Dawn of the First Day

~~First~~ Third – first to see wksh.

- Recall all the notes made on the previous wksht.
- Let $X^\times$ be the set of invertible elements. As a consequence of assoc. $X^\times$ is closed under $*$: If $a, b \in X^\times$, then $(a*b)^{-1} = b^{-1} * a^{-1}$
  $\Sigma \{a_1, \dots, a_n\} \subseteq X^\times$, so $(a_1 * \dots * a_n)^{-1} = a_n^{-1} * \dots * a_1^{-1}$.

~~Let~~

- Let ~~X~~ Y be a set. M_Y = the set of all self-functions on ~~X~~ Y, ie $\{f \mid f: Y \to Y\}$.

  Consider $(M_Y, \circ)$ ← composition of functions.

- Lemma: "$\circ$" is associative. Let $f, g, h \in M_Y$. Let $y \in Y$. Some how →
  $f \circ (g \circ h)(y) = f(g \circ h(y)) = f[g(h(y))] =$ some steps $= (f \circ g) \circ h(y)$
  So it's true.
  Does $(M_Y, \circ)$ have an identity? YES!, it's the identity function.

- If Y is big, is $(M_Y, \circ)$ commutative? No!
- In general, not every elt. has an inverse.
- Consider the set of invertible etts. in $(M_Y, \circ)$, it's closed under "$\circ$"
  Let S_Y be the invertibles in M_Y.
  When Y is finite w/ $|Y| = n \in \mathbb{N}$, call it S_n. $|S_n| = n!$
  ★ Time to use the group words! ★

- A set G w/ a binary operation $*$, $(G, *)$ is a group if:
  (1) $*$ is associative (3) ~~every~~ elt $g \in G$ has an inverse.
  (2) there is an identity

Proposition 1: With $(G, *)$ a group,
(1) identity is unique (3) If $s, t \in S$, $(s*t)^{-1} = t^{-1} * s^{-1}$
(2) inverses are unique (4) $(s^{-1})^{-1} = s$

(4) proof: $s \times s^{-1} = e = s^{-1} s$ & b/c inverses are unique, it's true.

Proposition 2: If a,b,c in G, then

1) $ca = cb \Rightarrow a = b$
2) $ac = bc \Rightarrow a = b$

- G is a group. Let $b \in G$. Then the order of b, denoted $|b|$, is

$$|b| = \begin{cases} \min \{k \in \mathbb{N} : b^k = e\}, & \text{if it exists} \\ \infty & \text{otherwise} \end{cases}$$

Side bar: $n \in \mathbb{N}$, $b^n = \underbrace{b \times \dots \times b}_{n \text{ times}}$ $\quad b^{-n} = \underbrace{b^{-1} \times \dots \times b^{-1}}_{n \text{ times}}$

We should note that $\forall i,j \in \mathbb{Z}$, $(b^i)^j = b^{ij}$ but if $a,b,c \in \mathbb{Z}$, $n \in \mathbb{N}$, is $(ab)^n = a^n b^n$?

not always true, must commute.

Ex In $\mathbb{Z}/3\mathbb{Z}$ $(\{0,1,2\}, +)$

$|0| = 1$
$|1| = 3$
$|2| = 3$

Ex $(\mathbb{Z}, +)$

$|0| = 1$
$|1| = \infty$

If $m \in \mathbb{Z} - \{0\}$ $|m| = \infty$.

Ex S_3 is a group

non-abelian (not commutative)

eg. $\alpha = (12)$

$$\alpha \mid \begin{matrix} 1 & 2 & 3 \\ 2 & 1 & 3 \end{matrix}$$

$\beta = (23)$

$$\beta \mid \begin{matrix} 1 & 2 & 3 \\ 1 & 3 & 2 \end{matrix}$$

$\beta\alpha = (132)$

$\alpha\beta = (123) = (321)$ $\quad \alpha\beta \neq \beta\alpha$

$|\alpha| = 2$ $\quad |\beta| = 2$

$|\alpha\beta| = 3$ $\quad |\beta\alpha| =$

Example probs from book:

#16) G is a group, $x^2 = e$ where $x \in G$, so $|x| \in \langle 1, 2 \rangle$.
In fact $|x| = 1$ iff $x = e$.
If $x \neq e$, then $x^2 = e$ implies $|x| = 2$.

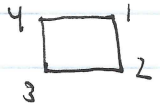
#17) Ex $|x| = n \in \mathbb{N}$, then $x^{n-1} = x^{-1}$
proof: well $x * x^{-1} = e = x^{-1} * x$
since $|x| = n$, $x^n = e$. So $x^{n-1} x = e = x x^{n-1}$

#18) $|x| = |x^{-1}|$. Suppose $|x|$ is finite & $|x| = n \in \mathbb{N}$. So $x^n = e$
& $(x^n)^{-1} = e$, by laws of exponents, $(x^{-1})^n = e$.
So $|x^{-1}| \leq |x|$
Use some kind of "symmetric argument" to show $|x^{-1}| \geq |x|$

#26) G is a group, H is a non empty subset of G, & H is closed under $*$ of G, & also closed under inverse. Then H is said to be a subgroup of G.
Show $(H, *)$ is a group. - fairly obvious

Ex) A, B are groups. $A \times B = \{(a, b) : a \in A, b \in B\}$.
$(a_1, b_1) \cdot (a_2, b_2) = (a_1 *_{\text{op of } A} b_1, a_2 \circ_{\text{op of } B} b_2)$
identity (e_A, e_B), & $(a, b)^{-1} = (a^{-1}, b^{-1})$

#36) fun problem to prevent on board if I finish.



special permutations on the square.

look at 1.1 exercises, & go over 1.2 soon.

• G is a group, $g, h \in G$, $n \in \mathbb{N}$

1) $|g| = |g^{-1}|$
2) $(ghg^{-1})^n = gh^n g^{-1}$
3) $|ghg^{-1}| = |h|$
4) $\left|\begin{pmatrix}1&1\\0&1\end{pmatrix}\right| = ?$

↳ 1) $\forall\, n \in \mathbb{N}$, $(g^n)^{-1} = (g^{-1})^n$.

Thus ~~if~~ $g^n = e$ iff $(g^{-1})^n = e$. If $|g|$ is finite, then $|g^{-1}|$ is finite, & $|g| = |g^{-1}|$. Apparently $|g| = \infty$ iff $|g^{-1}| = \infty$.

2) $(ghg^{-1})^n = gh^n h^{-1}$, Follows from associativity noting that terms telescope onto each other.

3) $|ghg^{-1}| = |h|$, use a similar argument to 1), $\forall\, n \in \mathbb{N}$, $(ghg^{-1})^n = e$ iff $h^n = e$.

4) $\left|\begin{pmatrix}1&1\\0&1\end{pmatrix}\right| = ?$ $M_2(F)$ → 2×2 matrices over the field F.

$\left\{\begin{pmatrix}a&b\\c&d\end{pmatrix} \mid a,b,c,d \in F\right\}$ → group under $+$

Under mult., $\cdot$, associative...

has an identity...

Does every elt. in $M_2(F)$ have an inverse?

The invertibles: $GL_2(F)$ ← how they're notated ← it's a group

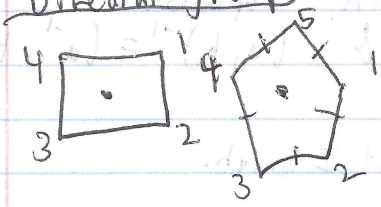
$\forall\, F \to \left|\begin{pmatrix}1&1\\0&1\end{pmatrix}\right| = \text{char}(F)$

↳ # of times you add 1 to itself to get 0

$\begin{pmatrix}1&1\\0&1\end{pmatrix}\begin{pmatrix}1&1\\0&1\end{pmatrix} = \begin{pmatrix}1&2\\0&1\end{pmatrix}$

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

• Dihedral group



90° on square — permutation

r (1234)

s (24) reflection across

pentagon

rotation r (12345)

reflection s (25)(43)

on

for any n-gon

Fixed point arguments show that rotations...

$r, r^2, r^3, \ldots, r^{n-1}, r^n = e$ → all different b/c they act on 1 in different ways.

Dihedral cont.

↳ We have n reflections on an n-gon as well. No rotation is equal to any reflection. So we have n distinct rotations, & n distinct reflections (rotations intersect reflections $= \emptyset$), so at least $2n$ elements.

- Observe that $\exists$ symmetries that carry 1 to any $i \in \langle 1, \dots, n \rangle$. Even the rotations act transitively on $\langle 1, \dots, n \rangle$.
- Suppose $\alpha(1) = i$. Consider $\alpha(2)$.
  ↳ only 2 possibilities (rotation or reflection)
  Since edges are also preserved under symmetries.

Once $\alpha(1)$, $\alpha(2)$ are known, α is known. Our upper bound for the total # of symmetries is $2n$. Thus there are exactly $2n$.

Observe that if we compose symm. the result is another symmetry. We have an operation, viewed as operations have an identity, & each symmetry has an inverse.

We have a group! D_{2n}

Claim

$rs = sr^{-1}$ Before we prove the claim, our aim is to find a canonical form for the elts of D_{2n}, a non-abelian group.

---

probs for hw

① G is a group, $g \in G$. $|g| = n \in \mathbb{N}$...
Then $e = g, g^2, \dots, g^{n-1}$ consist of n distinct elts.
$|g| = \infty \Rightarrow \forall\, m \in \mathbb{Z} - \{0\}$, $g^m = e$

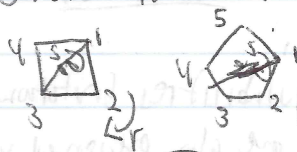
② $|g| = n$ $i, j \in \mathbb{Z}$, $g^i = g^j$ iff $n \mid i-j$.
↳ proof of (2)
Suppose $j \geq i$ & $g^i = g^j$ So
$g^{j-i} = e$ use the division algorithm to try and see $n \mid j-i$.
by the div. thm, $n = q(j-i) + r$ $0 \leq r < j-i$
$e = g^n = g^{q(j-i)+r}$
$= g^r$

$j - i = nq + r$ $0 \leq r < n$, so $g^{j-i} = g^{nq+r} = e^q g^r = e$
by def of order & that $|g| = n$, we can conclude $r = 0$, thus
$n \mid j-i$ ✓ QED

Conversely:
Assume $n \mid j-i$. WTS $g^i = g^j$
well $|g|=n$, & by the division algorithm:

$g^{nq} = e = g^{q(j-i)}$ ~~$g^n = e = g^{q(j-i)}$~~ thus $g^i = g^j$ QED

Back to dihedral groups:



① $|r|=n$
$|s|=2$

② g is determined by what it does on an edge (sorta)

③ From ② there are no more than $2n$ symmetries.

④ $rs = sr^{-1}$

⑤ $\forall\, j \in \mathbb{Z}$ $r^j s = s r^{-j}$ inductively.

⑥ "words" in $\{r, s\}$ ← alphabet

⑦ observe that every such word is equivalent to one of the form
$s^i r^j$, $i \in [0,1] \to 0 \le j < 2$
$0 \le j < n$

⑧ If $s^i r^j = s^{i'} r^{j'}$ where $0 \le i, i' < 2$ & $0 \le j, j' < n$.
then $i = i'$ & $j = j'$: to show this is so can be done in a few ways need to have shown that reflections & rotations @ form non-intersecting sets.
So the language $\{s^i r^j : i \in \{0,1\}, 0 \le j < n\}$ consists of $2n$ inequivalent symmetries.
So all symmetries can be expressed in the above words.

⑨ since we can move s to the left using $rs = sr^{-1}$

⑩ The mult. table of D_{2n} is determined by r & s,
$r^n = e = s^2$, & $rs = sr^{-1}$

generators ↓

$\langle r, s \mid r^n = e = s^2, rs = sr^{-1} \rangle$ ← Presentation of D_{2n}
So D_{2n} is 2 generated & determined by the relations given.

- On the other hand, there could be a group H w/ presentation $\langle r, s \mid r^n = e = s^2, rs = sr^{-1} \rangle$, eg $H = \{e\}$
H is presented by $\langle \rangle$. What's special about D_{2n} in terms of the above presentation?

more dihedral stuff cont.

Notice that any group w/ the above presentation has no more than $2n$ elements.

- Let's look at another presentation:

$$\langle x, y \mid xy = yx \rangle$$

- it's an abelian group

- have 2 groups: $G = (G, *)$

$H = (H, \circ)$ $\quad \Gamma : G \to H$

is a group homomorphism if $\forall\, x, y \in G$: $\Gamma(x * y) = \Gamma(x) \circ \Gamma(y)$

Γ doesn't have to be onto

If Γ is one-to-one & onto, then Γ is said to be an isomorphism. & H is said to be isomorphic to G.

- Does $\exists$ an isomorphism $\phi : H \to G$?

consider $\Gamma^{-1} : H \to G$ a bijection ... needs to be a homomorphism.

Γ^{-1} is compatible w/ the ops.

Let $u, v \in H$. So consider $\Gamma^{-1}(u \circ v)$. Γ is onto means that

$\exists\, x, y \in G$, $\Gamma(x) = u$, $\Gamma(y) = v$,

Now $\Gamma^{-1}(u \circ v) = \Gamma^{-1}(\Gamma(x) \circ \Gamma(y)) = \Gamma^{-1}(\Gamma(x * y)) = (x * y)$

$= \Gamma^{-1}(u) \circ \Gamma^{-1}(v)$

leading up to something useful...

Euclid's Lemma: p prime, $p \mid ab$ $(a,b \in \mathbb{Z})$ $\Rightarrow p \mid a$ or $p \mid b$.

Suppose $n, a, b \in \mathbb{N}$, $\gcd(n,a) = 1$, $n \mid ab \Rightarrow n \mid b$.

Proof: If $\gcd(n,a) = 1$, $\exists\ s,t \in \mathbb{Z}$ $sn + ta = 1$.

So $snb + tab = b$ n divides both summands so $n \mid b$.

—Moving on:

G is a group, $g \in G$, $|g| = n \in \mathbb{N}$. Let $j \in \mathbb{Z}$, Then $|g^j| = \frac{n}{\gcd(n,j)}$

Proof: Suppose $k \in \mathbb{N}$ & $(g^j)^k = e$. ie $g^{jk} = e$

by earlier lemma, $n \mid jk$ since $|g| = n$.

So $\frac{n}{\gcd(j,k)} \mid \frac{j}{\gcd(n,j)} k$. Not difficult to show that $\left(\frac{n}{\gcd(j,k)}, \frac{j}{\gcd(n,j)}\right)$ are rel. prime. By the lemma above,

$$\frac{n}{\gcd(n,j)} \mid k.$$

So $k \geq \left(\frac{n}{\gcd(n,j)}\right)$. Also $g^{j \frac{n}{\gcd(n,j)}} = g^{nm}$ where $m = \frac{j}{\gcd(n,j)} \in \mathbb{Z}$

$= e$.

But time moving on

Homomorphism: $\Gamma : G \to H$

$\Gamma(a * b) = \Gamma(a) \circ \Gamma(b)$ $\forall\ a, b \in G$.

Ex $G = (\mathbb{Z}, +)$, $H = (\mathbb{Z}/n\mathbb{Z}, +)$ $n \in \mathbb{N}$.

$\Gamma : (\mathbb{Z}, +) \to (\mathbb{Z}/n\mathbb{Z}, +)$

$z \to \{z\}$ ← we've shown that $y, z \in \mathbb{Z}$,

then $\Gamma(y+z) = [y+z] = [y] + [z] = \Gamma(y) + \Gamma(z)$

Ex $D : GL_2(\mathbb{R}) \to (\mathbb{R} - \langle 0 \rangle, \cdot)$

$A \mapsto \det(A)$ well $\det(AB) = \det(A)\det(B)$

So D is compatible w/ the operations.

