?

Def $N \triangleleft G$ means $N < G$ and $\forall h \in G$ $N^h = h^{-1}Nh = N$.

Claim If $\varphi: G \to H$, $\ker\varphi \triangleleft G$.

Q Given $N \triangleleft G$, is there a surjective $\phi: G \to H$ with $\ker\phi = N$?

Aside surjections are the same as equivalence relations. [define, explain]

Sol'n: $g_1 \sim g_2 \; \big[\Leftrightarrow \phi(g_1) = \phi(g_2) \Leftrightarrow \phi(g_1^{-1}g_2) = e \big]$ wishful thinking

$\Leftrightarrow g_1^{-1}g_2 \in N \Leftrightarrow g_2 \in g_1N \Leftrightarrow g_1N = g_2N$

Let $H = G/N = \{[g]\}$ where $[g] = gN \underset{\uparrow !}{=} Ng$

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

Define $[g_1][g_2] = [g_1g_2]$
$[g]^{-1} = [g^{-1}]$ well defined?

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

done line

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

Proof Construct $R: \longrightarrow$ by $[g] \longrightarrow \phi(g)$
$L: \longleftarrow$ by $h \longmapsto [g]$ with $\phi(g) = h$.

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

25-347 Hours 10-11 on Wed Sep 24: Isomorphism theorems.
Finished Monday: http://drorbn.net/Theta

$G/N := \{gN : g \in G\}$. If $N \triangleleft G$, $(g_1N)\cdot(g_2N) = g_1g_2N$ makes it a group.

Example $\mathbb{Z}/n\mathbb{Z}$ aka $\mathbb{Z}/n$

Aside If $H < G$, $|G| = |G/H| \cdot |H|$, and so $|G/H| \mid |G|$ & $|H| \mid |G|$ "Lagrange's thm"

$(G:H)$, the index of H in G

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

Proof Construct $R : \longrightarrow$ by $[g] \longrightarrow \phi(g)$

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

2^{nd} Iso preview: $H, K < G$, $H \subset N_G(K) \Rightarrow HK/K \cong H/H\cap K$.

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

Pf $\Leftarrow$ $(h_1k_1)(h_2k_2) = h_1h'k'k_2$ $\quad (hk)^{-1} = k^{-1}h^{-1} = h'k'$

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

Def

$C_G(X) := \{g \in G : \forall x \in X,\ xg = gx\}$ "The centralizer of X in G"

$Z(G) := C_G(G)$ "The centre"

$N_G(X) := \{g \in G : Xg = gX\}$ "The normalizer of X in G"

All are subgroups $\nabla_<$

Examples $G_0 = \{\pm 1, \pm i\}$

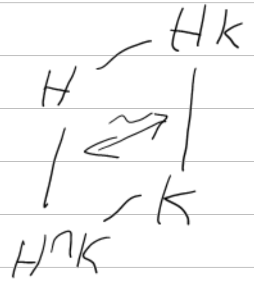
$G = \{\pm 1, \pm i, \pm j, \pm k\}$ "The unit quaternions"

$C_G(\{\pm 1, \pm i\}) = \{\pm 1\}$ $\quad Z(G) = \{\pm 1\}$ $\quad N_G(G_0) = G$

The 2nd Isomorphism Thm If $H, K < G$, $H < N_G(K)$,

Then $HK = KH$, $K \triangleleft HK$, $H \cap K \triangleleft H$, and

$$HK/K \cong H/H \cap K$$



done line

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

The 3rd Isomorphism Thm: If $K, H \triangleleft G$ and $K < H$,

then $\dfrac{G/K}{H/K} \cong G/H$.

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

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

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

The 4th Isomorphism Thm If $N \triangleleft G$ then $\pi : G \to G/N$

induces a "faithful" between subgroups of G/N and

$\{H : N < H < G\}$: * $A < B \iff \pi(A) < \pi(B)$ [and then, $(B:A) = (\pi(B):\pi(A))$]

* $A \triangleleft B \iff \pi(A) \triangleleft \pi(B)$ * $\pi(A \cap B) = \pi(A) \cap \pi(B)$

25-347 Hour 12 on Fri Sep 26: More isomorphism theorems.
HW2 is due 11:59pm; HW3 is online.

The 2nd isomorphism Thm If $H, K < G$, $H < N_G(K)$, Then $HK = KH$, $K \lhd HK$, $H \cap K \lhd H$, and

$$HK/K \cong H/H\cap K$$

$$\begin{tikzcd} & HK \\ H \arrow[ur, dash] \arrow[r, phantom, "\cong"] & \\ & K \arrow[uu, dash] \\ H\cap K \arrow[uu, dash] \arrow[ur, dash] & \end{tikzcd}$$

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

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

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

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

$[g_1]_K [g_2]_K^{-1} = [h]_K \implies g_1 g_2^{-1} = hk = h'$

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

- $A < B \iff \pi(A) < \pi(B)$ $\left[\begin{array}{l}\text{and then,}\\ (B:A) = (\pi(B):\pi(A))\end{array}\right]$
- $A \lhd B \iff \pi(A) \lhd \pi(B)$
- $\pi(A \cap B) = \pi(A) \cap \pi(B)$

If time: simple groups

$\mathbb{Z}/n$ simple iff n is prime.

sign σ and A_n

Thm A_n is simple.

25-347 Hours 13-14 on Wed Oct 1: Iso 4, simple groups, Jordan-Holder.

Pick up a handout!

Iso 1: $\phi: G\to H$ $\quad G/\ker\phi \cong \operatorname{im}\phi$

Iso 2 $H,K<G$, $K^H=K$ $\quad \frac{H}{H\cap K} \cong \frac{KH}{K}$

Iso 3 $A\triangleright B$, $A \triangleright C$, $B\triangleright C$ $\quad \frac{A/C}{B/C} \cong A/B$

board line

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

- $A<B \iff \pi(A)<\pi(B)$ [and then, $(B:A)=(\pi(B):\pi(A))$]
- $A\triangleleft B \iff \pi(A)\triangleleft\pi(B)$ $\quad$ ⁂ $\pi(A\cap B)=\pi(A)\cap\pi(B)$

simple groups

subgroups of $\mathbb{Z}$: $n\mathbb{Z}$.

$\mathbb{Z}/n\mathbb{Z}$ simple $\iff$ no $n\mathbb{Z}\subsetneq m\mathbb{Z}\subsetneq\mathbb{Z}$; no m s.t. $m|n$.

$\mathbb{Z}/n$ simple iff n is prime.

$$\operatorname{sign}\sigma=(-1)^\sigma = \text{parity of }\sigma = \operatorname{sign}\prod_{i<j}(\sigma i-\sigma j) = \prod_{i<j\le n} s_{ij}(\sigma)$$

$$(-1)^{\sigma\tau} = \operatorname{sign}\left[\prod_{\{i,j\}} \frac{\sigma\tau i-\sigma\tau j}{\tau i-\tau j}\cdot\frac{\tau i-\tau j}{i-j}\right] \quad \text{w/ } s_{ij}(\sigma)=\frac{\sigma i-\sigma j}{i-j}$$

$$=(-1)^\sigma(-1)^\tau$$

Every permutation is a product of transpositions.

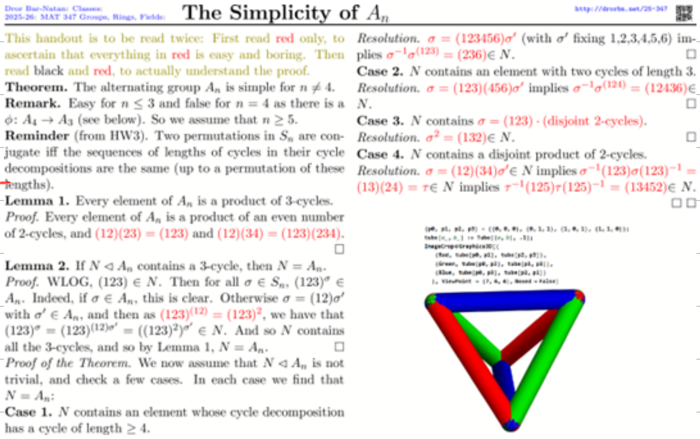
The parity is the parity of the number of transpositions.

Def A_n

Claim $A_n\triangleleft S_n$ (how do I know) don't

Thm A_n is simple. /handout. handout red can be assumed.

If time: state Jordan-Holder.



Dror Bar-Natan: Classes: 2025-26: MAT 347 Groups, Rings, Fields:

The Simplicity of A_n

http://drorbn.net/25-347

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 is simple for $n\neq 4$.

Remark. Easy for $n\le 3$ and false for $n=4$ as there is a $\phi: A_4\to A_3$ (see below). So we assume that $n\ge 5$.

Reminder (from HW3). Two permutations in S_n are conjugate iff the sequences of lengths of cycles in their cycle decompositions are the same (up to a permutation of these lengths).

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

Proof. Every element of A_n is a product of an even number of 2-cycles, and $(12)(23)=(123)$ and $(12)(34)=(123)(234)$. □

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

Proof. WLOG, $(123)\in N$. Then for all $\sigma\in S_n$, $(123)^\sigma\in A_n$. Indeed, if $\sigma\in A_n$, this is clear. Otherwise $\sigma=(12)\sigma'$ with $\sigma'\in A_n$, and then as $(123)^{(12)}=(123)^2$, we have that $(123)^\sigma=(123)^{(12)\sigma'}=((123)^2)^{\sigma'}\in N$. And so N contains all the 3-cycles, and so by Lemma 1, $N=A_n$. □

Proof of the Theorem. We now assume that $N\triangleleft A_n$ is not trivial, and check a few cases. In each case we find that $N=A_n$:

Case 1. N contains an element whose cycle decomposition has a cycle of length ≥ 4.

Resolution. $\sigma=(123456)\sigma'$ (with σ' fixing 1,2,3,4,5,6) implies $\sigma^{-1}\sigma^{(123)}=(236)\in N$. □

Case 2. N contains an element with two cycles of length 3.

Resolution. $\sigma=(123)(456)\sigma'$ implies $\sigma^{-1}\sigma^{(124)}=(12436)\in N$. □

Case 3. N contains $\sigma=(123)\cdot(\text{disjoint 2-cycles})$.

Resolution. $\sigma^2=(132)\in N$. □

Case 4. N contains a disjoint product of 2-cycles.

Resolution. $\sigma=(12)(34)\sigma'\in N$ implies $\sigma^{-1}(123)\sigma(123)^{-1}=(13)(24)=\tau\in N$ implies $\tau^{-1}(125)\tau(125)^{-1}=(13452)\in N$. □ □

25-347 Hour 15 on Fri Oct 3: Iso 4, Simplicity of An, Jordan-Holder.

Pick up a handout!

Thm A_n is simple / handout

Red is done!

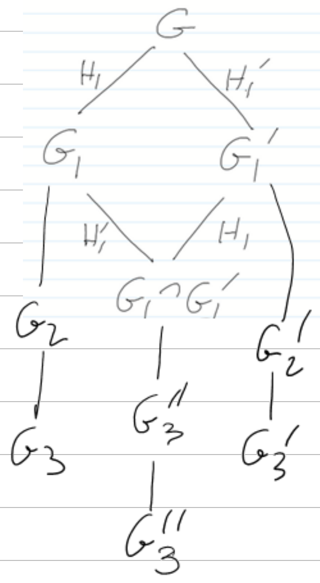
The Jordan-Hölder Theorem. Let G be a finite group. Then there exist a sequence $G=G_0 \triangleright G_1 \triangleright G_2 \triangleright \dots \triangleright G_n=\{e\}$ s.t. $H_i = G_i/G_{i-1}$ is simple. Furthermore, the sequence (H_i), the "composition series" of G, is unique up to a permutation. $4 \to A_4 \to A_3$

Example 2 $\underset{24}{S_4} \triangleright \underset{12}{A_4} \triangleright \underset{4}{\{(12)(34), (13)(24), (14)(23)\}} \triangleright \underset{2}{(12)(34)} \triangleright \{e\}$

Proof by induction on $|G|$.

Existance: Let G_1 be a maximal normal proper subgroup.

Uniqueness: Use the "diamond principle":

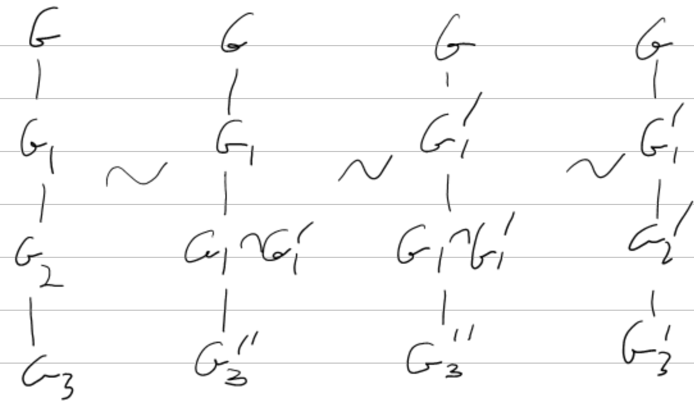


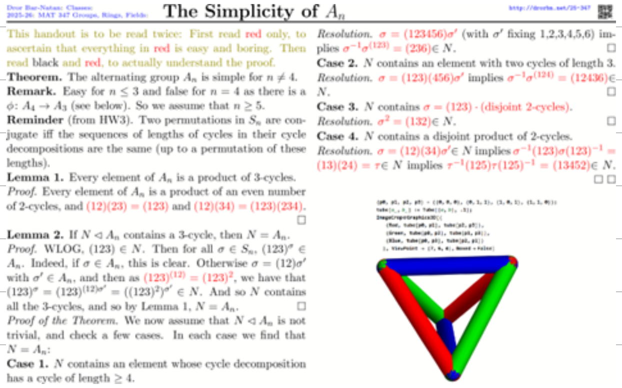
$G \triangleright G_1 \triangleright G_2 \dots$

$G \triangleright G_1' \triangleright G_2' \dots$

Claim $G = G_1G_1'$

Pf G_1G_1' is normal in G yet bigger that G_1, G_1'.





Dror Bar-Natan: Classes:
2025-26: MAT 347 Groups, Rings, Fields:

The Simplicity of A_n

http://drorbn.net/25-347

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 is simple for $n \neq 4$.

Remark. Easy for $n \leq 3$ and false for $n = 4$ as there is a $\phi\colon A_4 \to A_3$ (see below). So we assume that $n \geq 5$.

Reminder (from HW3). Two permutations in S_n are conjugate iff the sequences of lengths of cycles in their cycle decompositions are the same (up to a permutation of these lengths).

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

Proof. Every element of A_n is a product of an even number of 2-cycles, and $(12)(23) = (123)$ and $(12)(34) = (123)(234)$. ☐

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

Proof. WLOG, $(123) \in N$. Then for all $\sigma \in S_n$, $(123)^\sigma \in A_n$. Indeed, if $\sigma \in A_n$, this is clear. Otherwise $\sigma = (12)\sigma'$ with $\sigma' \in A_n$, and then as $(123)^{(12)} = (123)^2$, we have that $(123)^\sigma = (123)^{(12)\sigma'} = ((123)^2)^{\sigma'} \in N$. And so N contains all the 3-cycles, and so by Lemma 1, $N = A_n$. ☐

Proof of the Theorem. We now assume that $N \triangleleft A_n$ is not trivial, and check a few cases. In each case we find that $N = A_n$:

Case 1. N contains an element whose cycle decomposition has a cycle of length ≥ 4.