Isomorphism: $\Gamma: G \to H$ is an isomorphism if Γ homomorphism & is bijective.
The examples above are not isomorphisms, ex) GL_2 is not one to one $\left|\begin{bmatrix} 1 & 0 \\ 0 & 1 \end{bmatrix}\right| = 1 \quad \left|\begin{bmatrix} 0 & 1 \\ 1 & 0 \end{bmatrix}\right| = 1$, see?

Automorphism: $\Gamma: G \to G$, homomorphism, bijective, w/ same domain & codomain.

Ex) Let G be a group, $g \in G$. $C_g: G \to G$
$h \mapsto ghg^{-1}$
We have $C_g(hj) = ghjg^{-1} = (ghg^{-1})(gjg^{-1}) = C_g(h)\,C_g(j)$
with compatible by operation.
Then it's up to you to show it's a bijection

Let's return ourselves to dihedral groups:
$D_{2n} = \langle s, r \mid s^2 = r^n = e,\ rs = sr^{-1} \rangle$
Any group-forgetting D_{2n} -- which is presented as above, all elts. can be represented: $\langle s^i r^j : 0 \le i < 2,\ 0 \le j < n \rangle$.
If H is presented $\langle a, b : a^n = e = b^2,\ ab = ba^{-1} \rangle$.

Claim: H is a homomorphic image of D_{2n} ... $\exists\ \Gamma: D_{2n} \twoheadrightarrow H$ (onto)
let $\Gamma(s^i r^j) = b^i a^j$
Using the relations, it's easy to see that the function is compatible w/ the operations.

• Lastly in this chapter:
Group actions: G is a group A is a set
Function (our "action"), the elts. of the group act on the elts. of A. We denote what $g \in G$ does to $a \in A$ by "$g \cdot a$" → wouldn't think of this as multiplying.
(0) $\forall\ g \in G,\ a \in A,\ g \cdot a \in A$.
(1) $\forall\ g, h \in G,\ \forall\ a \in A,\ (gh) \cdot a = g \cdot (h \cdot a)$
(2) $e \cdot a = a \quad \forall\ a \in A$
ex) trivial action of G on A $g \cdot a = a$ $\forall\ g \in G\ \forall\ a \in A$.

now represented

G A

Ex S_3 $\{1,2,3\}$

perm $\rightarrow (1\ 2)$ $\quad g\cdot 1 = 2,\ g\cdot 2 = 1,\ g\cdot 3 = 3$

ex what if D_{2n} by a mult.

Lemma: We have a group G acting on a set A. Let $g \in G$, & let $\sigma_g : A \to A$, which $\sigma_g(a) = g\cdot a$ $\forall a \in A$. (fixing g, letting a vary) Then σ_g is a permutation.

~~Recall def~~ - review

Def: G acts on A: (0) $\forall g \in G, \forall a \in A$, $ga \in A$.

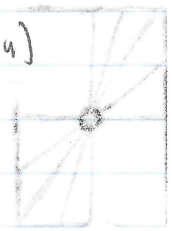
(1) $\forall g,h \in G$ $\forall a \in A$, $(gh)\cdot a = g(ha)$

(2) $\forall a \in A$, $ea = a$

Ex (1) S_n acts on $\langle 1,\dots,n\rangle$.

(2) D_{2n} acts on $\langle 1,\dots,n\rangle$.

(3) D_8 acts on $\langle \{1,3\},\{2,4\}\rangle$



Last time ... Given $g \in A$, let $\sigma_g : A \to A$ be defined by $\sigma_g(a) = ga$ $\sigma_g(a) = ga$ is well-defined

Lemma: $\forall g \in G$, σ_g is a perm of A.

Proof: Suppose $a,b \in A$ & $\sigma_g(a) = \sigma_g(b)$. WTS $a = b$.

So $g\cdot a = g\cdot b$

$\Rightarrow g^{-1}(g\cdot a) = g^{-1}\cdot(g\cdot b)$

Assuming (0), (1), (2).

By axiom (1) $a = (g^{-1}\cdot g)\cdot a = g^{-1}\cdot(ga) = g^{-1}\cdot(g\cdot b) = (g^{-1}\cdot g)\cdot b = b$

$\Rightarrow a = b$ by (2) in several places.

So σ_g is injective. If $b \in A$,

If $b \in A$, $\sigma_g(g^{-1}\cdot b) = b$ as can be checked. QED

- $\sigma : G \to S_A$ where $\sigma(g) = \sigma_g$

$\sigma : G \to S_A$ where $\sigma(g) = \sigma_g$

- **Lemma:** σ is a homomorphism.

  Proof: Let $g, h \in G$. We have $\sigma(gh) = \sigma_{gh}$
  we'd like to show $\sigma(gh) = \sigma(g) \circ \sigma(h)$.
  Let $a \in A$. We have $\sigma(gh)(a) = \sigma_{gh}(a) = gh \cdot a = g(h \cdot a)$
  Note that $\sigma(g) \circ \sigma(h)(a) = \sigma_g(\sigma_h(a)) = g \cdot (h \cdot a)$
  Since a is an arbitrary elt. of A, apparently we have
  $\sigma(gh) = \sigma(g) \cdot \sigma(h)$. QED.

Def: $\ker \sigma = \langle g \in G : \sigma(g) = e_{S_A} \rangle$

Def: if $\ker \sigma = \langle e_{S_A} \rangle$, (as small as possible) then the action is said to be **faithful**

Ex S_n on $\langle 1, \ldots, n \rangle$ is faithful
D_{2n} " " " "
D_8 on $\{\{1,3\},\{2,4\}\}$ isn't faithful. Why?

$\ker \sigma$ of $D_8 = \langle e, (1,3), (2,4), (13)(24) \rangle$

- **Permutations:** S_N (permutations on $\{1, \ldots, n\}$) (has n! elts)

  x : 1 2 3 4 5 6 7
  $\alpha(x)$: 3 2 1 4 7 6 5
  we view cycle notation:
  $(1\ 3) \circ (5\ 7)$

Def: $(a_1 \ldots a_k), (b_1 \ldots b_\ell)$
disjoint if $\{a_1, \ldots, a_k\} \cap \{b_1, \ldots, b_\ell\} = \emptyset$
non ex: $(1\ 2\ 3)\ (2\ 5\ 4)$
non disjoint - harder to deal with.

Fact 1 If $\alpha = (a_1 \ldots a_k)$
$\beta = (b_1 \ldots b_\ell)$ if α & β are disjoint then $\alpha\beta = \beta\alpha$
(not true if not disjoint .. $(12)(13) \neq (13)(12)$

Why? If $y \notin \{a_1, \ldots, a_k, b_1, \ldots, b_\ell\}$, Then $\alpha\beta(y) = y = \beta\alpha(y)$
suppose $z \in \{a_1, \ldots, a_k\}$ also disjoint.
Say $z = a_i$ .. so $\alpha\beta(z) = \alpha(z) = a_{i+1 \bmod k}$ &
$\beta\alpha(z) = \beta(a_{i+1 \bmod k}) = a_{i+1 \bmod k}$.

note identity of $S_n = \varepsilon$

Fundamental Lemma of S_n: If $\alpha \in S_n - \varepsilon$, $\alpha_1 \cdots \alpha_j = \alpha = \beta_1 \cdots \beta_k$, where α_i α_j is a product of disjoint cycles, $\beta_1 \cdots \beta_k$ is a prod. of disjoint cycles.

Then up to ordering the factorizations are the same.

Proof: If y is moved by α, it's moved in exactly one α_i & exactly one β_j. Now "following" y in the two representations (α_i, β_j) the same things must happen. So $\alpha_i = \beta_j$.

Fun thing: $S_n \to$ let's take a transposition (a 2-cycle): $(3\ 4) \in S_n$

$\beta \in S_n \quad \beta(3\ 4)\beta^{-1} = \gamma$

$\gamma(\beta(3)) = ? = \beta(3\ 4)\beta^{-1}(\beta(3)) = \beta(3\ 4)(3) = \beta(4)$

$\gamma(\beta(4)) = ? = \beta(3\ 4)\beta^{-1}(\beta(4)) = \beta(3\ 4)(\beta(4)) = \beta(3)$

$\beta(3\ 4)\beta^{-1} = \beta(3)\ \beta(4)$ clears the smoke clears

Choose $y \notin \{\beta(3), \beta(4)\}$ Then $\beta(3\ 4)\beta^{-1}(y) = y$

In general $\beta(a_1 \ldots a_k)(b_1 \ldots b_\ell) \ldots (z_1 \ldots z_r)\beta^{-1}$

$\beta(a_1 \ldots a_k)\beta(b_1 \ldots b_\ell) \ldots \beta(z_1 \ldots z_r)$

Last thought for 2.1 G is a group, H is non-empt subset $H \leq G$ if either criterion is satisfied:

1) G finite: $H \leq G$ iff H is closed under the opp.

one step subgroup test. → 2) $H \leq G$ iff $\forall\ y, z \in H$ $yz^{-1} \in H$

Def: G is a group, $b \in G$

centralizer → 1) $C_b(G) = \{g \in G : gb = bg\}$

If $A \leq G$, A is nonempty, $C_A(G) = \{g \in G : \forall a \in A, ga = ag\}$

It turns out $C_b(G) \leq G$ & $C_A(G) \leq G$

Ex) $C_{(13)}(S_4)$ ... ~~when we'll start next time.~~

Ex) G Abelian, $a \in G$ $C_a(G) = G$

Ex) $C_{(12)}(S_3) = \{\beta \in S_3, \beta(12)\beta^{-1} = (12)\}$

comments in any group G $\{u, v\} \subseteq G$, $uv = vu$ iff $uvu^{-1} = v$. (side note)

Comment 2: $\beta(12)\beta^{-1} = (\beta(1)\beta(2))$ so $C_{e,3}(S_3) = \{e, (12)\}$.

Comment 3: $\beta(a,b)\beta^{-1} = (\beta(a)\beta(b))$

Ex) $C_{(23)}(S_4) = \{\beta \in S_4 : \beta(23)\beta^{-1} = (23)\}$
$= \{e, (23), (14), (23)(14)\}$

↳ comment 3 should be the ^(in S_n of $\beta \in S_n$) that $\beta(a_1 \dots a_k)\beta^{-1} = (\beta(a_1) \dots \beta(a_k))$

Proof of this generalization:

If $y \in \{1, \dots, n\}$, $\beta^{-1}(y) \notin \{a_1, \dots, a_k\}$, $\beta(a_1 \cdots a_k)\beta^{-1}(y) = \beta(\beta^{-1}(y)) = y$

& $y \in Fix(\beta(a_1 \cdots a_k)\beta^{-1})$.

If $\beta^{-1}(y) \in \{a_1, \dots, a_k\}$

$\beta(a_1 \cdots a_k)\beta^{-1}(y)$ & let's say $\beta^{-1}(y) = a_i$, some i, $1 \le i \le k$.

Consider $\beta(a_1 \cdots a_k)\beta^{-1}(y) = \beta(a_1 \cdots a_k)(a_i) = \beta(a_{i+1})$

The elements that are fixed by $\beta(a_1 \cdots a_k)\beta^{-1}$ are now characterized.

The elements that are moved are of the form ...

now we can reread, filling in details & see that the move effects are $\beta(a_1), \dots, \beta(a_k)$ everything else is fixed & $\beta(a_1 \cdots a_k)\beta^{-1}$ moves $\beta(a_i)$ to $\beta(a_{i+1})$

Defi G is a group $Z(G) = \{g \in G : \forall h \in G, gh = hg\}$

Observe:

$$Z(G) = \bigcap_{a \in G} C_a(G)$$

So G is Abelian iff $Z(G) = G$.

Ex) $Z(S_3)$

$C_{(12)}(S_3) \cap$
$C_{(23)}(S_3) \cap$ ⊗
$C_{(31)}(S_3) = \{e\}$

$\Big\rangle$ $Z(S_3) = \{e\}$ (is trivial)

Ex)

~~$Z(S_n) = \begin{cases} S_n, & \text{if } 2 \geq n \\ \{e\}, & \text{otherwise} \end{cases}$~~

Back to an earlier comment:

$\beta(a_1 \cdots a_k)\beta^{-1} = (\beta(a_1) \cdots \beta(a_k))$

let's look at: $\beta(a_1 \cdots a_k)(b_1 \cdots b_{k_2})\beta^{-1} = \beta(a_1 \cdots a_k)\beta^{-1}\beta(b_1 \cdots b_{k_2})\beta^{-1}$

$= (\beta(a_1) \cdots \beta(a_k))(\beta(b_1) \cdots \beta(b_{k_2}))$

Ex) D_8, $Z(D_8) = ?$

Instead of operating in "S_n-arithmetic" world, can write it as sr^i $0 \leq i < 4$

$sr^i s = r^i s = sr^{-i}$ & $sr^i = sr^{-i}$ iff $i = 2, 0$

We only consider sr^2 & $s = sr^0$

$r(sr^2) = sr^{-1}r^2 = sr$

$(sr^2)r = sr^3 \neq sr$

$rs \neq sr$

What about elts in center of form r^j, $j = 0, 1, 2, 3$

Well, r^j commutes w/ r.

Look at $sr^j = r^j s$?

$r^j s = sr^{-j}$, and we have equality with $sr^{-j} = sr^j$ iff $j = 0$ or 2

$Z(D_8) = \{e, r^2\}$. Same arguments work for D_{2n} when n is even. When n is odd, $Z(D_{2n}) = \{e\}$.

$Z(D_{2n}) = \{\{e\}, r^{n/2}\}$

- Cyclic Groups: A group G is cyclic if $G = \langle g \rangle$, for some $g \in G$.

$\langle g \rangle = \{g^k : k \in \mathbb{Z}\}$

Ex) $(\mathbb{Z}, +) = \langle 1 \rangle = \langle -1 \rangle$

Ex) $n \in \mathbb{Z}$, $\mathbb{Z}/n\mathbb{Z} = \langle 1 \rangle$

Ex] $n=4$ & $n=5$

Generators of $\mathbb{Z}/4\mathbb{Z}$, are $\{1,3\}$

$\langle 2\rangle = \{0,2\}$ not a generator

$n=5$:

generators: $\{1,2,3,4\}$

$k \in \mathbb{Z}/n\mathbb{Z}$ is a generator iff $\gcd(k,n)=1$

2 properties of cyclic groups

- If G is cyclic, & $\Gamma: G \twoheadrightarrow K$ is an onto homomorphism, then K is cyclic

(not necessarily true that K is cyclic if not onto.)

Proof: Let $\langle g\rangle = G$. Consider $\langle \Gamma(g)\rangle$. b/c Γ is onto, every elt. k in K is of form $\Gamma(h)$, $h \in G$.

But $h = g^j$ for some $j \in \mathbb{Z}$. So $k = \Gamma(g^j)$ b/c Γ is homomorphism $(\Gamma(g))^j$.

- If G is cyclic, G is abelian

Proof: Let $a,b \in G$, a cyclic group w/ $G=\langle g\rangle$. So $ab = g^s g^t$ for some s,t in $\mathbb{Z}$, so $ab = g^s g^t = g^{s+t} = g^{t+s} = g^t g^s = ba$.

- Is every Abelian group cyclic?

$\mathbb{Z}/2\mathbb{Z} \times \mathbb{Z}/2\mathbb{Z} = \{([0],[0]), ([0],[1]), ([1],[0]), ([1],[1])\}$

(orders: 1, 2, 2, 2)

✱ Cyclicity is not in general preserved by direct products. ✱

✱ Is every subgroup of a cyclic group cyclic?

Cyclic Groups

Recall: G is cyclic (or "1-generated") if $\exists\, g \in G \ni G = \{g^k \mid k \in \mathbb{Z}\}$.