Resolution. $\sigma = (123456)\sigma'$ (with σ' fixing 1,2,3,4,5,6) implies $\sigma^{-1}\sigma^{(123)} = (236) \in N$. ☐

Case 2. N contains an element with two cycles of length 3.

Resolution. $\sigma = (123)(456)\sigma'$ implies $\sigma^{-1}\sigma^{(124)} = (12436) \in N$. ☐

Case 3. N contains $\sigma = (123) \cdot (\text{disjoint 2-cycles})$.

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

Case 4. N contains a disjoint product of 2-cycles.

Resolution. $\sigma = (12)(34)\sigma' \in N$ implies $\sigma^{-1}(123)\sigma(123)^{-1} = (13)(24) = \tau \in N$ implies $\tau^{-1}(125)\tau(125)^{-1} = (13452) \in N$. ☐ ☐

Example 1 $\mathbb{Z}/n$. The key: suppose $n = p_1 \cdots p_k$, a product of primes.

$$\mathbb{Z} \triangleright p_1\mathbb{Z} \triangleright \underbrace{p_1p_2\mathbb{Z}}_{m} \triangleright \dots \triangleright n\mathbb{Z}$$

$$\frac{m\mathbb{Z}}{mp_3\mathbb{Z}} \cong \mathbb{Z}/p_3\mathbb{Z}$$

Example 3: for $n \geq 5$ $S_n \triangleright A_n \triangleright \{e\}$

Examples 1–3 done, J-H thm not even stated.

25-347 Hours 16-17 on Wed Oct 8: group actions.

on side BB:

Example 1 $n=p_1 \dots p_k$

$\mathbb{Z}/n \rhd p_1\mathbb{Z}/n \rhd p_1p_2\mathbb{Z}/n \dots \rhd \{e\}$

Example 2

$S_4 \rhd A_4 \rhd (\mathbb{Z}/2)^2 \rhd \mathbb{Z}/2 \rhd \{e\}$

Example 3 $n \geq 5$ $S_n \rhd A_n \rhd \{e\}$

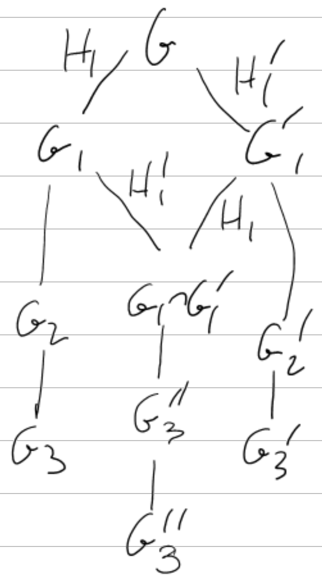
The Jordan-Hölder Theorem. If G is finite, there exists a sequence $G=G_0 \rhd G_1 \rhd G_2 \rhd \dots \rhd G_n=\{e\}$ s.t. $H_i = G_i/G_{i+1}$ is simple. Furthermore, the sequence (H_i), the "composition series" of G, is unique up to a permutation.

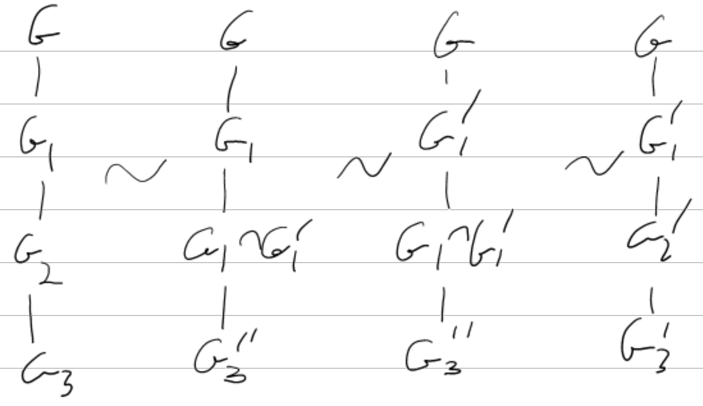
Proof By induction on $|G|$.

Existance: Let G_1 be a maximal normal proper subgroup of G...

Uniqueness: Suppose we have $G \rhd G_1 \rhd G_2 \dots$ and $G \rhd G_1' \rhd G_2' \rhd \dots$ WLOG, $G_1 \neq G_1'$, or else, use the induction.

Claim $G = G_1G_1'$ **Pf** $G_1G_1' \lhd G$ and bigger than G_1 & G_1'.





Def A G-set ("left G-set") is X w/ $G \times X \to X$ s.t. $ex = x$ & $(g_1 g_2)x = g_1(g_2 x)$. Say "G acts on X", write $G \curvearrowright X$. Same as $\alpha : G \longrightarrow S(X)$.

Def "right G-sets".

Examples 0. G itself, under left multiplication

[Thm: Every group is a subgroup of a perm group]

1. G itself, under conjugation.
2. Subgroups(G), under conjugation.
3. G/H when H is not necessarily normal.

Sub example: S_n/S_{n-1}: $\sigma S_{n-1} = \sigma' S_{n-1}$ iff $\sigma(n) = \sigma'(n)$. So take τ_i with $\tau_i(n) = i$ and then $\sigma \tau_i S_{n-1} = \tau_{\sigma i} S_{n-1}$. So

$$S_n/S_{n-1} \cong S_n \curvearrowright \{1, \ldots, n\}$$

4. $S^2 = SO(3)/SO(2)$.

Claim G-sets make a category!

If X_1 & X_2 are G-sets, the so is $X_1 \sqcup X_2$

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 $|X| \mid |G|$)

stated, not proven

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:

$$|G| = \overset{\substack{\text{the centre of } G\\ \downarrow}}{|Z(G)|} + \sum_i \big(G : \overset{\substack{\text{the centralizer}\\ \text{of } y_i \text{ in } G\\ \downarrow}}{C_G(y_i)}\big)$$

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 $\{e\}$.

25-347 Hour 18 on Fri Oct 10: Group actions, Sylow 1.
Enjoy the long weekend!!

$G \curvearrowright X$ means morphism $G \to S(X)$ means $(g,x) \mapsto gx$ 1. $ex = x$ 2. $(g_1g_2)x = g_1(g_2x)$

$X \curvearrowleft G$ means anti-mor. $G \to S(X)$ means $(x,g) \mapsto xg$ 1. $xe = x$ 2. $x(g_1g_2) = (xg_1)g_2$

both are categories, both have $\sqcup$

"Transitive" means $\neq \emptyset$ & $\forall x_1, x_2 \; \exists g \; gx_1 = x_2$

Thm 1. Every G-set is a disjoint union of transitive ones.

2. If X is transitive and $x_0 \in X$, then

$$X \cong G/[\mathrm{Stab}_X(x_0) := \{g : gx_0 = x_0\}]$$

so $|X| \,|\, |G|$

Thm If $G \curvearrowright X$ & x_i are representatives of the orbits,

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

The class eqn: $G \curvearrowright G$ by conjugation; pick one y_i from each non-singleton conjugacy class. Get

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

done line.

Corollary If G is a p-group, meaning $|G| = p^\alpha$ for some prime p, the centre of G is non-trivial, meaning $Z(G) \neq \{e\}$.

$|G| = p^\alpha m$, p prime, $p \nmid m$ [write $p^\alpha \| |G|$].

$\mathrm{Syl}_p(G) := \{P < G : |P| = p^\alpha\}$ "the Sylow subgroups of G"

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

Proof By induction on $|G|$.

write $|G| = \underbrace{|Z(G)|}_{1} + \underbrace{\sum_i (G : C_G(y_i))}_{2}$

Either both are divisible by p, or neither.

If neither, for some y_i $p \nmid (G : C_G(y_i)) \Rightarrow$

$p^r \| C_G(y_i)$ & $C_G(y_i) \lneqq G$, so find S' in $C_G(y_i)$.

If both, find x in $Z(G)$ with $|x| = p$, find a Sylow-p subgroup S' of $G' = G/\langle x \rangle$, and pull it back to a subgroup S of G.