Clearly G cyclic $\Rightarrow$ G abelian. Last time we showed all abelians aren't cyclic.

Proposition: G is cyclic, $G=\langle g\rangle$

$\cong$ isomorphic

A) $|g|=n\in\mathbb{N}$, Then $G=\{e, g, g^2, \dots, g^{n-1}\}$ n distinct elts & $G\cong \mathbb{Z}/n\mathbb{Z}$

B) $|g|=\infty$. Then $\forall\ i,j\in\mathbb{Z}$, $g^i=g^j$ iff $i=j$; & $G\cong(\mathbb{Z},+)$

Proof: A) We showed that A is a group & $|a|=m\in\mathbb{N}$, Then $\{a^0, a^1, a^2, \dots, a^{m-1}\}$ comprise m distinct elts. Indeed $m>j\geq i\geq 0$, $a^j=a^i$, then $a^{j-i}=e$, and $m>j-i$, & $|a|=m$, so $j-i=0$ so $j=i$.

Quiz proof

So we know since $|g|=n$, that $\{g^0, g^1, g^2, \dots, g^{n-1}\}$ has n distinct elts. Given an arbitrary elt. $g^j\in\langle g\rangle$, & $j\in\mathbb{Z}$, WTS $g^j\in\{g^0, g^1, \dots, g^{n-1}\}$.

By the division thm, $j=nq+r$ $0\leq r<n$.

Consider $g^j=g^{nq+r}=g^{nq}g^r=g^r$ ... completing distinctness.

Consider $\Gamma: G\to \mathbb{Z}/n\mathbb{Z}$ $0\leq j<n$

ie $g\mapsto j$ so Γ is clearly a bijection, & by inspection Γ respects the ops. QED

B) Suppose $|g|=\infty$. Then we showed that $g^j=g^k$ $\forall\ k,j\in\mathbb{Z}$ iff $j=k$.

$G=\langle g^j : j\in\mathbb{Z}\rangle$. Consider $\Gamma: G\to\mathbb{Z}$

ie $g^j\mapsto j$ clearly bijective & computible. QED

Thm: G cyclic, $G=\langle g\rangle$, & $H\leq G$ (H is a subgroup of G), then H is cyclic.

Proof: First case: $H=\{e\}=\langle e\rangle$

Now assume H is nontrivial so $\exists\ b\in H-\{e\}$.

Let $J=\{k\in\mathbb{N} : g^k\in H\}$, we know $b=g^j$, some $j\in\mathbb{Z}-\{0\}$.

If $j>0$, then $J\neq\emptyset$. What if $j<0$? Consider $b^{-1}\in H$.

Now $b^{-1}=g^{-j}$ & $-j\in\mathbb{N}$. We've shown J is non-empty, & we can apply well-ordering.

$\exists$ a least elt. $m\in J$ ie. $m=\min J$.

Claim: $H=\langle g^m\rangle$

Proof: Clearly since $g^m\in H$ & $H\leq G$, $\{(g^m)^\ell : \ell\in\mathbb{Z}\}\subseteq H$, ie $\langle g^m\rangle\subseteq H$. Suffices to show $H\subseteq\langle g^m\rangle$

Let $c\in H$. Since $H\leq G$ $\exists\ n\in\mathbb{Z}$ $\ni$ $c=g^n$.

By the division Thm $n=mq+r$ $0\leq r<m$.

Cont. on next page.

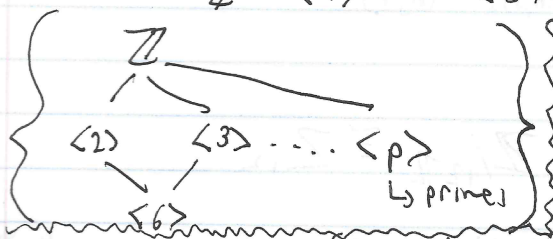
Cont. from previous page

Note that $g^r = g^{n-mq} = g^n (g^{-m})^q$ $\quad g^m \in H$, $g^{-m} \in H$, so $g^r \in H$

Thus $r = 0$. So $n \mid n$, & so $g^n \in \langle g^m \rangle$, completes the proof. QED

- Subgroups of $\mathbb{Z}$: If $H \leq \mathbb{Z}$, H is cyclic, so $H = \langle n : n \in \mathbb{Z} \rangle$.
  We can take n to be non-negative.

Examples: $\{0\} = \langle 0 \rangle$ $\quad \langle 2 \rangle$: evens $\quad \langle 621 \rangle$: multiples of 621.
$\mathbb{Z} = \langle 1 \rangle$ $\quad \langle 3 \rangle$: multiples of 3



lattice. ooooh.

- Thm: G is cyclic, $|g| = n \in \mathbb{N}$. Then the complete list of subgroups of G is $\{\langle g^{(k,n)} \rangle : n \geq k \geq 0\}$ & these subgroups are distinct..., which can also be more easily be understood as $\{\langle g^d \rangle \mid d \mid n\}$ & these are pairwise distinct.

RECALL $(n,k) = \gcd(n,k)$

Ex) $\mathbb{Z}/6\mathbb{Z} = \langle 1 \rangle$ $\quad |1| = 6$

subgroups: $\langle 2 \rangle, \langle 3 \rangle, \langle 1 \rangle, \langle 0 \rangle$.

Proof: Claim 1 - For $0 \leq k \leq n$, $\langle g^k \rangle = \langle g^{(n,k)} \rangle$. Observe that $(n,k) \mid k$.
That is, $\exists\, m \in \mathbb{N}$, $(n,k)m = k$. So $g^{(n,k)m} = g^k$
So $g^k \in \langle g^{(n,k)} \rangle$. So using closure, $\langle g^k \rangle \subseteq \langle g^{(n,k)} \rangle$.
How can I get $g^{(n,k)}$ in $\langle g^k \rangle$? We know $(n,k) = sn + tk$ for some $s, t \in \mathbb{Z}$. So $g^{(n,k)} = g^{sn+tk} = (g^n)^s g^{tk} = e(g^k)^t = (g^k)^t$. Now by closure (again) $\langle g^{(n,k)} \rangle \subseteq \langle g^k \rangle$. So $\langle g^k \rangle = \langle g^{(n,k)} \rangle$. QED
- All subgroups we have are $\{\langle g^{(n,k)} \rangle : \ldots\}$, they are pairwise distinct. Maybe $\langle g^{(n,k)} \rangle = \langle g^{(n,j)} \rangle$.

In all groups A, if $|a| = t$, $|a^j| = \frac{t}{(t,j)}$. If $n > k \geq j \geq 0$, then $|g^{(n,k)}| = \frac{n}{(n,(n,k))} = \frac{n}{(n,k)}$, $|g^{(n,j)}| = \frac{n}{(n,(n,j))} = \frac{n}{(n,j)}$.

Lastly (n,k) is a divisor of n.

Moreover, divisors of n (d, less than n) are of the form "(n,j)".

- We're now in 2.4 in the book.

Preview: Let $A \subseteq G$, $A \neq \emptyset$. Wanna talk about subgroup of G generated by A.
Want: smallest subgroup of G containing A.

We've seen the intersection of any set of subgroups $\{H_i : i \in I, H_i \leq G\}$ is closed under intersection.
(This will be reviewed)

Quiz 1 done... phew.

③ All subgroups of G are cyclic. [know how to prove for exam 1]

$\uparrow$ G is cyclic

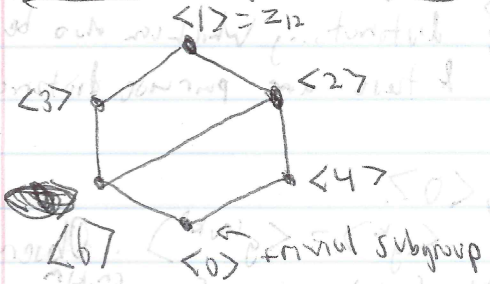
Question: Why if $n \geq j \geq i \geq 1$ $o(n,j) \neq (n,i)$ is $\langle g^{(n,j)} \rangle \neq \langle g^{(n,i)} \rangle$? (recall: gcd's)

Answer: $|g^{(n,j)}| \neq |g^{(n,i)}|$

$\| \qquad\qquad\qquad\qquad \|$

$\frac{n}{(n,(n,j))} = \frac{n}{(n,j)} \qquad \frac{n}{(n,(n,i))} = \frac{n}{(n,i)}$

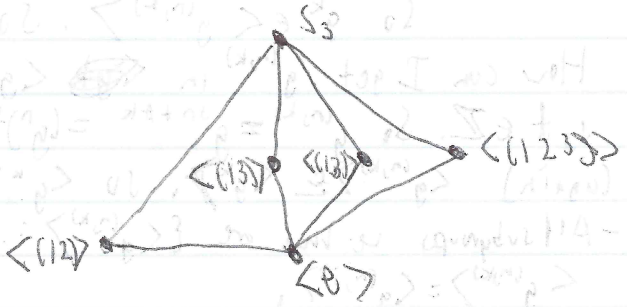
- **Lattice subgroups** - Ex) $\mathbb{Z}/12\mathbb{Z} \cong Z_{12}$



Note: What is a poset? Google it

More about lattices in a bit (lattice "=" poset (partially ordered set) w/ l.u.b.'s, g.l.b.'s)

Lattice of subgroups of S_3



- G is a group, A non empty subset of G:

$\langle A \rangle = \bigcap \{H \leq G : A \leq H\}$

$\uparrow$ subgroup generated by A

The intersection of a collection of subgroups of a group G, is again a subgroup of G.

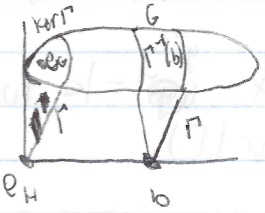
- Alternative characterizations of $\langle A \rangle$ using "words" in A (and A^{-1})

$\langle A \rangle = \{a_1^{\alpha(1)} \cdots a_k^{\alpha(k)} : k \in \mathbb{N},\ \alpha(i) \in \{1, -1\},\ i = 1, \ldots, k,\ a_i \in A\}$

$\uparrow$ words in $A \cup A^{-1}$.

$(a_1^{\alpha(1)} \cdots a_k^{\alpha(k)})^{-1} = (a_k^{-\alpha(k)} \cdots a_1^{-\alpha(1)})$ ✓

• $\Gamma : G \to K$ onto homo.

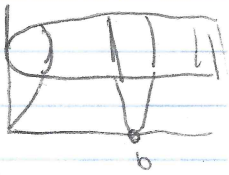


Ex| Fiber of e_K is $\ker\Gamma$

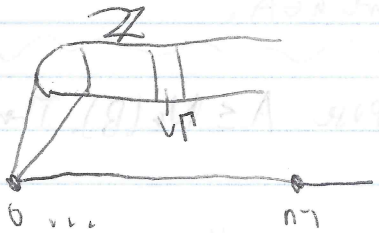
"Fiber over b" in $G = \Gamma^{-1}(b) = \{g \in G : \Gamma(g) = b\}$

- The fibers partition G.

could also be infinite so the blob could look like this:



Ex|



$\Gamma(z) = z \bmod n$

$\leftarrow Z_n$

Lemma: The partition $\{\Gamma^{-1}(b) : b \in K\}$ is compatible w/ the operation of G.

Proof: Let $u, v \in \Gamma^{-1}(b)$ & $w \in G$ with $w \in \Gamma^{-1}(c)$.

Now $\Gamma(uw) = \Gamma(u)\Gamma(w) = bc$

& $\Gamma(vw) = \Gamma(v)\Gamma(v) = bc$ which completes the proof. QED

- Could define a "new" group on $G/\ker(\Gamma)$

Pretty clear that $G/\ker(\Gamma) \cong K$

- Another take on the fibers:

Cosets of the $\ker(\Gamma)$. Let $g \in G$, $g\ker(\Gamma) = \{gk : k \in \ker(\Gamma)\}$

this is a left coset of the kernel.

- Claim: Each left coset is a fiber of some elt. $b \in K$ & each fiber is a left coset of $\ker(\Gamma)$.

- Let $g\ker(\Gamma)$ be a left coset of $\ker(\Gamma)$. We have

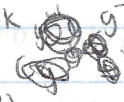
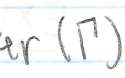
$\Gamma(g\ker(\Gamma)) = \{\Gamma(gk) : k \in \ker\Gamma\} = \{\Gamma(g) : k \in \ker\Gamma\} = \{\Gamma(g)\}$

So $g\ker\Gamma \subseteq$ fiber of $\Gamma(g)$.

cont. items on next page

cont. from previous page

• If $c \in G$ is in the fiber of $\Gamma(g)$, then $\Gamma(c) = \Gamma(g)$.

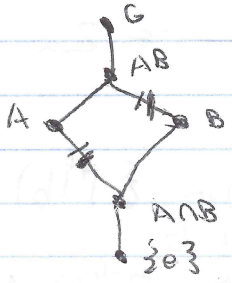
So $\Gamma(g) = e_K$  Then  $\in \ker(\Gamma)$, &  $= k$, some $k \in \ker(\Gamma)$. i.e. $c = gk \in g\ker(\Gamma)$.

• Now let's generalize. Let A be any group, $H \leq A$.
Then $aH = \{ah : h \in H\}$, where $a \in A$.

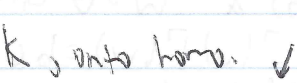
Call this ★J★

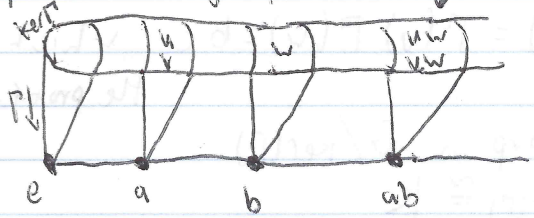
G is a group; $A, B \leq G$. Suppose $A \leq N_G(B)$. Then

1) $AB \leq G$
2) $B \trianglelefteq AB$
3) $A \cap B \trianglelefteq A$
4) $AB/B \cong A/A\cap B$



"Diamond"

$\Gamma : G \twoheadrightarrow K$, onto hom.  $\Gamma^{-1}(ab)$



$G/\ker\Gamma$: fibers of Γ in G.
The partition determined by fibers is <u>compatible</u> with <u>the operation of G</u>

& $G/\ker\Gamma$ is a group: $\Gamma^{-1}(a) \cdot \Gamma^{-1}(b) = \Gamma^{-1}(ab)$.
(fiber of a · fiber of b = fiber of (ab))

Identity, Inverses?
associativity is no problem.
identity is the kernel: $\ker(\Gamma)$
inverses $(\Gamma^{-1}(a))^{-1} = \Gamma^{-1}(a^{-1})$

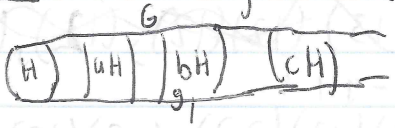
• Left cosets of $\ker\Gamma$ ... $u\ker\Gamma = \{uk : k \in \ker\Gamma\}$

<u>Lm.</u> If $u \in \Gamma^{-1}(u)$ (fiber of u), then $\Gamma^{-1}(u) = u\ker\Gamma$. i.e. proved this last time.

• Now we can consider $G/\ker\Gamma$ as consisting of left cosets of $\ker\Gamma$ in G.
$(u\ker\Gamma)(v\ker\Gamma) = uv(\ker\Gamma)$
Verify set equality, not just containment for this ←

• Given any $H \leq G$

Review: For $b \in G$, $bH = \{bh : h \in H\}$



* have to be able to prove these *

Staple of M521

1) $\forall b \in G$, $bH = H$ iff $b \in H$
2) $\forall a, b \in G$ $aH = bH$ iff $a^{-1}b \in H$
3) $\forall a, b \in G$, $aH \cap bH \neq \emptyset$ iff $aH = bH$.