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 $r = 0$.

with one y_i from each non-singleton conjugacy class of G,

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

Pf consider $G \curvearrowright G$ by conjugation

Corollary If G is a p-group, meaning $|G| = p^\alpha$ for some prime p, the centre of G is non-trivial, meaning $Z(G) \neq \{e\}$.

$|G| = p^\alpha m$, p prime, $p \nmid m$ [write $p^\alpha \| |G|$].

$\mathrm{Syl}_p(G) := \{P < G : |P| = p^\alpha\}$ "The Sylow subgroups of G"

$n_p(G) := |\mathrm{Syl}_p(G)|$

Thm (Sylow in one) 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 $n_p(G) = 1 \bmod p$ and $n_p(G) \mid |G|$.

Groups of order 15

First, a group of order p (prime) is $\mathbb{Z}/p$.

Let $|G| = 15$. $P_5 = \langle x \rangle \overset{?}{\trianglelefteq} G$ $P_3 = \langle y \rangle \overset{?}{\trianglelefteq} G$

y commutes with P_5; otherwise $|y| \mid |\mathrm{Aut}\, P_5| = 4$

So $G = \{x^i y^j : 0 \le i \le 4,\ 0 \le j \le 2\}$

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

check mult rule & find

$G = \mathbb{Z}/5 \times \mathbb{Z}/3 = \mathbb{Z}/15$

sneaky: take $G = \mathbb{Z}/15$.

Thm 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

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

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

$n_p \equiv 1 \bmod p \Rightarrow q \equiv 1 \bmod p \Rightarrow p \mid q-1$

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

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

HW?

Proof of Sylow $Syl_p(G) \neq \emptyset$: By induction on $|G|$.

write $|G| = \underbrace{|Z(G)|}_{1} + \underbrace{\sum_i (G:C_G(y_i))}_{2}$

Either both are divisible by p, or neither.

If neither, for some y_i: $p \nmid (G:C_G(y_i)) \Rightarrow$

$p^k \| C_G(y_i)$ & $C_G(y_i) \lneq G$, so find S in $C_G(y_i)$.

If both, find x in $Z(G)$ with $|x|=p$ (IOU), find a Sylow-p subgroup S' of $G' = G/\langle x \rangle$, and pull it back to a subgroup S of G.

"Cauchy's Thm" If G is finite Abelian, p prime, and $p \mid |G|$, then $\exists x \in G$ $|x|=p$.

Pf Enough to find z w/ $p \mid |z|$, for if $|z| = p \cdot n$, take $x = z^n$.

Pick $z \in G$, $z \neq e$. If $p \nmid |z|$, then $p \mid |G/\langle z \rangle|$ so by induction pick $y \in G$ with $|\bar{y}| = p$ in $G/\langle z \rangle$. Use:

Claim If $\phi : G \longrightarrow H$ is a morphism & $y \in G$, $|\phi(y)| \mid |y|$.

Pf $\phi(y)^{|y|} = \phi(y^{|y|}) = e$.

done line

The "extension trick", "can't extend a Sylow by something of order p".

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 $|\text{conjugates of } P| = 1 \bmod p$. (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 sites of all other orbits are divisible by p.

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. $H < N_G(P')$.

25-347 Hour 21 on Fri Oct 17: More Sylow, maybe |G|=21.
HW6 is online, HW5 is due at 11:59pm, return of HW4 will be 2-3 days delayed.

$|G| = p^\alpha m$, p prime, $p \nmid m$ [so $p^\alpha \| |G|$].

$\mathrm{Syl}_p(G) := \{P < G : |P| = p^\alpha\}$ $\quad n_p(G) := |\mathrm{Syl}_p(G)|$

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

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

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

4. $n_p(G) \equiv 1 \bmod p$ and $n_p(G) \mid |G|$.

Lemma 1. If $P \in \mathrm{Syl}_p(G)$ & $H < N_G(P)$ is a p-group, then $H < P$.

2. If $P \in \mathrm{Syl}_p(G)$, $|x| = p^\beta$, $x^{-1}Px = P$ then $x \in P$

"can't extend a Sylow by something of order p^n"

Reformulation: $P \in \mathrm{Syl}_p(G)$, $|H| = p^\beta \Rightarrow N_H(P) = H \cap P$

Claim If $P \in \mathrm{Syl}_p(G)$, then $|\text{conjugates of } P| \equiv 1 \bmod p$

$$|\mathcal{C}| = n_p \quad (\text{and } n_p \mid |G|, \text{ of course})$$

Pf $\mathcal{C} \circlearrowleft P$ by conjugation

$P' \in \mathcal{C}$ The $|\mathrm{Orb}_P(P')| = |P| / |\mathrm{Stab}_{\mathcal{C}}(P')|$

$$= p^\alpha / |N_P(P')| = p^\alpha / |P \cap P'| = \begin{cases} 1 & \text{if } P = P' \\ p^\beta,\ \beta > 0 & \text{otherwise} \end{cases}$$

Claim If $H < G$ is a p-group & $P \in \mathrm{Syl}_p(G)$, then H is contained in a conjugate of P

(in particular, all Sylow-p subgroups are conjugate)

Pf w/ same $\mathcal{C}$, $\mathcal{C} \circlearrowleft H$ by conjugation

There must be a singleton orbit, a P' s.t.

$H < N_G(P') \xRightarrow{\text{lemma}} H < P'$.

done line

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

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

$|G| = p^{\alpha+\beta} m$ w/ maximal α. By counting & binomial nonsense, $p^\alpha \mid |X|$ yet $p^{\alpha+1} \mid |X|$. 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 $|H| = p^\beta$.

Skip

Groups of order 21. $P_7 \lhd G$, 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. $\underset{\substack{\shortparallel \\ (\mathbb{Z}/p)^*}}{\mathrm{Aut}(\mathbb{Z}/p)}$ is cyclic;

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

skip

25-347 Hours 22-23 on Wed Oct 22: |G|=21, semi-direct products, Abelian groups.
HW Solutions Sets! TT discussion on Friday.

Thm (Sylow) 1. $Syl_p(G) \neq \emptyset$.

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

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

4. $n_p(G) \equiv 1 \mod p$ and $n_p(G) \mid |G|$.

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

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

[Aside: If $K, H \triangleleft G$ & $KH = G$ & $K \cap H = \{e\}$, then $G = K \times H$]

otherwise, $P_7 = \langle x \rangle$ $P_3 = \langle y \rangle$

We have $x^y = x$ or x^2 or x^4. What does it mean?

$x^2 \longrightarrow x^4$ isomorphic via $y \mapsto y^2$.

Semi-Direct Products

$N < G$, $H < G$ compare $N \times H$ w/ NH. There's always $\mu : N \times H \twoheadrightarrow NH$. (not a homomorphism!)

In general, nothing to say.

If $N \cap H = \{e\}$ injective but image may not be a group
e.g. $\langle (123) \rangle, \langle (345) \rangle \subset S_5$

If $N \cap H = \{e\}$ & $N \triangleleft G$ & $H \triangleleft G$ then $[N, H] = \{e\}$ & $N \times H \xrightarrow[\mu]{\sim} NH$.

The interesting case is when $N \cap H = \{e\}$, $N \triangleleft G$, $H < G$.

Get $\phi : H \to Aut(N)$ by $h \mapsto (n \mapsto n^{h^{-1}} = hnh^{-1})$ or $\phi_h(n) = hnh^{-1}$

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

$(nh)^{-1} = h^{-1} n^{-1} = h^{-1} n^{-1} h h^{-1} = \phi_{h^{-1}}(n^{-1}) \cdot h^{-1}$

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

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

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

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

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

done line

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

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

Groups of order 21 $\mathbb{Z}/7 \rtimes \mathbb{Z}/3 = (\langle x \rangle / x^7 = e) \rtimes (\langle y \rangle / y^3 = e)$

$\phi_y(x) = x$ or x^2 or x^4

sketch

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

Aside, F_n

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

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

"Braids are easy"

25-347 Hour 24 on Fri Oct 24: Semi-direct products, |G|=12.
HW06 due at 11:59.
Joe Repka will not be returning in time for the second semester; so Dror will be teaching the whole course :(.
TT: Tue Nov 4 7-9pm at EX 310. Material: *everything*. Content: 1/3 class,1/3 HW,1/3 fresh.
Dror's prep strategy.
5 office hours by TAs, 3 by me.

$N, H, \ \phi: H \to \mathrm{Aut}(N) \quad h \mapsto \phi_h \qquad N \rtimes_\phi H := N \times H$ w/

$(n_1, h_1)\cdot(n_2\, h_2) \overset{u}{:=} (n_1 \phi_{h_1}(n_2), h_1 h_2) \qquad (nh)^{-1} = (\phi_{h^{-1}}(n^{-1}), h^{-1})$

Thm $\quad N \rtimes_\phi H$ is a group, $N \triangleleft N \rtimes H$, $H < N \rtimes H$
$N \rtimes H / N \cong H$ $\qquad$ (so write nh instead of (n,h))

Examples 2. $\{ax+b\} \cong \mathbb{R}_b^+ \rtimes \mathbb{R}_a^\times$ $\qquad$ 0. $\phi \equiv Id \quad N \rtimes H \cong N \times H$
1. $D_{2n} = \mathbb{Z}/n \rtimes \{\pm 1\}$

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

4. The Poincare/relativity group $\mathbb{R}^4_+ \rtimes SO(3,1)$

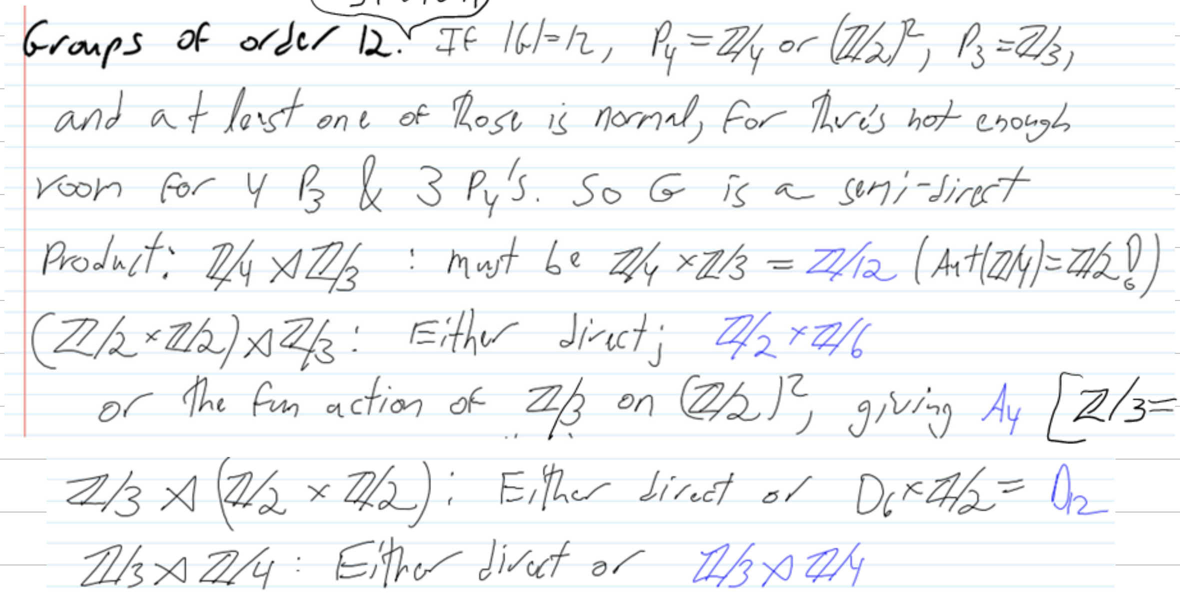
Groups of order 21 $\quad \mathbb{Z}/7 \rtimes \mathbb{Z}/3 = (\langle x \rangle / x^7 = e) \rtimes (\langle y \rangle / y^3 = e)$

$\phi_y(x) = x$ or x^2 or $x^4 =: \phi_1, \phi_2, \phi_4$

$\mathbb{Z}/7 \rtimes_{\phi_4} \mathbb{Z}/3 \xrightarrow{\sim} \mathbb{Z}/7 \rtimes_{\phi_2} \mathbb{Z}/3$ by $\begin{array}{l} x \mapsto x \\ y \mapsto y^2 = y^{-1} \end{array}$

could use a re-do

done line



(sketch)

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 $\left[\mathbb{Z}/3 = \langle (234) \rangle \quad (\mathbb{Z}/2)^2 = \left\{ \begin{array}{l} e, (12)(34) \\ (13)(24), \\ (14)(23) \end{array} \right\} \right]$

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

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

Aside. F_n; $\qquad PB_n$, $\ \rho: PB_n \longrightarrow PB_{n-1}$, $\ \ker \rho = F_{n-1}$

$PB_n = F_{n-1} \rtimes PB_{n-1} = F_{n-1} \rtimes (F_{n-2} \rtimes \ldots)$ $\qquad$ "Braids are easy"

MAT347 Planning

12 hours to end of Semester

Group Theory:

1. More 21, 12, PBn 2 hours ||
2. F.G Abelian groups 3 hours. |||

Ring Theory. Budget: 7 hours.

1. Definitions, quotients, isomorphism Thms 2 hours ||
   Aside: Cayley-Hamilton 1 hour. |
2. Maximal ideals & Fields. 1 hour
3. Euc $\Rightarrow$ PID $\Rightarrow$ UFD 3 hours
4. If time: localization, Fields of fractions.

2nd Semester:

1. F.g. modules over a PID. (5-10 hours)
   took 8 hours in 14-1100, but can be simplified a lot if uniqueness, which uses "the ring of modules", is removed, and if the explicit work on the JCF is removed.
2. Field Theory. ~8 weeks in 07-401, missing some of the punch lines.
3. The "Topological proof". 2 hours.

25-347 Hours 25-26 on Wed Nov 5: Sketch-level |G|=12 and braids, finitely generated Abelian groups.
I hope TT1 went well!
TT2 on Tue Feb 3 at 7-9pm?

$N,\ H,\ \phi: H \longrightarrow \mathrm{Aut}(N)\ \ (h \mapsto \phi_h)$

$G = N \rtimes_\phi N := N \times H$ with $n_1 h_1 n_2 h_2 = n_1 \phi_{h_1}(n_2) h_1 h_2$

<u>Thm</u> A group, $N \triangleleft G$, $H < G \ldots$

Groups of order $\overbrace{\text{12.}}^{\text{sketch}}$ 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 $\left[\mathbb{Z}/3 = \langle(234)\rangle \quad (\mathbb{Z}/2)^2 = \{e, (12)(34), (13)(24), (14)(23)\}\right]$

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

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

Aside. F_n; PB_n, $\rho: PB_n \longrightarrow PB_{n-1}$, $\ker \rho = F_{n-1}$

$PB_n = F_{n-1} \rtimes PB_{n-1} = F_{n-1} \rtimes (F_{n-2} \rtimes \ldots)$ "Braids are easy"

<u>Goal</u> If A is a $\overbrace{\text{finitely generated Abelian}}^{\text{explain}}$ group then $\exists\, r, p_i, s_i$ s.t. $A \cong \mathbb{Z}^r \oplus \bigoplus_i \mathbb{Z}/p_i^{s_i}$. Furthermore, r is determined uniquely, as is the list $((p_i, s_i))_{i=1}^{k}$ (up to a permutation).

<u>Pf</u> Gaussian elimination.

25-347 Hours 25-26 on Wed Nov 5: Sketch-level |G|=12 and braids, finitely generated Abelian groups.
I hope TT1 went well!
TT2 on Tue Feb 3 at 7-9pm?