3 says the cosets of H in G partition G.

Proof of #1: Suppose $bH = H$. Then since $H \leq G$, $e \in H$, & $b = be \in H$.
Conversely, if $b \in H$, then $bH \subseteq H$ by closure under the op.
Let $h \in H$. Look at $b^{-1}H$. Now $b^{-1}h \in H$, so $h \in bH$.

Proof of 2: You do it.

Proof of 3: Suppose $aH \cap bH \neq \emptyset$. Let $y \in aH \cap bH$. $\exists\ h_1, h_2 \in H$, $y = ah_1$, $y = bh_2$. So $yH \subseteq aH$ & $yH \subseteq bH$.
Complete the proof yourself

Notice if G is finite, $\forall a, b \in G$, $|aH| = |H| = |bH|$.

↪ each blob has the same # of elts. $|G|$ = # of cosets of H × $|H|$

So $|H| \mid |G|$, Lagrange's thm.

• Corollaries: G is finite, $g \in G$. Then $|g| \mid |G|$.
Proof: We've seen that $|g| = |\langle g \rangle|$. Thus it follows $|g| \mid |G|$ QED

• $|G| = p$, prime, then $G \cong Z_p$
Proof: Let $g \in G - \{e\}$, then $|g| \mid |G| = p$. Since $g \neq e$, $|g| > 1$, thus $|g| = p$. But $|\langle g \rangle| = p$, so $\langle g \rangle = G$. So it's isomorphic to Z_p.
wrt. QED.

Me

- Under what conditions does the set of cosets of H ($H \leq G$) admit a multiplication st. we could talk about G/H?

Look at: $S_3 \geq \langle (12) \rangle = H$

$\{e, (12)\}$ | $\{(13), (13)(12)\}$ | $\{(23), (23)(12)\}$

$= (123)$ $= (132)$

~~$(13)H\,(12)H = ?$~~

~~$= \{(13)(12), (13)(12)(12), (12)\}$~~

this example technically wrong

$(13)H(23)H = ? = gH$?

$= \{(13)(23), (13)(12)(23), (13)(12), (13)(23)(12)\}$

$= \{(213), (12), (123), (123)\}$

$\neq gH$ it's too big

Moral of the story: this doesn't necessarily work.

- Def: (Refresher):

– $A \subseteq G$, $C_G(A) = \{g \in G : \forall a \in A,\ ga = ag\}$ or $gag^{-1} = a$ centralizer of A

We proved $C_G(A) \leq G$

– $N_G(A)$ normalizer $= \{g \in G : gAg^{-1} = A\}$

So $C_G(A) \subseteq N_G(A)$

Check $C_G(A) \leq N_G(A)$ ← might be useful.

- Def: A subgroup N in G is normal if $\forall\ g \in G$, $gNg^{-1} = N$. (denoted $N \trianglelefteq G$)

- Ex: TFAE: $N \trianglelefteq G$ iff $\forall g \in G$, $gNg^{-1} \subseteq N$.

- Lemma: $N \trianglelefteq G$ iff $\forall g \in G$, $gN = Ng$ iff $\forall g, h \in G$, $gNhN = ghN$.

proof on next page

Proof: Suppose $N \trianglelefteq G$, & consider gN, we know that for $n \in N$, $gng^{-1} = n'$, some $n' \in N$. So we have $gn = n'g \in Ng$

The other containment can be done essentially the same way.

Now suppose $\forall\, g \in G$, $gN = Ng$. So $gNg^{-1} = Ngg^{-1} = N$.

- For the next part, if $N \trianglelefteq G$ & $g, h \in G$, $n_1, n_2, n_3 \in N$

$gn_1hn_2 = ghh^{-1}n_3h^{-1}hn_2 = ghn_3n_2$

$n_3n_2 \in N$ so we get ghN for some $n_3 \in N$

So we get $gNhN = ghN$.

could also do it this way: $gNhN = g(Nh)N = ghNN = ghN$ by associativity.

- It's an exercise to show $ghN \subseteq gNhN$.

I we'll leave the other direction for an exercise. It can be done in a # of ways.

Note: the other direction is "$\forall\, g, h \in G$, $gNhN = ghN \Rightarrow N \trianglelefteq G$".

* So if $N \trianglelefteq G$, we can form the quotient group G/N w/ mult. $gNhN := ghN$.

G/N is a group: assoc is inherited, N is the identity elt. of G/N, & $(gN)^{-1} = g^{-1}N$

* Lemma: $N \trianglelefteq G$ iff N is the kernel of some onto homo. $\exists$ a group K & $\Gamma : G \twoheadrightarrow K$.

* Lemma: If $\Gamma : G \to K$, is a homo. then $\ker \Gamma \trianglelefteq G$.

Proof: If $g \in G$, $n \in \ker G$, $\Gamma(gng^{-1}) = \Gamma(g)\Gamma(n)\Gamma(g)^{-1} = \Gamma(g)\Gamma(g)^{-1} = e$. ($\Gamma(n) = e$)

Proof: Suppose $N \trianglelefteq G$.

Let $K = G/N$, consider $\Gamma : G \to G/N$, $g \mapsto gN$.

$u, v \in G$.

$\Gamma(uv) = uvN = uNvN = \Gamma(u)\Gamma(v)$. Now let $g \in \ker \Gamma$,

$\Gamma(g) = gN = N$ iff $g \in N$ by that coset property.

idea for the day

TFAE - the following are equivalent

things we'll be going over

1. Normality ✓
2. $aHbH = yH$ ... condition ✓
3. $\ker \Gamma \trianglelefteq G$ ✓
4. $N \trianglelefteq G$ iff $\exists \ldots \Gamma \ldots$ ✓
5. $|HK| =$
6. $HK \leq G$ iff $HK = KH$
7. Isomorphisms
8. S_n

• Normality ... normal subgroups

$H \leq G$

TFAE: (1) $H \trianglelefteq G$ (2) $\forall g \in G, gH = Hg$

(3) $gHg^{-1} \subseteq H$ (4) $\forall a, b \in G \; aHbH = abH$

if $H = N$ normal, we have a well defined factor group.

4 means that we can define

G/H ← "quotient group" the elements are the left cosets of H in G.

- Another equivalence is (5) $H \trianglelefteq G$ iff $\forall a, b \in G, \exists y \in G$ $\ni aHbH = yH$ & $yH = abH$

- why it's true: Since $e \in H$, $aHbH = yH$

$\Rightarrow ab \in yH$ iff $abH = yH$. Now easy to show $H \trianglelefteq G$.

- we showed last time that $\ker(\Gamma) \trianglelefteq G$ when $\Gamma: G \to K$ is a homomorphism.

→> onto - Lemma: If G is a group & $N \trianglelefteq G$, then $\exists$ a group K & a homo. $\Gamma: G \to K$ $\ni N = \ker \Gamma$.

Proof: Let $K = G/N$. Let $\Gamma: G \to G/N$

$g \mapsto gN$

We have for $g, h \in G$, $\Gamma(gh) = ghN$. b/c $N \trianglelefteq G$,

$= gNhN = \Gamma(g)\Gamma(h)$

So $\Gamma(g) = gN = N$

iff $g \in N$, so $N = \ker(\Gamma)$. QED

- Thm: (1st Isomorphism Thm):
If $\Gamma : G \to K$ (onto homo.), then $G/\ker(\Gamma) \cong K$

Proof: Let $\Gamma^* : G/\ker\Gamma \to K$, where $\Gamma^*(u \ker\Gamma) = \Gamma(u)$.
must verify Γ^* is well defined, Γ^* is a homo, & Γ^* is a bijection.
well defined: cosets of $\ker\Gamma$ are fibers. so it's well defined.
it's a homomorphism b/c it's basically trivial to verify.
Γ^* is onto b/c Γ is onto. If $\Gamma^*(g\ker\Gamma) = \Gamma^*(h\ker\Gamma)$
iff $\Gamma(g) = \Gamma(h)$ &
by properties of homomorphisms, iff $\Gamma(g^{-1}h) = e$ iff $g^{-1}h \in \ker\Gamma$
iff $g\ker\Gamma = h\ker\Gamma$ so it's one-to-one. QED.

Comment: To locate all homomorphic images of a group G suffices to look at or know it's normal subgroups... & all it's homo. images are G/N, $N \trianglelefteq G$.

- segway back to subgroups

- Proposition: G is a finite group, $H, K \leq G$. $|HK| = \frac{|H||K|}{|H \cap K|}$.
- Comments - HK is not necessarily a subgroup.
Ex) $S_3 = G$, $\langle(12)\rangle\langle(13)\rangle = \{e, (12), (13), (12)(13)\}$
by Lagrange's Thm, this isn't a subgroup.

Proof of prop: Note $HK = \bigcup \{hK : h \in H\}$
↑ union of left cosets of K in G.
so we could have $a, b \in H$, $a \neq b$, could have $aK = bK$.
we have $a, b \in H$, $aK = bK$ iff $a^{-1}b \in K$
but $a, b \in H$, so $a^{-1}b \in K \cap H$, we're here. So we're looking for the # of distinct left cosets of $H \cap K$ in K, of which there are $|K| / |K \cap H|$
So then we do the same with right cosets & H to get
$\frac{|H||K|}{|H \cap K|}$ QED.

- When is $HK \leq G$?

Lemma: $H, K \leq G$, $HK \leq G$ iff $HK = KH$.

↑ does not mean the elements commute, rather, it has to do w/ cosets.

counter example: $G = D_8$

$\langle r \rangle \langle s \rangle = D_8$

so by the lemma,

$\langle r \rangle \langle s \rangle = \langle s \rangle \langle r \rangle$, but they most certainly don't commute.

Proof will be saved for next time.

- Recall the "diamond" from ✡ J ✡ (flip back 3 pages to the page. that is the 2nd Isomorphism picture.

hypothesis is $A, B \leq G$, $A \leq N_G(B)$.

Then ✡J✡ is true.

why? 1) $AB \leq G$: Let $a \in A$, $b \in B$, look at ab, & $aba^{-1} a \in B$ ($b' \in B$)

so apparently $AB \leq BA$. so the other direction is easy.

2) $B \trianglelefteq AB$: $a \in A, b \in B, b' \in B$ ... $(ab)b'(ab)^{-1} = \underbrace{abb'b^{-1}}_{B} a^{-1} = b''$

3) $A \cap B \trianglelefteq A$ trivial. must use to prove it

4) $AB/B \cong A/A\cap B$ ↓

Let $\Gamma : A \to AB/B$

$\ker(\Gamma) = A \cap B$, then we just need Γ to be onto, then by the 1st isomorphism thm, we're done.

well, $a \mapsto aB$

Is Γ a hom, is it onto, & what is it's kernel?

Let $a_1, a_2 \in A$, so $\Gamma(a_1 a_2) = a_1 a_2 B = a_1 B \, a_2 B = \Gamma(a_1)\Gamma(a_2)$ by normality.

If $a \in A, b \in B$, $abB \in AB/B$

Find pre image of $abB = aB$ & $\Gamma(a) = abB = aB$ so onto.

$x \in \ker\Gamma$ means $\Gamma(x) = B$, iff $xB = B$ iff $x \in B$ & $x \in A$, so if $x \in A \cap B$. so the kernel is correct, so by the 1st isomorphism thm. the image is isomorphic to the preimage: $\frac{AB}{B} \cong \frac{A}{A\cap B}$ QED.

• It's been a while:
$H, K \leq G$, form $HK = \{hk : h \in H, k \in K\}$
Ex $\langle (12) \rangle = H$, $\langle (13) \rangle = K$.
$|HK| = 4$ ✗, but $4 \nmid 6 = |S_3|$ so $HK \not\leq G = S_3$.

• Lemma: $HK \leq G$ iff $HK = KH$.

Ex D_{2n} ... $\langle s \rangle \langle r \rangle = D_{2n} \leq D_{2n}$ but by the lemma,
$\langle r \rangle \langle s \rangle = \langle s \rangle \langle r \rangle$,
However $s \in \langle s \rangle$, $r \in \langle r \rangle$, but $sr \neq rs$.

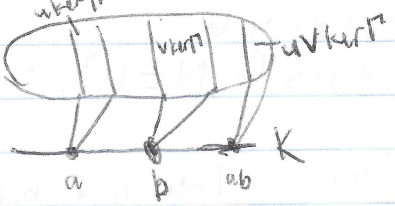
doesn't mean commutivity

↳ Proof of previous lemma: Suppose $HK \leq G$ ...
Let $h \in H$ & $k \in K$. So hk is generic elt. in $HK \leq G$, so
$\exists\, y \in HK \ni (hk)^{-1} = y$. So $y = h_1 k_1$ & $hk = k_1^{-1} h_1^{-1} \in KH$.
Now $H \subseteq HK$, $K \subseteq HK$. Since $HK \leq G$. So $KH \subseteq HK$.
the opposite direction is similar.

Now suppose $HK = KH$. Let $h_1 k_1, h_2 k_2 \in HK$. Now
$h_1 k_1 (h_2 k_2)^{-1} = h_1 k_1 k_2^{-1} h_2^{-1}$
$= h_1 h^* k^*$ where $h^* \in H$ & $k^* \in K$
$\in HK$ note $h^* \neq h_2^{-1}$ & $k^* \neq h_1 k_2^{-1}$

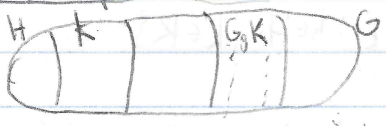
• Lemma: $N \trianglelefteq G \Rightarrow \exists\, K$ which is a group, & hom. $\Gamma : G \to K$ w/ $\ker \Gamma = N$.
Proof: flip back a page. we've already done this.

• 1st Isomorphism Thm: If $\Gamma : G \twoheadrightarrow K$ then $G/\ker\Gamma \cong K$.



• 2nd Isomorphism Thm: mentioned earlier. If needed, check out the book.

• 3rd Isomorphism Thm: $G \trianglerighteq K$, $G \trianglerighteq H$, $K \geq H$.



Notice K/H is a disjoint of cosets of H.

so $\frac{G/H}{K/H} \cong G/K$

Proof: We have to show $G/H \trianglerighteq K/H$.

Let $kH \in K/H$, $k \in H$. Let $g \in G$ & consider $gH(kH)g^{-1}$

b/c $H \trianglerighteq G$, $= gkg^{-1}H$

b/c $k \in G$ $= k_x H$ where $k_x \in K$

$\in K/H$.

(We'll show $K/H \leq G/H$ later in 4th Isomorphism thm.)

Let $\Gamma : \frac{G}{H} \to G/K$, so $\Gamma(gH) = gK$. Now $u \in G$,

$\Gamma(gHuH) = \Gamma(guH)$ by normality

$= guK = gKuK$ Thus Γ is a homo.

Let $gK \in G/K$, now $\Gamma(gH) = gK$, so Γ is an onto homo.

By the 1st Isomorphism thm, after checking $\ker \Gamma = K/H$,

$G/K \cong \frac{G/H}{K/H}$ $\quad \Gamma$

to do this $\Gamma(gH) = gK$, then

ie $g \in K$ ~~$(gH)K = K$ or $gK = K$.~~

so $gH \in \frac{K}{H}$. QED.

• G is a group, $N \trianglerighteq G$

Sub(G) ...

lattice of subgroups of G

$I[N, G] = \{H \leq G : N \leq H\}$, the interval

sub G/N

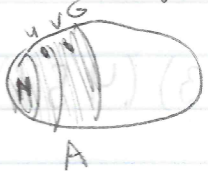
There is a bijective order preserving function ~~from~~ $I[N, G] \to$ Sub(G/N) under $F : I[N, G] \to$ Sub(G/N)

$F(H) = H/N$. It's fairly obvious that $H \leq G \Rightarrow \frac{H}{N} \leq G/N$.