$N, H, \phi: H \longrightarrow \mathrm{Aut}(N)$ $(h \mapsto \phi_h)$

$G = N \rtimes_\phi N := N \times H$ with $n_1 h_1 n_2 h_2 = n_1 \phi_{h_1}(n_2) h_1 h_2$

Thm A group, $N \triangleleft G$, $H < G$...

$|G| = 12$ (sketch) $P_3 = \mathbb{Z}/3$, $P_4 = \mathbb{Z}/4$ or $(\mathbb{Z}/2)^2$ (why?)

At least one must be normal, or else $n_3(G) = 4$, $n_2(G) = 3$, too much!

$P_4 = \mathbb{Z}/2 \times \mathbb{Z}/2$: direct, $\mathbb{Z}/3 \times (\mathbb{Z}/2 \times \mathbb{Z}/2) \cong \boxed{\mathbb{Z}/2 \times \mathbb{Z}/6}$

$\mathbb{Z}/3 \rtimes (\mathbb{Z}/2 \times \mathbb{Z}/2)$: $\boxed{D_6 \times \mathbb{Z}/2}$

$(\mathbb{Z}/2 \times \mathbb{Z}/2) \rtimes \mathbb{Z}/3$: $\boxed{A_{12}}$! $\left\{ \begin{matrix} e \\ (12)(34) \\ (13)(24) \\ (14)(23) \end{matrix} \right\} \rtimes \langle (234) \rangle$

$P_4 = \mathbb{Z}/4$: direct $\boxed{\mathbb{Z}/12}$

$\mathbb{Z}/4 \rtimes \mathbb{Z}/3$ no such thing or $\boxed{\mathbb{Z}_3 \rtimes \mathbb{Z}_4}$

Aside. F_n; PB_n, $\rho: PB_n \longrightarrow PB_{n-1}$, $\ker \rho = F_{n-1}$

$PB_n = F_{n-1} \rtimes PB_{n-1} = F_{n-1} \rtimes (F_{n-2} \rtimes \dots)$ "Braids are easy"

done line

$$\text{Goal If } A \text{ is a } \overbrace{\text{finitely generated Abelian}}^{\text{explain.}} \text{ group}$$

then $\exists\, r, p_i, s_i$ s.t. $A \cong \mathbb{Z}^r \oplus \bigoplus_i \mathbb{Z}/p_i^{s_i}$.

Furthermore, r is determined uniquely, as is the list $((p_i, s_i))_{i=1}^{k}$ (up to a permutation).

Pf Gaussian elimination.

Construction If $M \in M_{m \times n}(\mathbb{Z})$ we can associate to it a f.g. Abelian group:

$$M \longmapsto \phi_M : \mathbb{Z}^n \xrightarrow{M} \mathbb{Z}^m \longmapsto A_M := \mathbb{Z}^m / \operatorname{im} \phi_M$$

Examples $M = (0), (1), (12)$

Can be generalized! $M \in M_{G \times X}(\mathbb{Z})$ G finite, X maybe not

$$M \longmapsto \phi_M : \underset{\text{finite support.}}{\mathbb{Z}^X_{f.s.}} \xrightarrow{M} \mathbb{Z}^G \longmapsto A_M := \mathbb{Z}^G / \operatorname{im} \phi_M$$

Claim Every f.g. Abelian group arises this way.

Proof

$$\begin{tikzcd} \mathbb{Z}^X \arrow[r, two heads] \arrow[rr, bend left, "\phi_M"] & \ker \pi \arrow[r] & \mathbb{Z}^G \arrow[r, two heads, "\pi"] & A \end{tikzcd}$$

By iso 1, $A \cong \mathbb{Z}^G / \ker \pi \cong \mathbb{Z}^G / \operatorname{im} \phi_M$

Claim If $M' = PMQ$ where P is invertible in $M_{G \times G}(\mathbb{Z})$ and Q is invertible & col-finite in $M_{X \times X}(\mathbb{Z})$, w/ col-finite inverse, then $A_M \cong A_{M'}$

Proof

$$\begin{tikzcd} \mathbb{Z}^X \arrow[r, "M"] & \mathbb{Z}^G \arrow[r] \arrow[d, "P"] & A = \mathbb{Z}^G / \operatorname{im} M \arrow[d] & {[\alpha]_{\operatorname{im} M}} \arrow[d] \\ \mathbb{Z}^X \arrow[r, "M'"] \arrow[u, "Q"] & \mathbb{Z}^G \arrow[r] & A' = \mathbb{Z}^G / \operatorname{im} M' & {[P\alpha]_{\operatorname{im} M'}} \end{tikzcd}$$

Claim Can remove 0 columns from M w/o changing A_M

Moral: Can do restricted row/col ops (& 0-col-removals) on M w/o changing A_M

25-347 Hour 27 on Fri Nov 7: Finitely generated Abelian groups.
HW07 is online! TT2 on Tue Feb 3 at 7-9pm!

Goal If M is a $\overbrace{\text{finitely generated Abelian}}^{\text{explain}}$ group then $\exists\, r, p_i, s_i$ s.t. $M \cong \mathbb{Z}^r \oplus \bigoplus_i \mathbb{Z}/p_i^{s_i}$.
Furthermore, r is determined uniquely, as is the list $((p_i, s_i))_{i=1}^{k}$ (up to a permutation).

Pf Gaussian elimination.

Construction If $A \in M_{m\times n}(\mathbb{Z})$ we can associate to it a f.g. Abelian group:

$$A \longmapsto \phi_A : \mathbb{Z}^n \xrightarrow{A} \mathbb{Z}^m \longmapsto M_A := \mathbb{Z}^m / \operatorname{im} \phi_A$$

Examples $A = (0), (1), (12)$

Can be generalized! $A \in M_{G\times X}(\mathbb{Z})$ G finite, X maybe not

$$A \mapsto \phi_A : \mathbb{Z}^X_{\text{f.s.}} \xrightarrow{A} \mathbb{Z}^G \longmapsto M_A := \mathbb{Z}^G / \operatorname{im} \phi_A$$

finite support.

Claim Every f.g. Abelian group arises this way.

Proof
$$\begin{tikzcd} \mathbb{Z}^X \arrow[r, two heads] \arrow[rr, bend left, "\phi_A"] & \ker \pi \arrow[r] & \mathbb{Z}^G \arrow[r, two heads, "\pi"] & M \end{tikzcd}$$

By iso 1, $M \cong \mathbb{Z}^G / \ker \pi \cong \mathbb{Z}^G / \operatorname{im} \phi_A$

done line

claim If $A' = PAQ$ where P is invertible in $M_{G\times G}(\mathbb{Z})$ and Q is invertible & col-finite in $M_{X\times X}(\mathbb{Z})$, then
w/ col-finite inverse.

$M_A \cong M_A$

Proof

$$\begin{tikzcd}
\mathbb{Z}^X \arrow[r, "A"] & \mathbb{Z}^G \arrow[r] \arrow[d, "P"] & M_A = \mathbb{Z}^G/\mathrm{im}A \arrow[d] & {[\alpha]_{\mathrm{im}A}} \arrow[d] \\
\mathbb{Z}^X \arrow[r, "A'"] \arrow[u, "Q"] & \mathbb{Z}^G \arrow[r] & M_{A'} = \mathbb{Z}^G/\mathrm{im}A' & {[P\alpha]_{\mathrm{im}A'}}
\end{tikzcd}$$

Claim Can remove 0 columns from A w/o changing M_A

Moral: Can do restricted row/col ops (& 0-col-removals) on A w/o changing M_A

Fall Term Test Results

Dear Students -

As you probably already know, the results of the term test are in. They are excellent.

How should you read your grade?

- If you got 100 you should pat yourself on your shoulder and feel good.
- If you got something like 90, you're doing great. You made a few relatively minor mistakes; find out what they are and try to avoid them next time.
- If you got something like 80, you're doing fine but you did miss something significant, probably more than just a minor thing. Figure out what it was and make a plan to fix the problem for next time.
- If you got something like 65 you should be concerned. You are still in position to improve greatly and get an excellent grade at the end, but what you missed is quite significant and you are at the risk of finding yourself far behind. You must analyze what happened - perhaps it was a minor mishap, but more likely you misunderstood something major or something major is missing in your background. Find out what it is and try to come up with a realistic strategy to overcome the difficulty!
- If you got something like 50, most likely you are not gaining much from this class and you should consider dropping it, unless you are convinced that you fully understand the cause of your difficulty (you were very sick, you really couldn't study at all for the two weeks before the exam because of some unusual circumstances, something like that) and you feel confident you have a fix for next time. If you do decide to drop the class, don't feel too bad about it - it's one of the most abstract math classes here at UofT, and it really is tough.

Note that problems with writing are problems, period. Perhaps you got a low grade but you feel you know the material enough for a high grade only you didn't write everything you know or you didn't it write well enough or the silly graders simply didn't get what you wrote (and it isn't a simple misunderstanding - see "appeals" below). If this describes you, don't underestimate your problem. If you don't process and resolve it, it is likely to recur.

Solution Sets. There will be no "official" solution set, yet students are encouraged to submit the solutions to be placed on the class's web site, in a manner similar to the solutions for the HW assignments.

Appeals. Remember! We try hard yet grading is a difficult process and mistakes always happen - solutions get misread, parts are forgotten, etc. You must read your exam and make sure that you understand how it was graded. If you disagree with anything, don't hesitate to complain! (Though first consider very carefully the possibility that the mistake is actually yours). Your first stop should be the person who graded the problem in question, and only if you can't agree with him you should appeal to Dror (within a day or two).

Dror marked question 1, Jacob marked questions 2 and 3, and Matt marked 4 and 5. The deadline to start the appeal process is Wednesday November 19 at 5PM. Once you've started the process by talking to Dror or to one of the TAs, it ends when a final decision is made, with no deadline.

Best,

Dror.

25-347 Hours 28-29 on Wed Nov 12: Finitely generated Abelian groups.

Goal If M is a finitely generated Abelian group then $\exists\, r, p_i, s_i$ s.t. $M \cong \mathbb{Z}^r \oplus \bigoplus \mathbb{Z}/p_i^{s_i}$.

Furthermore, r & $\{(p_i, s_i)\}$ are unique.

Pf Gaussian elimination.

$$A \in M_{\underset{\text{finite}}{G} \times \underset{\text{maybe not}}{X}}(\mathbb{Z}) \longmapsto \phi_A : \underset{\text{finite support.}}{\mathbb{Z}^X_{F.S.}} \xrightarrow{A} \mathbb{Z}^G \longmapsto M_A := \mathbb{Z}^G / \operatorname{im}\phi_A$$

A is called "a presentation matrix for M_A"

Example $A = (a) \Rightarrow M_A \cong \mathbb{Z}/a\mathbb{Z}$

Claim Every M arises this way.

Claim If $A = A_1 \oplus A_2$, then $M_A = M_{A_1} \oplus M_{A_2}$ HW: complete this $A = \begin{pmatrix} A_1 & 0 \\ 0 & A_2 \end{pmatrix}$

Claim If $A' = PAQ$ where P is invertible in $M_{G\times G}(\mathbb{Z})$ and Q is invertible & col-finite w/ col-finite inverse in $M_{X\times X}(\mathbb{Z})$, then $M_{A'} \cong M_A$

HW: A f.g. group w/ a non-f.g. subgroup.

Proof

$$\begin{tikzcd}
\mathbb{Z}^X \arrow[r, "A"] & \mathbb{Z}^G \arrow[r] \arrow[d, "P"] & M_A = \mathbb{Z}^G/\operatorname{im}A \arrow[d] & {[\alpha]_{\operatorname{im}A}} \arrow[d] \\
\mathbb{Z}^X \arrow[r, "A'"] \arrow[u, "Q"] & \mathbb{Z}^G \arrow[r] & M_{A'} = \mathbb{Z}^G/\operatorname{im}A' & {[P\alpha]_{\operatorname{im}A'}}
\end{tikzcd}$$

Claim Can remove 0 columns from A w/o changing M_A

Moral: Can do restricted row/col ops (& 0-col-removals) on A w/o changing M_A

Now of all the presentation matrices of M, pick one with the least positive entry. WLOG,

1. It is a_{11}
2. The row & col of a_{11} otherwise vanish.
3. Every other entry of M is divisible by a_{11}

Now repeat. Get

$$A = \begin{pmatrix} a_{11} & & & \\ & a_{22} & & \\ & & a_{33} & \\ & & & \ddots \end{pmatrix} \quad \text{w/ } a_{11} | a_{22} | a_{33} | \dots$$

Thus "our" M_A is $\mathbb{Z}^k \oplus \bigoplus \mathbb{Z}/a_{ii} = \mathbb{Z}^k \oplus \bigoplus \mathbb{Z}/p_i^{s_i}$

Claim If

$$\mathbb{Z}^{k_1} \oplus \bigoplus \mathbb{Z}/p_{1i}^{s_{1i}} \cong \mathbb{Z}^{k_2} \oplus \bigoplus \mathbb{Z}/p_{2i}^{s_{2i}}$$

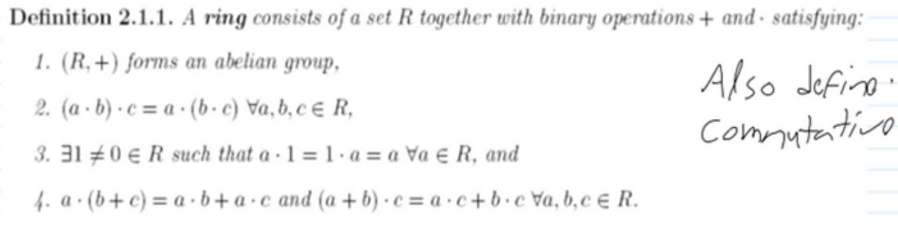
Then $k_1 = k_2$ & up to a permutation,

$$((p_{1i}, s_{1i})) = ((p_{2i}, s_{2i}))$$

Proof $\boxed{\text{See HW 8}}$.

We'll get back to this after rings and modules. done 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. $\mathbb{Z}$, $R[x]$, $M_{n\times n}(R)$, RG

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

done line (in 2014)

5. $M_{n\times n}(R[x]) \cong M_{n\times n}(R)[x]$
6. If $\varphi : G \to H$, $\varphi_* : RG \to RH$

25-347 Hour 30 on Fri Nov 14: Rings, morphisms, quotients.
HW07 is due at 11:59pm, HW08 is online. It's a tough one!

A word about Gaussian Elimination & nVidia.

not done.

Def A ring is $(R,+,\cdot)$ s.t.

1. $(R,+)$ is an Abelian group 2. $(ab)c=a(bc)$

3. $\exists\, 1\neq 0$ s.t. $a1=1a=a$ 4. $a(b+c)=ab+ac$, $(a+b)c=ac+bc$

Note: "commutative ring", "ring w/o unit".

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

done line.

Morphisms: - - - So Rings is a Category.

Examples:

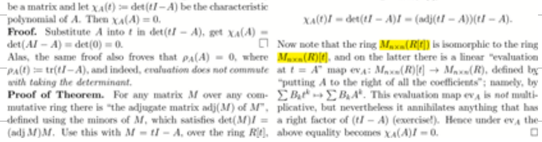
1. $\mathbb{Z}\to\mathbb{Z}/n\mathbb{Z}$ 2. $R\to M_{n\times n}(R)$ as diagonal.

3. $R\to R[x]$ at deg 0. 4. $ev_u: R[x]\to R$ if $u\in R$ & R is commutative or u is central.