If h_1N & $h_2N \in HN$, then $h_1N(h_2N)^{-1} = h_1h_2^{-1}N \in H/N$ can

Continued: $h_1 h_2^{-1} N \in H/N$ since $H \leq G$.

Def'n: Let $A \leq G/N$, A a subset of left cosets of N in G.
Let $\hat{A} \leq G$ consist of elts in G contained in the cosets of G.



$\hat{A} \leq G$, $N \leq \hat{A}$.
$u \in g_1 N \in A$, $v \in g_2 N \in A$
$uv^{-1} \in g_1 g_2^{-1} N \in A$

• S_n = perms of $\{1, \ldots, n\}$. $\alpha \in S_n$

How does α affect the order of the subsets?

let $n=3$ $\alpha = (12)$ (123)

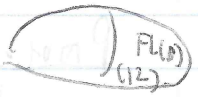
$\beta \in S_n$

$X := \{(i,j) : n \geq j > i \geq 1\}$

Ex) $n=3$ $\{(1,2), (2,3), (1,3)\}$

"Apply" β to X.

Let $\beta = \alpha = (12)$



Define a subset of S_n: even elts. of S_n are those whose flipped set has an even # of elts. "GUD".

• What we'll start w/ next time:

There's a function $\Gamma : S_n \to Z_2 = \{0, 1\}$

$$\Gamma(\beta) = \begin{cases} 0 & \text{if } \beta \text{ is even} \\ 1 & \text{if } \beta \text{ is odd} \end{cases}$$

We'll show Γ is a homomorphism. $\ker \Gamma$ = "evens"

Talking about S_n $\{1, 2, \ldots, n\}$

$\beta \in S_n$, then $\exists$ a representation $\beta = \alpha_1 \cdots \alpha_k$ where α_i's are cycles & the cycles are pairwise disjoint.

Ex) S_6 $\quad x \quad 1\ 2\ 3\ 4\ 5\ 6$

$\alpha(x) \quad 3\ 2\ 1\ 5\ 6\ 4 \qquad (13)(456)$ ← disjoint cycle representation.

$|\beta| = \text{lcm}(|\alpha_1|, \ldots, |\alpha_k|)$

- transpositions (or 2-cycles) (ij) $i \neq j$
- Putting things together:

Every $\beta \in S_n$ can be represented as a prod. of transpositions:

ex) $(456)(13)$

$= (46)(45)(13)$

Apparently $S_n = \langle (ij) : n \geq j \geq i \geq 1 \rangle$

S_X groups are really important, where X is a set.

finite Cayley's Thm. → Ex) If G is finite $\exists\ n \in \mathbb{N} \Rightarrow G \hookrightarrow S_n$

"embed" "homo. that's injective"

Proof: Let G be a finite group.

Let $\Phi : G \to S(G)$, where $\Phi(g)(h) = gh$, $\forall\ h, g \in G$.

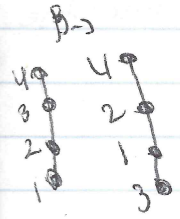
phi of g of h

It's one-to-one by cancellation ... so it's an inj

Also, $\forall x \in G$: $\Phi(gh)(x) = (gh)x = g(hx) = \Phi(g)(\Phi(h)(x))$ $\forall\ x \in G$.

Thus $\Phi(gh) = \Phi(g) \circ \Phi(h)$

$\beta =$



$|\text{Flip}(\beta)|$

$= 2$

$= \{(3,1), (1,3)\}$

We'll decompose S_n into 2 disjoint subsets as follows...

We've skipped around.

$\Gamma : S_n \to \{0, 1\}$ where $\Gamma(\alpha) = \begin{cases} 0 & \text{if } |\text{Flip}(\alpha)| \text{ is even} \\ 1 & \text{if } |\text{Flip}(\alpha)| \text{ is odd} \end{cases}$

Ex): in S_4, $|\text{Flip}(13)| = 3$ so $\Gamma((13)) = 1$

$\Gamma((123)) = 0$

Consider $\Gamma: S_n \to (\langle 0,1 \rangle, +)$ where $\Gamma(\alpha) = \begin{cases} 0 & \text{as before} \\ 1 & \text{if it is} \end{cases}$

Proposition: Γ is a homomorphism

Proof: Let $\alpha, \theta \in S_n$

Consider $\Gamma(\theta\alpha)$

$|Flip(\alpha)| = j$ & $|Flip(\theta)| = k = k_1 + k_2$ where k_1 is # of pairs flipped by α & θ.

So $|Flip(\theta\alpha)| = j - k_1 + k_2$ this is almost equal to $j + k_1 + k_2$

so $(j - k_1 + k_2) \bmod 2 = (j + k_1 + k_2) \bmod 2$

It follows that Γ is a homomorphism. QED.

The kernel of Γ is the even permutations. So the $\ker\Gamma$ is a normal subgroup, called A_n.

Ex| $A_3 = \{e, (123), (132)\}$.

We've observed that (12) is odd. Claim: (ij), $n \geq i > j \geq 1$.

Find $\beta \in S_n$ s.t. $\beta(12)\beta^{-1} = (ij)$

where $\beta(1) = i$ & $\beta(2) = j$.

Now,

$$\Gamma(\beta(12)\beta^{-1}) = \Gamma(\beta) + \Gamma((12)) + \Gamma(\beta^{-1})$$
$$= \Gamma(\beta) + 1 - \Gamma(\beta) = 1$$

- All transpositions are odd... so A_n is the subset of S_n consisting of perms representable as a product of an even # of transpositions.
- So what is $|A_n|$?

$S_n = A_n \cup (12) A_n$

If β is odd, $\beta = (ij)(i_2j_2)\cdots(i_kj_k)$

k is odd, $k-1$ is even $= (ij)\gamma$, $\gamma \in A_n$.

So $|A_n| = n!/2 = \frac{n!}{2}$

Def: An in a non trivial group G is simple. Its only normal subgroups are $\{e\}, G$.

- Suppose $[G:H]=2$ (just 2 cosets). Then $H \trianglelefteq G$.

Proof: Since $[G:H]=2$, $\exists\ g \in G \ni$

$G = H \cup gH$ (H | gH) i.e. disjoint union is $\cup$

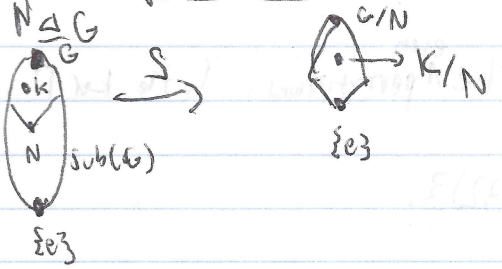
Of course $Hg \cap H = \emptyset$ b/c $g \notin H$. & $G = H \cup Hg$.

The conclusion is that $Hg = gH$.

Now not difficult to show $\forall\ b \in G$, $bH = Hb$.

So $H \trianglelefteq G$.

- 4th Isomorphism Thm. (we've seen this before)



There's a function

$S: \text{sub}(G) \to \text{sub}(G/N)$

$\cup$

$S: I[N, G] \to \text{Sub}(G/N)$

s.t. $S(K) = K/N$.

$= \{kN \mid k \in K\}$.

So we have to show this is a well defined map that's a bijection. S is an order preserving bijection.

Consider $B \leq G/N$

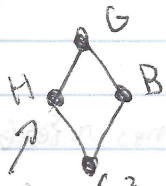
so $S^{-1}(B)$ is nonempty b/c onto.

$S^{-1}(B)$ = twice elts of G in the cosets that form B.

- If K is normal in G, (K ≥ N), then K/N is normal in G/N.

Conversely, if $B \trianglelefteq G/N$, $S^{-1}(B) \trianglelefteq G$.

can see this in a lattice diagram.

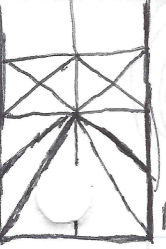


maximal b/c it's directly under G

- Let G be a group. Then a subgroup $H \leq G$ is maximal if H is a proper subgroup & if $K \leq G$ & $H \leq K$, then $K = G$.
  - $N \trianglelefteq G$ is maximal normal subgroup of G, if N is a proper subgroup & if $J \trianglelefteq G$, $N \leq J$, Then $J = G$.
  - It's clear that a finite group has maximal subgroups & it has maximal normal subgroups.

Ex| $\langle (12) \rangle$ → not normal, but maximal subgroup in S_3.

$\langle (123) \rangle$ → maximal normal subgroup in S_3.



Maximality cont.

- Could have a maximal normal subgroup that isn't maximal.
- G is <u>simple</u> if its only normal subgroups are G & $\{e\}$.
- Last time we classified the simple Abelian groups:
  $\mathbb{Z}_p$ — p is prime.

Lemma Let G be a group. $N \trianglelefteq G$, then G/N simple iff N is a maximal normal subgroup.

<u>Proof</u>: If N is maximal in G, then the 4th isomorphism thm guarantees that G/N has no proper nontrivial normal subgroups. i.e., G/N is simple.

- <u>Composition series</u>
  - $\{e\} \trianglelefteq N_1 \trianglelefteq N_2 \dots \trianglelefteq N_k = G$ where $N_i \trianglelefteq N_{i+1}$ for $i = 0, \dots, k-1$.
  - ✱ [we're not saying that the N_i's are normal in G] ✱
    ↓ N_{i+1}/N_i is simple.
  - <u>Lemma</u>: If G is finite then G has a composition series.

<u>Ex</u> $\mathbb{Z}_2 \times \mathbb{Z}_3$

comp. series → $\{e\} \trianglelefteq \mathbb{Z}_2 \times e \trianglelefteq \mathbb{Z}_2 \times \mathbb{Z}_3$

$\{e\} \trianglelefteq e \times \mathbb{Z}_3 \trianglelefteq \mathbb{Z}_2 \times \mathbb{Z}_3$

↑ both are simple composition series, but notice there can be more than one.

<u>Ex</u> Consider D_8

$\{e\} \trianglelefteq \langle r^2 \rangle \trianglelefteq \langle r \rangle \trianglelefteq D_8$ $\quad [D_8 : \langle r \rangle] = \frac{4}{2} = 2$

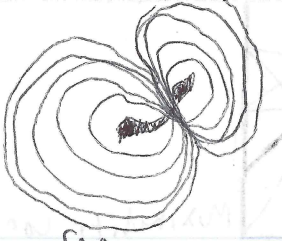
Factors in this series are simple. $D_8/\langle r \rangle$ is simple.

✱ Note factors are the N_{i+1}/N_i from def. ✱

- <u>Holder's Thm</u>

Let G be a group. The factors given ✱ 2 composition series for G, the factors, including multiplicities, are the same.

If proofs aren't in the notes, always check the book!



- Def: G is solvable if it has a composition series all of whose factors are Abelian.

Note: Abelian $\Rightarrow$ solvable
But D_8 is solvable but not Abelian.
A_5 is the smallest example of not solvable. (even permutations)

- Orbit-Stabilizer Thm

Review: G is acting on a set A. Let $b \in A$, $\mathcal{O}_b = \{g \cdot b \mid g \in G\}$.
G_b = stabilizer of b under this action $= \{g \in G \mid g \cdot b = b\}$.

Ex: $G = S_3$, G acts on $G = A$ by conjugation.
ie. $g \cdot h = ghg^{-1}$
$st \cdot h = sthts^{-1} = sthts^{-1} = s \cdot (t \cdot h)$ ✓

$\mathcal{O}_e = \{e\}$
$\mathcal{O}_{(12)} = \{(i\ j) \mid 3 \geq i \geq j \geq 1\}$
$\mathcal{O}_{(123)} = \{(123), (132)\}$

- Now the Thm (Orbit stabilizer Thm)
G acts on A, $b \in A$, then $|\mathcal{O}_b| = [G : G_b]$

Proof:
$\forall\ g, h \in G$, any $b \in A$, $g \cdot b = h \cdot b$
iff $g^{-1}h \in G_b$ iff $gG_b = hG_b$

- Ex: Let G act on itself by conjugation. So $G = A$...
$\forall\ g, h \in G$, $g \cdot h = ghg^{-1}$. Defines a very important action.

- By the orbit-stabilizer Thm, there's a relationship
$\mathcal{O}_h = \{ghg^{-1} \mid g \in G\}$
$|\mathcal{O}_h| = [G : C_G(h)]$

Ex) With the previous action (conjugation) & $G = S_n$, the orbits under this action are determined by "partitions of n"

e.g. S_4

$\mathcal{O}((123)) = \mathcal{O}_{(123)} = \{\beta(123)\beta^{-1} = (\beta(1)\beta(2)\beta(3))\}$ so we get all elements in S_4 of a given shape (in this case a 3-cycle)

$\mathcal{O}_{(12)(34)} =$

"shape" is 2,2

- Review $Z(G)$ (the center of the group)

$Z = \{g \in G \mid \forall h \in G,\ hg = gh$ ie. $hgh^{-1} = g\}$

Ex) G is abelian iff $Z(G) = G$.

$Z(S_3) = \{e\}$

$Z(D_8) = \{e, r^2\}$

- $Z(G) \trianglelefteq G$ → really easy to prove (probably in book)

- Automorphisms of a group G, Γ is an automorph. if $\Gamma: G \to G$ that is an isomorphism.

- he have a special class of automorphisms:

Let $g \in G$, & Let $h^g := ghg^{-1}$ ↪ this is just a notation thing

$x^g: G \to G$ where $x^g(h) := h^g$

review this def.

$\forall g \in G$, $x^g: G \to G$,

↳ x^g is an automorphism. → Proof probably in book.

↳ - $Inn(G)$ → inner automorphisms of G

↳ $= \{x^g \mid g \in G\}$

note: $Inn(G)$ = automorphisms under conjugation

Let $Aut(G)$ be the set of all automorphs of G. Observe that $Aut(G)$ is a group where the operation is composition.

- Note $Inn(G) \leq Aut(G)$

Think about whether or not this is normal.

- Think $Aut(Z_n)$. Here our group is abelian. Well, If G is Abelian iff $Inn(G) = \{e\}$.

- Suppose $\phi \in Aut(Z_n)$ & let $\phi(1) = k$.
ϕ is a hom. $\forall\, m \in Z_n$ so $\phi(m) = mk$.
Also $\phi(Z_n) = \langle k \rangle$ (all powers of k)
For ϕ to be onto, k must generate Z_n.
So $\phi(x) = kx$ is onto iff ϕ is an automorph. iff
$\langle k \rangle = Z_n$ iff $(k, n) = 1$
Remember: $Z_n^\times$ is invertible elements of Z_n under mlt.

• Define a map $\Gamma : G \to Inn(G)$
So $\Gamma(g) = x^g$ ie, $\Gamma(g)(h) = ghg^{-1} = x^g(h)$
Let $g, h \in G$, then
can be proved on our own. → $\Gamma(gh) = x^{gh} = (x^g)^h = \Gamma(g)\Gamma(h)$ ✓ so Γ is a hom.

- What is $\ker(\Gamma)$? ↳ the center.
It's $Z(G) = \ker(\Gamma)$.
So by the first isomorphism Thm,
$G/Z(G) \cong Inn(G)$, Hmmmm...

• Let G be a finite group, G acts on G by conjugation.
Orbits = conjugacy classes.
These conjugacy classes partition G.

Here's our partition

$$\underbrace{\{e\} \mid \{z\} \mid \dots \mid \{z_k\}}_{\text{singleton conjugacy}} \mid \underbrace{\{a_1, \dots\} \mid \{a_2, \dots\} \mid \dots \mid \{a_\ell, \dots\}}_{\text{chosen a representative from each non-singleton conjugacy class.}}$$

Each one is in $Z(G)$ & conversely

a_i's

This leads us to...