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

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

If time, Cayley-Hamilton:



Dror Bar-Natan: Classes: 2025-26: MAT 347 Groups, Rings, Fields:

The Cayley-Hamilton Theorem

http://drorbn.net/25-347

Theorem. Let R be a commutative ring, let $A\in M_{n\times n}(R)$ be a matrix and let $\chi_A(t) := \det(tI-A)$ be the characteristic polynomial of A. Then $\chi_A(A)=0$.

Froof. Substitute A into t in $\det(tI-A)$, get $\chi_A(A)=\det(AI-A)=\det(0)=0$. ☐

Alas, the same froof also froves that $\rho_A(A)=0$, where $\rho_A(t):=\operatorname{tr}(tI-A)$, and indeed, *evaluation does not commute with taking the determinant.*

Proof of Theorem. For any matrix M over any commutative ring there is "the adjugate matrix $\operatorname{adj}(M)$ of M", defined using the minors of M, which satisfies $\det(M)I=(\operatorname{adj}M)M$. Use this with $M=tI-A$, over the ring $R[t]$, and find that in the ring $M_{n\times n}(R[t])$ we have

$$\chi_A(t)I=\det(tI-A)I=(\operatorname{adj}(tI-A))(tI-A).$$

Now note that the ring $M_{n\times n}(R[t])$ is isomorphic to the ring $M_{n\times n}(R)[t]$, and on the latter there is a linear "evaluation at $t=A$" map $ev_A\colon M_{n\times n}(R)[t]\to M_{n\times n}(R)$, defined by "putting A to the right of all the coefficients"; namely, by $\sum B_kt^k\mapsto\sum B_kA^k$. This evaluation map ev_A is *not* multiplicative, but nevertheless it annihilates anything that has a right factor of $(tI-A)$ (exercise!). Hence under ev_A the above equality becomes $\chi_A(A)I=0$. ☐

im, subring, ker, ideal. (ideals are subrings but never 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. $\varphi: R\to S \Rightarrow R/\ker\varphi = \operatorname{im}\varphi$.

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

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

25-347 Hours 31-32 on Wed Nov 19: Morphisms, quotients, maximal ideals and fields.

Q. How much is Gaussian Elimination worth?

Ring: $(R,+,\cdot,0,1)$ * $(R,+,0)$ an Abelian group
* $(R,\cdot,1)$ a monoid.
* Distributive law

Commutative ring, rngs: Rings w/o i.

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

Morphisms: ... So Rings is a category. Examples:

1. $\mathbb{Z}\to\mathbb{Z}/n\mathbb{Z}$ 2. $R\to M_{n\times n}(R)$ as diagonal.

3. $R\to R[x]$ at deg 0. 4. $ev_u: R[x]\to R$ if $u\in R$ & R is commutative or u is central.

5. If $\varphi: G\to H$, $\varphi_*: RG\to RH$. 6. $M_{n\times n}(R[x])\cong M_{n\times n}(R)[x]$

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:

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

Right proof.

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

$\det(tI-A)\cdot I=\operatorname{adj}(tI-A)(tI-A)=(\sum B_it^i)(tI-A)$ in

now substitute $t=A$. The B_i's commute with A

because $(tI-A)\operatorname{adj}(tI-A)=\operatorname{adj}(tI-A)(tI-A)$.

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

Q. Is every $\overset{\text{proper}}{}$ ideal a Kernel?

Ans. Define R/I.

done thru.

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

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

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

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

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

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 $\Leftrightarrow R/I$ 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.

25-347 Hour 33 on Fri Nov 21: Quotients, iso theorems, maximal ideals, fields.
HW08 is due 11:59pm, HW09 is online.

Q. How much is Gaussian Elimination worth?

Ideal: A subring $I \subset R$ w/ $IR = RI = I$

$R \xrightarrow{\pi_I} R/I = \{[x]_I = x + I : x \in R\}$ w/ 0, 1, +, · induced from R

Thm R/I is a ring.

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

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

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

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

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

useful for 3D rotations, etc...)

done line

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 $\Leftrightarrow$ R/I is a field.

Fishy proof: Use the 4th isomorphism theorem.

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

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

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

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

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

Proof using Zorn's Lemma.

25-347 Hours 34-35 on Wed Nov 26: "Better Rings" and ideals, primes and irreducibles, decompositions, asides.
RIP Prof. Joe Repka, 1949-2025.

Aside: division ring, a "non commutative field".

Example $\mathbb{H} := \{a+bi+cj+dk : \begin{smallmatrix} a,b,c,d \\ \in\mathbb{R} \end{smallmatrix}\} \Big/ \begin{smallmatrix} i^2=j^2=k^2=-1 \\ ij=k \text{ + cyc perms} \end{smallmatrix}$

useful for rotations in $\mathbb{R}^3$!

From now on, R is commutative.

Maximal Ideals. 1. Definition.

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

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. $S = l^\infty = \{\begin{smallmatrix} \text{bndd seq's} \\ \text{in } \mathbb{R} \end{smallmatrix}\}$ $\quad A_n = \{(a_i) : a_n = 0\}$

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

Proof using Zorn's Lemma.

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

J - a maximal ideal containing I.

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

Theorem Lim satisfies:

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

Definition R is an "integral domain" if it has no 0-divisors. Namely, if $ab = 0 \Rightarrow a = 0 \vee b = 0$.

In a domain, $ab = ac$ w/ $a \neq 0 \Rightarrow b = c$.

E.g. $\mathbb{Z}[x]$: yes
$\mathbb{Z}/6$: No.
$M_{22}(\mathbb{Z})$: No

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.

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

don. line.

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

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

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

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 irred. is decomposed, the decomposition must have length 1.

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

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

Thm. In a UFD gcd's always exist.

25-347 Hour 36 on Fri Nov 28: Primes and irreducibles, decompositions, asides.
Enjoy the holidays! No tutorials today.

All rings are assumed commutative

R/I a field $\iff$ I is maximal

R/I a domain (no 0-divisors) $\iff$ I is prime ($ab\in I \Rightarrow a\in I \vee b\in I$)

All rings are assumed to be domains!

Definitions 1. $a|b$ means $a\neq 0$ & $\exists q$ s.t. $aq=b$

2. If $a|b$ & $b|a$, "a&b are associates", write $a\sim b$ $\iff$ $a=ub$ where u is a unit [Aside $R^*=\{u\in R : u \text{ is a unit}\}$ is a multiplicative group]

3. "q is a gcd of a,b" if ......
unique up to a unit! Write gcd(a,b) } skipped.

4. A non-zero non-unit x is "irreducible" means

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

5. A non-zero non-unit x is "prime" means

$$p|ab \Rightarrow p|a \vee p|b$$

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

Claim Prime $\Rightarrow$ irreducible

Pf $p=ab \Rightarrow p|a \Rightarrow a=pc$
$\Rightarrow p=pcb \Rightarrow cb=1 \Rightarrow b\in R^*$

Counter example:
In $\mathbb{Z}[\sqrt{-5}]$ 2 is irred. for norm [std norm in $\mathbb{C}$] reasons but not prime as $2|(1-\sqrt{-5})(1+\sqrt{-5})=6$

done line

Def A UFD (unique fact. domain) is a domain in which every non-zero element can be factored into primes: $x = u p_1 p_2 \dots p_n$

Thm Such a factorization is unique up to units & a permutation.

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

Pf If an irred. is factored, it is presented as a product of a single prime.

Thm R is a UFD $\Leftrightarrow$ Every $x \neq 0$ has a unique decomposition into irreds.

Pf $\Rightarrow$ done.

$\Leftarrow$ need irred $\Rightarrow$ prime. If x is irred & $x | ab$, then $zx = \underbrace{a_1 \dots a_n}_{\text{irreds}}, \underbrace{b_1 \dots b_m}_{\text{irreds}} \Rightarrow \begin{matrix} x \sim a_i \\ \text{or} \\ x \sim b_i \end{matrix} \Rightarrow x | a$ or $x | b$.

Thm In a UFD, gcd's always exist.