★ - Class Equation: $|G| = |Z(G)| + \sum_{i=1}^{\ell} C_G(a_i)$

$= |Z(G)| + \sum_{i=1}^{\ell} [G : C(a_i)]$

- Note in this equation, $\forall a_i$, by the orbit-stab. Thm, $[G : C(a_i)]$ = # of elts in the conjugacy class of a_i.

• **Def:** A group G is a p-group (where p is a prime) if $|G| = p^n$ where $n \in \mathbb{N}$.

- We saw that $Z(G) = \{e\}$ where $G = S_3$.

- **Lemma:** If G is a p-group, then $Z(G)$ is non-trivial.

Proof:

What do we know about $[G : C(a_i)]$ if a_i is not in $Z(G)$? ie, $C(a_i)$ is a proper subgroup of G, so $[G : C(a_i)] = p^i$ where $i > 0$.

So $\forall a_i$, $p \mid [G : C(a_i)]$. So $\sum_{i=1}^{\ell} [G : C(a_i)]$ (the sum of the sizes of the non-$Z(G)$ conjugacy classes) is a multiple of p.

Since $|G| = p^n = |Z(G)| + p^r$ where $r \in \mathbb{N} \Rightarrow p \mid |Z(G)|$

$\Rightarrow Z(G)$ is non trivial. QED.

- **Lemma:** Suppose G is a finite group & $G/Z(G)$ is cyclic, then G is Abelian.

Proof: Let $u, v \in G$. We have also that $G/Z(G) = \langle h Z(G) \rangle$.

So for some $j, k \in \mathbb{N} \cup \{0\}$, $u \in h^j Z(G)$

$v \in h^k Z(G)$

ie. $\exists\ u = h^j z_u$ & $v = h^k z_v$ & $\exists$ elements $z_u, z_v \in Z(G)$.

Now $h^j z_u h^k z_v = uv$

WTS $uv = vu$ ie $h^j z_u h^k z_v = h^k z_v h^j z_u$.

Well, $h^j z_u h^k z_v = h^j h^k z_u z_v = h^k h^j z_u z_v = h^k z_v h^j z_u = vu$.

QED.

- **Corollary:** $|G| = p^2$ where p is prime, then G is Abelian.

Proof: If $Z(G) = G$, we're done.

Otherwise $|Z(G)| = p$ bc we showed $Z(G)$ is non-trivial.

Now $G/Z(G) \cong \mathbb{Z}_p$ by cardinality, which is cyclic. Now apply the last result. QED

~~•~~ • P is prime, Consider $|g| = ps \Rightarrow |g^s| = \frac{ps}{(ps)} = \frac{ps}{s} = p$

Important Problem. → • G is abelian & $p \mid |G| \Rightarrow \exists g \in G$, $|g| = p$.

Proof: $|G| = p^{\alpha} m$ where $(m, p) = 1$ & $\alpha \in \mathbb{N}$. Proof is by induction on ~~[illegible]~~ $|G|$.

Base case: $|G| = p$. By earlier results, $G \cong \mathbb{Z}_p$ which has an element of order p.

Hypothesis: Assume $\forall$ groups $|G|$, $p \mid |G|$ of order less than k that such G have elts. of order p.

Step: Suppose $|G| = K$. If G has a proper (non-trivial) subgroup J w/ $p \mid |J|$, so by the induction hypothesis, $\exists$ $j \in J$ w/ order p. B/c $J \leq G$, we're done. ~~[illegible]~~

Note J is non-trivial & proper — such a subgroup exists since $G \neq \mathbb{Z}_p$. We know $J \trianglelefteq G$.

Suppose $p \nmid |J|$, where J is non-trivial. Since G is abelian, $J \trianglelefteq G$.

Consider G/J (an abelian group), we know $|G/J| = |G|/|J|$

So $p \mid |G/J|$. Well $|G/J| < K$.

So G/J has an elt of order p. Let $|gJ| = p$ where $g \in G$.

Note that $g^{|gJ|} = e \in J$. We've shown $|gJ| = \min\{b \mid g^b \in J\}$.

So $p \mid |g|$. Now $\exists s \in \mathbb{N} \ni |G| = ps$. B/ ~~[illegible]~~, $|g^s| = p$.

QED.

• This is sort of a converse of Lagrange's Thm, right?

Let's look at A_4, well $|A_4| = 12$ (b/c $S_4 = 4! = 24$)

Lemma: A_4 has no subgroup of order 6.

Proof: By contradiction, assume A_4 has a subgroup $H \ni |H| = 6$, so $H \trianglelefteq A_4$ b/c $[A_4 : H] = 2$ & we're proved.

So $A_4 = H \cup gH$ where $g \in A_4 \setminus H$. Observation: $g^2 \in H$, or not $g = g^{-1}g^2 \in H$. Now all 8 3-cycles ~~[illegible]~~ in S_4 are in A_4. This means $\exists \alpha \notin H$, $|\alpha| = 3$ (3-cycle). But $\alpha^2 \in H$, so $(\alpha^2)^2 \in H$, but $(\alpha^2)^2 = \alpha$, thus we have our contradiction of the choice of α.

QED.

• Def: $|G| = p^\alpha m$ where $(p, m) = 1$, $\alpha \in \mathbb{N}$.

Def: A sylow p-subgroup P of G is a subgroup satisfying $|P| = p^\alpha$.

Ex) S_4 ... $|S_4| = 2^3 \cdot 3$

Consider $D_8 \leq S_4$ is a sylow-2 subgroup.

• Sylow's Thm (for real now)

1) $\exists$ at least one subgroup of order p^α (ie. $\exists$ sylow p-subgroups).
2) If Q is a p-subgroup of G, then $\exists$ a sylow-p subgroup $P \ni Q \leq P$
3) Sylow p-subgroups are pairwise conjugate, ie. if P_1, P_2 are P-sylow, then $\exists\ g \in G$, $gP_1g^{-1} = P_2$.
4) With n_p (the number of p-sylow subgroups), $n_p \equiv 1 \bmod p$ & $n_p \mid m$.

Proof: 1) We'll use induction here.

$|G| = p^\alpha m$: Base case: $|G| = p$, then G itself is the p-sylow;

Hypothesis: Suppose for some $K \in \mathbb{N}$, all groups H, $|H| = p^\Delta n < K$ we have a sylow group.

Step: Suppose $|G| = k = p^\alpha m$.

- case1) $p \mid |Z(G)|$. Note that $Z(G) \trianglelefteq G$, moreover if $A \leq Z(G)$, then $A \trianglelefteq G$. Since $Z(G)$ is Abelian, & $p \mid |Z(G)|$, $\exists\ g \in Z(G)$, $|g| = p$ ie. we can take $\langle g \rangle$. We know $\langle g \rangle \trianglelefteq G$.

If $\alpha = 1$, then $\langle g \rangle$ is our p-sylow. Assume $\alpha > 1$. Consider $G/\langle g \rangle$. We know $|G/\langle g \rangle| = p^{\alpha-1} m$, $m - 1 > 0$. By induction hypothesis, since $|G/\langle g \rangle| < k$, it has a sylow p-subgroup P_0, of order $p^{\alpha-1}$. We pull back P_0 into G & we get a subgroup P of order p^α.

- Case 2) $p \nmid |Z(G)|$. Consider Class equation, $|G| = |Z(G)| + \sum_{i=1}^{k} [G : C_G(a_i)]$. Since $p \mid |G|$ & $p \nmid |Z(G)|$, so $\exists\ a_i \ni p \nmid [G : C_G(a_i)]$. Now $p^\alpha m = |G|$ & $[G : C_G(a_i)] = |G| / |C_G(a_i)|$, so $p^\alpha \mid |C_G(a_i)|$ but since $a_i \in Z(G)$, $C_G(a_i)$ is not all of G. Apply induction hypothesis to the centralizer $Z(G)$ & find a subgroup of order p^α. So we've found our Sylow-p in G.

The rest of the proof should be read.

Cauchy's Thm

- **Corollary:** $p \mid |G|$, then $\exists$ an element $g \in G$, $|g| = p$

  Proof: $|G| = p^\alpha m$, for some $\alpha \in \mathbb{N}$, $(p, m) = 1$.

  So $\exists$ P_1, a p-sylow subgroup, $|P| = p^\alpha$. By Lagrange's Thm any non-trivial elt. $b \in P$ has order p^β, $\beta \leq \alpha$. $p^\beta = ps$, for some $s \in \mathbb{N}$. By $\not\alpha$, G has an elt of order and we get a p-subgrp P of order p^α. QED.

these ideas are important for test.

Recall P is a Sylow-p subgroup if $|P| = p^\alpha$.

How did we show that $\exists$ a subgroup of order p^α?

Induction → Cases ⇄ $p \mid |Z(G)|$; $p \nmid |Z(G)|$.

- Let n_p = # of sylow-p's,

  $n_p \equiv 1 \bmod p$ & $n_p \mid m$ where $|G| = p^\alpha m$ & $(p, m) = 1$

- Let's play with this

  Let $|G| = p^\alpha m$ $(m, p) = 1$

- **Lemma:** $Q \leq G$, $|Q| = p^\beta$, $\alpha \geq \beta > 0$. Let P be a p-sylow of G. Then $N_G(P) \cap Q = Q \cap P$.

  [Comment: we know $P \leq N_G(P)$ so lemma says, $N_G(P) \cap Q$ is as small as possible].

  - **Proof:** Suppose not, so $\exists$ $s \in (N_p(G) - P) \cap Q$. Consider $P\langle s \rangle$, so $|P\langle s \rangle| = \frac{|P||\langle s \rangle|}{|P \cap \langle s \rangle|} > p^\alpha$ but also $\langle s \rangle \leq N_p(G)$ $\Rightarrow P\langle s \rangle \leq G$.

    So $|P\langle s \rangle| = p^{\alpha + j}$ where $j > 0$, But $P\langle s \rangle \leq G$, which contradicts Lagrange's Thm. QED

- Continuing on...

Let P_1 be a p-sylow subgroup (we know this exists).

Consider $\{g P_1 g^{-1} : g \in G\} = A$. G acts on A by conjugation.

— Any subgroup of G acts on A by conjugation.

Let P_1 act on A, what is the orbit of P_1 under this action? It's just P_1! Duh!

— Suppose $g P_1 g^{-1} \neq P_1$. The orbit has size $[P_1 : N_{P_1}(g P_1 g^{-1})]$ by the orbit stabilizer thm. cont.

↱ by Lemma we proved above

Notice $[P_1 : N_P(gP_1g^{-1})] = [P_1 : P_1 \cap gP_1g^{-1}]$, since $gP_1g^{-1} \neq P_1$,
$P_1 \cap gP_1g^{-1} \subsetneq P_1$.

↳ proper subset so $P_1 \cap gP_1g^{-1}$ has fewer than p^α elements.

Therefore $[P_1 : N_G(gP_1g^{-1})]$
$= [P_1 : P_1 \cap gP_1g^{-1}]$ is a multiple of p.

So $|A| \equiv 1 \bmod p$.

• Lemma: If Q is a p-subgroup of G, $\exists$ a sylow-p-subgroup containing Q.

Proof:

Let Q act on $A = \{gP_1g^{-1} : g \in G\}$ by conjugation. Suppose there's no sylow-p in which Q is contained. We look at the orbits under this action, their sizes...

$[Q : Q \cap gP_1g^{-1}]$ ← size of the orbit of gP_1g^{-1} under the action of Q.

But $Q \cap gP_1g^{-1}$ is proper in Q b/c $Q \not\subseteq Q \cap gP_1g^{-1}$, so it's a multiple of p. This holds for each orbit, contradicting that $|A| = 1 \bmod p$.

If we let P be any sylow-p, then we know P must be equal to some subgroup in A.

Since $|P| = p^\alpha = |gP_1g^{-1}|$ where $g \in G$. So $P \in A$, so A is the set of all sylow-P subgroups. Therefore $n_p \equiv 1 \bmod p$.

But also each pair of sylow-p's is conjugate.

Lastly, apparently # of conjugates of any sylow-p is $[G : N_G(P)]$.

Note $|N_G(P)| \geq p^\alpha$. So $n_p \mid M$ by Lagrange's Thm.

Q.E.D.

• Order of G (a group): $1, 2, 3, 4, 5, 6, 7, 8, 9, 10, 11, 12, \ldots$
trivial Z_2 Z_3 Z_4, $Z_2 \times Z_2$

look at $|G| = 6$. Abelian: Z_6

Not abelian: $n_3 = 1$ so there's a normal 3-sylow

$n_2 = 1$ or 3 → so $n_2 = 3$

If 1, then G abelian, nope

$|G| = p^n m$, $(p, m) = 1$, then $\exists$ subgroup of order p^α w/ n_p, the # of Sylow subgroups, $n_p \equiv 1 \bmod p$, $n_p | m$, & the p-Sylow subgroups are pairwise conjugate.

Review from last time:

5. Suppose G is six-element non-Abelian group. What can we say? Let's have a nice application of the Sylow-theorem:

$6 = 2 \cdot 3$ ... By Sylow-theorem, $\exists$ a subgroup Q of order 3 ... There are n_3 such subgroups, $n_3 \equiv 1 \bmod 3$, $n_3 | \frac{6}{3} = 2$, so $\boxed{n_3 = 1}$ so $Q \trianglelefteq G$

What about n_2? If $n_2 = 1$, then G would be Abelian since $n_2 = 1 \Rightarrow \exists$ a normal subgroup P of order 2 (i.e. the sylow 2 subgroup), & $P \cap Q = \{e\}$ by Lagrange's Thm. By a homework exercise, $G \cong P \times Q$, a product of Abelian groups, making G Abelian which is not the case, so $\boxed{n_2 > 1}$. But $|PQ| = \frac{|P||Q|}{|P \cap Q|} = 2 \cdot 3 = 6$ so $PQ = G$.

Also note $P = \langle a \rangle$ for some $a \in P$, $|a| = 2$ & $Q = \langle b \rangle$, some $b \in Q$ $|b| = 3$.

So $G = \langle a, b \rangle$.

Since $P \trianglelefteq G$, $aba^{-1} \neq b$ b/c G is not Abelian.

So what is aba^{-1}? well, $aba^{-1} = b^2 = b^{-1}$

So G satisfies the same relations as D_6 & $|G| = 6$, so $G = \langle a, b \mid a^2 = e = b^3, aba^{-1} = b^{-1} \rangle$! Yeesh

So $G \cong D_6 = S_3$.

Small Groups:

1 → Z_1 → trivial	let Q be normal Sylow-3 group. $Q = \langle b \rangle$, P be a sylow-2 $P = \langle a \rangle$, $G = \langle a, b \rangle$ b/c $G = PQ$	12 → $2^2 \cdot 3$ $A_4 \cong G$ $n_3 \in \{1, 4\}$ $n_2 \in \{1, 3\}$
2 → Z_2		13 → Z_{13}
3 → Z_3		14
4 → Abelian: Z_4, $Z_2 \times Z_2$		15
5 → Z_5		16
6 → done Z_6 or S_3		17
7 → Z_7		18
8 → non-trivial center: $Z(G) \trianglelefteq G$		19
9 → 3^2 ... so Abelian, $Z_3 \times Z_3$ or Z_9		20
10 → $n_5 = 1$, if $n_2 = 1$, non-abelian then $n_2 > 1$		21
11 → Z_{11}		22

Yeesh

similar argument to 6 we get D_{10}

2×5

★ p. 128 of book ★

• Simplicity of A_5

Note, A_4 is not simple (has a normal subgroup of size 4). This is necessary to point out.

— For contradiction, assume A_5 has a normal, proper, non-trivial subgroup H.

We show $5 \nmid |H|$. If $5 \mid |H|$, then H contains an elt of order 5 by Cauchy's Thm.

The Sylow-5's of H ... $|A_5| = 5 \cdot 12$

So $|H| = p^{\alpha} m = 5^1 m$ where $(5, m) = 1$. If $\alpha \in H$, $|\alpha| = 5$, $\langle \alpha \rangle$

→ sylow 5 of $G(A_5)$. So all Sylow 5's of A_5 are in H, of which there are $6 = n_5$, so there are 24 elts order 5 in H.

So $|H| = 30$ (b/c $|A_5| = 5 \cdot 12 = 60$) By cauchy, $\exists$ elts of order 3 in there, by normality they're all in H, here's our contradiction. ~~So A_5 is simple.~~

So $|H| \in \{2, 3, 4, 6, 12\}$. We can argue each group of those cardinalities has a normal sylow-p ... Since $H \trianglelefteq A_5$, A_5 must contain a normal subgroup of order 2, 3, or 4.

2: $H = \langle (ab)(cd) \rangle$

3: $H = \langle (abc) \rangle$

4: one step more in thinking...

$(ab)(cd)$ You can check this... maybe...

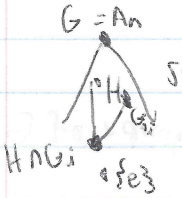
This proof is also in book!

• Let $n \geq 5$. Then A_n is simple

Proof: We'll use induction on n. Base step, $n = 5$, above.

Assume for $n > k \geq 5$, A_k is simple.

Suppose A_n is non-simple, w/ normal (proper, non-trivial) subgroup H.



Let $G_i = \{\alpha \in G \mid \alpha(i) = i\}$

Notice $G_i \cong A_{n-1}$, this is simple by the induction hypothesis.

Note that $H \cap G_i \trianglelefteq G_i$, which is simple.

2 cases to worry about here:

Either $G_i \cap H = \{e\}$ or $G_i \cap H = G_i$

* Comments about Composition Series & solvability.

- Recall $\{e\} \trianglelefteq N_1 \trianglelefteq \dots \trianglelefteq N_{k-1} \trianglelefteq N_k = G$
  - i) $N_i \trianglelefteq N_{i+1}$
  - ii) $\frac{N_{i+1}}{N_i}$ is simple
- Recall, G is solvable if it has a composition series satisfying $\frac{N_{i+1}}{N_i}$ is Abelian, $i = 0, \dots, n-1$.

- Now consider A_5 - is it solvable?

  Well, composition series for A_5

  $\{e\} \trianglelefteq A_5$ & that's it.

  So A_5 is not solvable, and this follows for the rest of the A_n.

  Notice though A_4 is solvable (do this on your own.

- We can also notice $\forall\ n \geq 5$, A_n is the only normal, proper, non-trivial subgroup of S_n.

* Recognizing Direct Products

Let G be a group, $A, B \leq G$. If $G = AB$, $A \trianglelefteq G$, $B \trianglelefteq G$, $A \cap B = \{e\}$, then $G \cong A \times B$.

Conversely, If G is a group & it "factors", $G \cong H \times K$ where H, K are neither trivial.

($\Rightarrow$)

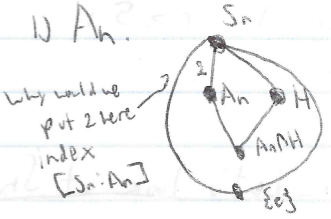
If we can factor, then $\exists\ H', K'$ normal subgroups of G, $\ni$ $G = H'K'$, $H' \cap K' = \{e\}$.

Ex) $S_3 \overset{?}{\cong} H \times K$, H & K are non-trivial. No, b/c S_3 is not Abelian.

• Coming back to the idea of the normal subgroup of S_n.

	Normal Subgroups
S_1	None interesting trivial
S_2	None interesting
S_3	Only A_3 is interesting & 3 2 elt. subgroups
S_4	A_4, also have "V" (Klein group) $= \{e, (12)(34), (13)(14), (14)(23)\}$
$S_n, n \geq 5$	A_n is normal.

Looks like if $n \geq 5$, the only nontrivial, proper, normal subgroup of S_n is A_n.

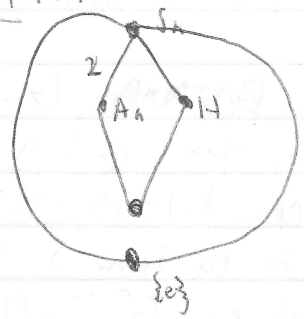


You can label the lattice of subgroups of a group G -- it's "edges" w/ the index of the smaller subgroup within the larger. Eg. label the edge A_n—S_n w/ the index it $[S_n : A_n] = 2$.

— Side note, let $G \geq B \geq A$, when G is a group. Is there a relation between $[G:B]$, $[G:A]$, & $[B:A]$?
Consider left-multiplication by g so $A \to gA$
$bA \to gbA$
so $\lambda_g : G \to G$ & we can see that λ_g is a bijection.
So how many left cosets of A are there in G, relative to the # of left cosets of B in G.

$$[G:A] = [G:B][B:A] \quad \text{QED}$$

— Returning to S_n, A_n & H...
Suppose $H \trianglelefteq S_n$, then



If H were not contained in A_n, then $\langle A_n, H \rangle$ i.e. the least subgroup containing $A_n \cup H$

since $S_n \trianglerighteq H$... then
$A_n \trianglelefteq A_n \cap H$. Since $n \geq 5$, A_n is simple, thus it's only normal subgroups are the uninteresting ones, thus $A_n \cap H$ is trivial or $A_n \cap H = A_n$. ① $A_n \cap H = A_n$ ② $A_n \cap H = \{e\}$
① $A_n \leq H$ in which case $H \in \{S_n, A_n\}$.
② So $H - \{e\}$ consists of odd elts of S_n. cont. on next page.

(2) If $H \cap A_n = \{e\}$, so $H - \{e\}$ consists of odd elts of S_n.
Let $b, c \in H - \{e\}$. Now $bc \in A_n$, so $bc = e$.
so $b = c^{-1}$ From here, you show $H = \{e\}$
Thus The only normal subgroup of S_n $n \geq 5$ is A_n.

- Composition Series for S_n, $n \geq 5$.
So $\{e\} \trianglelefteq N_1 \trianglelefteq N_2 \trianglelefteq \dots \trianglelefteq N_k = G$
N_{i+1}/N_i is simple.
Determine all composition series for S_n $n \geq 5$:
$\{e\} \trianglelefteq A_n \trianglelefteq S_n$

- Solvable if all factors are Abelian. Let's look at S_n
Is S_n solvable? (when $n \geq 5$)
~~So if $\frac{S_n}{A_n}$ abelian?~~
Factors: $\{ \frac{S_n}{A_n}, A_n \}$
$\frac{S_n}{A_n} \cong Z_2$ ↑ not Abelian
↑ so yes
So S_n isn't solvable

- Factoring Groups
Def: G is a group. G is directly factorizable if $\exists$ non-trivial groups $A, B \ni G \cong A \times B$.

- we showed if ~~[illegible]~~ $G = AB$, & $G \trianglerighteq A$, $G \trianglerighteq B$, & $A \cap B = \{e\}$, then $G \cong A \times B$
Reminder: Suppose $|G| = 15 = 3 \cdot 5$ $n_5 = 1$ & $n_3 = 1$
Let P be the Sylow 5 & Q be the Sylow 3.
Using the above, $G \cong P \times Q \cong Z_3 \times Z_5 \cong Z_{15}$
Conversely, if $G \cong A \times B$, then $\exists$ normal subgroups A', B' of G $\ni$ $A'B' = G$, $A' \cap B' = \{e\}$, $A \cong A'$, $B \cong B'$.
Indeed, use $B' = \{(e, b) : b \in B\}$ & $A' = \{(a, e) : a \in A\}$
— G is directly indecomposable if it has no direct factorization.
cont.

- If $S_3 \cong A \times B$, & neither A nor B was trivial $\Rightarrow \{|A|,|B|\} = \{2,3\}$.
But then A & B up to isomorphism would be as Z_2, Z_3, but these are abelian & S_n is not, so we have a contradiction.

Well, Looking at S_3 —

$A = A_3$, $\langle (12) \rangle = B$

We know $S_3 = AB$, $A \cap B = \{e\}$

Suppose $a_1, a_2 \in A = A_3$, $b_1, b_2 \in \langle (12) \rangle$ ... & $a_1 b_1 = a_2 b_2$.

So $a_2^{-1} a_1 = b_2 b_1^{-1}$

$\in A \quad \in B \quad = \{e\}$ so $a_1 = a_2$, $b_1 = b_2$.

$\exists$ a function $\phi : S_3 \to A \times B$ (bijection, well-defined)

If $g \in S_3$, $g = ab$ where $a \in A$, $b \in B$ uniquely.

Let $\phi(g) = (a, b)$

Let $g_1, g_2 \in S_3$ where $g_1 = a_1 b_1$, $g_2 = a_2 b_2$ } unique factorizations.

So what is $\phi(g_1 g_2)$?

$= \phi(a_1 b_1 a_2 b_2) = \phi(\underbrace{a_1 b_1 a_2 b_1^{-1}}_{\in A} \underbrace{b_1 b_2}_{\in B}) = (a_1 b_1 a_2 b_1^{-1}, b_1 b_2)$

b/c $A = A_3$ is normal

$= (a_1 a_2^{b_1}, b_1 b_2)$

- This is a <u>semidirect product</u>

Any time $G = AB$, $A \trianglelefteq G$, $B \leq G$, $A \cap B = \{e\}$,

we could $\phi : G \to A \times B$,

$(a_1, b_1) * (a_2, b_2) = (a_1 a_2^{b_1}, b_1 b_2)$

- <u>Generalizing what we've found (semi-direct products)</u>

Given any two groups A & B $\ni \exists$ a homomorphism $\phi : B \to \mathrm{Aut}\, A$, $b \mapsto x^b$

- $A \times B$ is the underlying set

So $(a_1, b_1) * (a_2, b_2) = (a_1 a_2^{b_1}, b_1 b_2)$ where

$a_2^{b_1} = \phi(b_1)(a_2) = \phi_{b_1}(a_2)$ ← whoa wah

Turns out this is associative w/ an identity, & inverses.

We can make groups from groups.

<u>Note:</u> If $\phi : B \to \mathrm{Aut}\, A$ is trivial, then it's just "direct product multiplication."

• Last time we tried to motivate semidirect products. We saw that S_3 cannot be directly decomposed. Then we looked at S_3 not from a weird point of view...

$S_3 \triangleright A_3 \cong Z_3 = A$, $\langle (12) \rangle = B$, $AB = S_3$, $A \cap B = \{e\}$. This must mean we have a "unique factorization" i.e. $g \in S_3$, $\exists\, a \in A$, $b \in$ $\Rightarrow g = ab$.

We saw we took $g_1, g_2 \in S_3 = G \Rightarrow g_1 = a_1 b_1$, $g_2 = a_2 b_2$,

$g_1 g_2 = a_1 b_1 a_2 b_2$

$= a_1 (b_1 a_2 b_1^{-1})\, b_1 b_2$ ("the unique rep'n of $g_1 g_2$

$= (\text{some } A) \cdot (\text{some } b)$

So we got $f: S_3 \to Z_3 \times Z_2$ a bijection, $f(g) = (a, b)$ whenever $g =$

Define $(a_1, b_1) * (a_2, b_2)$

$= (a_1 a_2^{b_1}, b_1 b_2)$

Then we generalized it, see previous page ★.

• Now let's show our op. is associative!

Let a_1, a_2, a_3 be in A, b_1, b_2, b_3 in B.

$[(a_1, b_1)(a_2, b_2)](a_3, b_3)$

$= (a_1 a_2^{b_1}, b_1 b_2)(a_3, b_3)$

$= (a_1 a_2^{b_1} a_3^{b_1 b_2}, b_1 b_2 b_3)$

$=$

$(a_1, b_1)[(a_2, b_2)(a_3, b_3)]$

$= (a_1, b_1)(a_2 a_3^{b_2}, b_2 b_3) = (a_1 (a_2 a_3^{b_2})^{b_1}, b_1 b_2 b_3)$

$= (a_1 a_2^{b_1} (a_3^{b_2})^{b_1}, b_1 b_2 b_3)$

$= (a_1 a_2^{b_1} a_3^{b_1 b_2}, b_1 b_2 b_3)$

So it's associative.

★ So semidirect products are groups! ★

- Identity? (e_A, e_B)

Since ϕ is a homo., ie

$(e_A, e_B)(a, b) = (e_A a^{e_B}, b) = (a, b)$ ... think about it.

- Inverse? $(a, b)^{-1} = ((a^{-1})^{b^{-1}}, b^{-1})$

$(a, b)((a^{-1})^{b^{-1}}, b^{-1}) = (a((a^{-1})^{b^{-1}})^b, e)$

Lemma: If G is a group, $A \trianglelefteq G$, $B \leq G$, $A \cap B = \{e\}$, & $G = AB$, then $G \cong A \rtimes_\phi B$, where $\phi : B \to \mathrm{Aut}(A)$, where ϕ_b is conjugation by b, all $b \in B$.

Ex) Let A be Abelian group, $B = (\{1, -1\}, \cdot)$. Since A is Abelian, $x \mapsto x^{-1}$ is a homomorphism, & is bijection, so it's an automorph. of A. Let $\phi : B \to \mathrm{Aut}\, A$, $\phi(1)(x) = x$
$\phi(-1)(x) = x^{-1}$

then ϕ is a group homo.

$$(a_1, b_1)(a_2, b_2) = \begin{cases} (a_1 a_2, b_1 b_2) & b_1 = 1 \\ (a_1 a_2^{-1}, b_1 b_2) & \text{otherwise.} \end{cases}$$

If $A = Z_n$, letting $\langle r \rangle = Z_n$ (think of "-1" as s.)
so $\langle s \rangle = B$, easy to show that
$A \rtimes_\phi B$ is generated by $\{r, s\}$ ∋
$r^n = e = s^2$ & $srs^{-1} = r^{-1} \cong D_{2n}$

Goodbye groups!
seeya later!

Rings

easier for a while.

$(R, +, \cdot, 0)$ — set; binary ops

Axioms: ① $(R, +, 0)$ is an Abelian group id. 0 s. "$-a$" is the unique elt. s.t. $a + -a$

② $(xy)z = x(yz)$ $\forall x, y, z \in R$

③ $x(y+z) = xy + xz$

④ $(y+z)x = yx + zx$

Ex $(\mathbb{Z}, +, \cdot, 0)$ $(\mathbb{R}, +, \cdot, 0)$
$(\mathbb{Q}, +, \cdot, 0)$ $(\mathbb{C}, +, \cdot, 0)$
$(\mathbb{Z}_n, +, \cdot, 0)$ ↑ add, & mult. mod n

These rings have an identity elt, $\neq$ ie. $1 \cdot x = x \cdot 1$

These are also known as commutative rings meaning $\forall x, y \in R \quad xy = yx$.

Ex Consider $2\mathbb{Z}$ is a commutative ring w/ no identity elt.

Ex $M_2(\mathbb{R})$ ← 2x2 matrices over $\mathbb{R}$.
this is a ring w/ identity being $I = \begin{pmatrix} 1 & 0 \\ 0 & 1 \end{pmatrix}$, non-commutative

Ex Set f Rings:
Let A be an Abelian group $\ni$ $xy = 0$ $\forall x, y \in A$.

- S is a subring of a ring R if closed under mult. & subtraction.
  Ex $2\mathbb{Z} \overset{\text{subring}}{\leq} \mathbb{Z}$.

- $f: R \to S$ is a homomorphism if compatible w/ the operations:
- ker of homomorphism?

$(a + \ker f)(b + \ker f) \equiv ab + \ker(f)$

$\leq \Rightarrow$ subring in these cases

- Recall: S is a subring of a ring R if it's closed under mult & subtraction.

Lemma: Let R be a ring. $\forall\ b \in R$, $0b = 0 = b0$.

Pf: Let $b \in R$, we have
$0b + 0b \overset{\text{dist.}}{=} (0+0)b = 0b$
$\Rightarrow$ Since $(R, +, 0)$ is an Abelian group, we have $-0b$ & we infer that
$0b = 0$, similar for $b0$. QED.

- Examples & properties

– "Number rings": $\mathbb{Z} \leq \mathbb{Z}[\sqrt{2}] \leq \mathbb{Q}[\sqrt{2}] \leq \mathbb{R} \leq \mathbb{R}[i] \cong \mathbb{C}$

- Note $\mathbb{Z}[\sqrt{2}] = \{a + b\sqrt{2} \mid a, b \in \mathbb{Z}\}$, & $\mathbb{Q}[\sqrt{2}] = \{c + d\sqrt{2} \mid c, d \in \mathbb{Q}\}$ & $\mathbb{Z} \leq \mathbb{Q} \leq \mathbb{Q}[\sqrt{2}]$
  we can check that these are closed under ops & subtraction.
- Also note $\mathbb{C} = \{a + bi \mid a, b \in \mathbb{R} \text{ & } i^2 = -1\}$ duh.
- If we're generous about "numbers", we can add $\mathbb{Z}_n = \mathbb{Z}/n\mathbb{Z}$ as a number ring

– "Function Rings": - Consider $\mathbb{R}[x] = \{a_n x^n + \dots + a_0 \mid a_i \in \mathbb{R}\ \forall i\}$
We can think of this ex. many ways. One way is as a ring of functions!
- Another class of function rings is $C[\mathbb{R}]$ (the continuous functions on $\mathbb{R}$)
- Also $C^\infty[\mathbb{R}]$ (infinite continuous functions on $\mathbb{R}$).

– "Matrix Rings": - Consider $M_2(\mathbb{R})$ (2×2 matrices of real #'s)
this distinguishes itself from the others, it's the first not commutative
$M_2(\mathbb{R}) \geq U_2(\mathbb{R})$
↑ upper triangular.

• Types of rings:

- Commutative Rings: R is commutative if $\forall a,b \in R$, $ab = ba$.
- Ring w/ 1 (ring w/ identity): Consider $2\mathbb{Z}$, it has no multiplicative identity

• Elements:

① Invertible: $b \in R$ is invertible if $\exists\ s \in R \ni sb = 1 = bs$

- Concerning invertibles, they're closed under mult. (not addition)
- by associativity, inverse of an invertible is well defined & unique.

② 0 divisors: Let R be a ring, $b \in R$ is a 0-divisor if $b \neq 0$ & $\exists\ c \in R - \{0\} \ni bc = 0$

Ex) Consider $\mathbb{Z}_6$. 3 is a 0-divisor b/c $3 \cdot 2 = 0$

Ex) Is $x \in \mathbb{R}[x]$ a 0-divisor?

No, infact, there are no 0-divisors in this ring.

——— s invertible $\Rightarrow$ not a 0-divisor.

Proof: Let a be invertible in R & $b \in R$ w/ $ab = 0$. WTS $b = 0$

• R is an integral domain if R is commutative w/ 1 & has no 0-divisors.

Ex) $\mathbb{Z}_6$ is not an int. domain

Ex) $\mathbb{Z}$ is, so is $\mathbb{Z}[x]$ & $\mathbb{Q}[x]$.

• Lemma: If R is an integral domain, $a \neq 0$, Then if $b, c \in R$, if $ab = ac$, Then $b = c$.

Proof: $ab = ac$ means that: ... $a(b-c) = 0$

$\Rightarrow b - c = 0 \Rightarrow b = c$.

• A ring R is a field if it's commutative w/ 1 & every nonzero elt. of R is invertible.

- Not-Every field is an integral domain.

Ex) $\mathbb{Q}$, $\mathbb{R}$, $\mathbb{C}$

Ex) $\mathbb{Z}$ is an int. domain, but not a field.

Ex) $\mathbb{Q}[\sqrt{2}]$ is a field. You can check this.

• Homomorphisms

Defn: $f: R \to S$ is a ring homomorphism if f is compatible w/ addition & mult.
(R, S: rings)

Ex) $f_n: \mathbb{Z} \to \mathbb{Z}/n\mathbb{Z}$ where $b \in \mathbb{Z}$ goes "$b \bmod n$". It's a homo.

Ex) Non-example.
$\det: GL_2(\mathbb{R}) \to \mathbb{R}$ where $\det(A)$ = determinant of A & $A \in M_2(\mathbb{R})$
Not compatible w/ addition.

Ex) $e_0: \mathbb{R}[x] \to \mathbb{R}$ where $e_0(f(x)) = f(0)$
this is indeed a ring homo.
for more information, see illustration of homomorphisms of rings 3 pages ago.

- Lemma: $\ker f \leq R$ where f is a ring homo & R is a ring, & $\forall w \in R$, $w \cdot \ker(f) \subseteq \ker f$
b/c If $k \in \ker f$, $f(kw) = 0$,

- Defn: R is a ring $I \subseteq R$ is an ideal of R if $I \neq \emptyset$, $I \leq R$, & $\forall w \in R$, $wI \subseteq I$ & $Iw \subseteq I$.

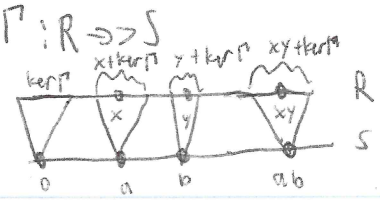
Ex) $\mathbb{Z} \leq \mathbb{R}$. Is $\mathbb{Z}$ an ideal of $\mathbb{R}$?
NO, $\frac{1}{2} \cdot 1 = \frac{1}{2} \notin \mathbb{Z}$.

Ex) $\mathbb{Z}[x] = R$, $\{q(x)(x^2-2) \mid q(x) \in \mathbb{Z}[x]\} = B$. Is B ideal in $\mathbb{Z}$? Yes, it is.

- As observed, $f: R \to S$ homomorphism $\Rightarrow \ker f$ is an Ideal of R.
We'll get a converse
What this converse will give us is this:
If I is an ideal, define $R/I = \{a + I \mid a \in R\}$
so we have an addition, but also $(a+I)(b+I) \subseteq ab + aI + Ib + II$
we define $(a+I)(b+I) := ab + I$ $\subseteq ab + I$
& this is well defined.
It's easy to show "$\cdot$" is associative & it satisfies the dist. props.
& I is the "0";

Converse - Let I be an Ideal in R, Consider R/I, and a function $\pi: R \to R/I$ to obvious given by $r \mapsto r + I$.

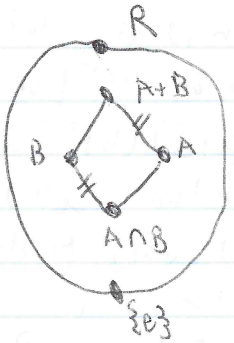
$\Gamma : R \twoheadrightarrow S$



- **1st Isomorphism Thm:** $S \cong \frac{R}{\ker \Gamma}$ under $\Gamma^* : R/\ker\Gamma \to S$, with $\Gamma^*(x+\ker\Gamma) = \Gamma(x)$, well defined. If $p+\ker\Gamma$, $q+\ker\Gamma$ are in $R/\ker\Gamma$,
$\Gamma^*((p+\ker\Gamma)(q+\ker\Gamma)) = \Gamma^*(pq+\ker\Gamma) = \Gamma(pq) = \Gamma(p)\Gamma(q)$
$= \Gamma^*(p+\ker\Gamma)\Gamma^*(q+\ker\Gamma)$. Leaving the additive part to you, ... We know know
If $\Gamma^*(p+\ker\Gamma) = \Gamma^*(q+\ker\Gamma)$ iff $\Gamma(p) = \Gamma(q)$ iff $p+\ker\Gamma = q+\ker\Gamma$
So Γ^* is injective. Now we want to show Γ^* is surjective.
Let $s \in S$. Since Γ is onto (defined above) $\exists\ r \in R$ with $\Gamma(r) = s$
So $\Gamma^*(r+\ker\Gamma) = \Gamma(r) = s$, thus it's surjective. So we have our bijection, QED (sort of)
- **Fact:** If I is an ideal of ring R, then $\exists$ a ring S & a homomorphism $\Gamma : R \twoheadrightarrow S$ s.t. $\ker\Gamma = I$.
Slight Proof: To show this, let $\Gamma : R \to \frac{R}{I}$ where $\Gamma(r) = r+I$ where $r \in R$. We can check Γ is a homomorphism. It's onto.
The zero of $\frac{R}{I}$ is I, so $\Gamma(r) = 0\ (= I) \iff r+I = I \iff r \in I$.
QED

- **Notice:** Ideals... the only ideals of $(\mathbb{Z}, +, \cdot, 0)$ are $k\mathbb{Z}$, $k \in 0 \cup \mathbb{N}$... It's a homework problem.

- **2nd Isomorphism Theorem:** R is a ring. A is an Ideal, B is a subring
1) $A+B$ is a subring of R (we should be able to prove this)
2) $A \cap B$ is ideal of B
3) A is an ideal of $A+B$
4)



$\frac{B}{A \cap B} \cong \frac{A+B}{A}$

- proof of 4) Let $\phi: B \to \frac{A+B}{A}$, so $\phi(b) = b + A$ where $b \in B$. Leaving to us to show it's an onto homomorphism. What is $\ker \phi$?
$\phi(b) = b + A = A$ iff $b \in A$, so $b \in A \cap B$, thus by the 1st Isomorphism Thm, $\frac{B}{A \cap B} \cong \frac{A+B}{A}$ QED.

- Let $\emptyset \neq A \subseteq R$ ring. $(A) :=$ least ideal of R containing A. In fact, $(A) = \cap \{I : A \subseteq I, I \text{ is ideal}\}$. Consider the special case, $A = \{a\}$. in which case $(a) :=$ "principal ideal generated by a". Special case: R is commutative w/ 1, $(a) = \{ra : r \in R\}$. R is commutative w/ 1 & all ideals are principal ideals, then R is called a Principal Ideal Domain (PID)

Ex) $(\mathbb{Z}, +, \cdot, 0)$ is a PID.

Ex) $\mathbb{Z}[x] = \{p(x) = a_n x^n + \dots + a_0 : a_i \in \mathbb{Z}, a_n \neq 0\}$
$(x) = \{p(x) \in \mathbb{Z}[x] : p(0) = 0\}$
$(2) = \{p(x) \in \mathbb{Z}[x] : 2 \mid a_i \ \forall 0 \leq i \leq n\}$
$(2) + (x)$ = add 2 ideals, get an ideal, so
$(2) + (x) = \{p(x) \in \mathbb{Z}[x] : 2 \mid p(0)$ iff $2 \mid a_0\}$ - this is proper in $\mathbb{Z}[x]$
- Is $(2) + (x)$ a PID?
Suppose it is for contradiction, and suppose it's generated by $g(x)$... ie. $(g(x)) = (2) + (x)$. So $\exists\ h(x)$ & $i(x) \ni g(x)h(x) = 2$ & $g(x)i(x) = x$.
But $\iff g(x) \in \{1, -1, 2, -2\}$, but if $g(x) \in \{1, -1\}$, then $(g(x)) = \mathbb{Z}[x]$, but it's supposed to be proper; so $g(x)$ must $\in \{2, -2\}$...
But $2i(x) = x$ or $-2i(x) = x$ which is clearly not possible, thus we have our counterexample. Thus $(2) + (x)$ is not a PID $\Rightarrow \mathbb{Z}[x]$ is not a PID.

- R has a 1, I is an ideal of R. $I = R$ iff $1 \in I$.

• R commutative w/ 1 & {0} & R only ideals iff R is a field.

Proof:

Suppose {0} & R are the only ideals of R. Let $b \in R - \{0\}$ & consid (b) ... it must be R b/c it's in $R - \{0\}$.

$(b) = R \Rightarrow$ that $1 \in (b)$ which is to say $\exists\, c \in R$ w/ $cb = 1$

So every non-0 elt. $b \in R$ has an inverse, so R is a field.

Conversely, R is a field & I is a proper ideal containing $b \in I$.. Since R is a field, $b = 0$, so $I = \{0\}$. QED.

• I is a maximal ideal if I is proper & whenever an ideal J contains I, $J = R$ or $J = I$.

Ex] Max ideals of $\mathbb{Z}$ ring.

$p\mathbb{Z}$ where p is prime is maximal.

Ex] $4\mathbb{Z}$ is not maximal.

$4\mathbb{Z} \subsetneq 2\mathbb{Z} \subsetneq \mathbb{Z}$

- Question: Is (x) maximal in $\mathbb{Z}[x]$?

Nope. $(x) \subsetneq (2)+(x) \subsetneq \mathbb{Z}[x]$

Funny enough (x) is max'l. in $\mathbb{Q}[x]$.

• Lemma: R is a commutative ring w/ 1, I is an ideal, & $\frac{R}{I}$ is a field iff I is a maximal ideal.

Proof:

$\frac{R}{I}$ is a field iff it's ideals are the trivial ideal & $\frac{R}{I}$, so by the 4th isomorphism thm., There are no ideals between R & I, so I is the maximal ideal.

Conversely, if I is maximal, then the ideals by the 4th isomorphism thm, are the trivial & $\frac{R}{I}$, which makes it a field. QED.

Prop: R comm. max'l ideal $\Rightarrow$ prime

• An ideal I is a prime ideal of R (R is comm w/ 1), if $ab \in I$, then $a \in I$ or $b \in I$ & $I \neq R$.

Ex] Prime ideals of $\mathbb{Z}$: (2) prime? $ab \in (2)$ yes! (p) where p is prime are indeed prime ideals

∀ statements made today, (if not specified otherwise)
R is comm. ring w/ 1.

• A bit of review:
- P prime ideal if it's proper & whenever $a, b \in R$ w/ $ab \in P$, then $a \in P$ or $b \in P$
- Ex (6) is an ideal of $\mathbb{Z}$, $2 \cdot 3 \in (6)$, but $2 \notin (6)$ & $3 \notin (6)$
Ex $\mathbb{Z}[x]$, $I = (x)$, it's a prime ideal.
If $s(x), t(x) \in \mathbb{Z}[x]$, $s(x)\,t(x) = u(x)\,x$, some $u(x) \in \mathbb{Z}[x]$
So $s(0)\,t(0) = u(0) \cdot 0 = 0$. since $\mathbb{Z}$ is an int domain $s(0) = 0$ or $t(0) = 0$, that is $s(x) \in (x)$ or $t(x) \in (x)$.

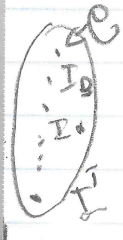
Review left off

- Prop: I is prime iff $\frac{R}{I}$ is int domain.
Proof: - Suppose I is prime
Let $a, b \in R$ & $(a+I)(b+I) = 0_I$ ($= 0$ in this set)
Thus $(a+I)(b+I) = ab + I$ so $ab \in I$, & I prime $\Rightarrow$ $a \in I$ or $b \in I$. It follows that $a+I$ or $b+I$ is I.
- Conversely, suppose $\frac{R}{I}$ is an int. domain, & $a, b \in R$, $ab \in I$, then we have $(a+I)(b+I) = ab + I = 0\ (= I)$ thus b/c R/I is an int. domain, $a+I = I$ or $b+I = I \Rightarrow a \in I$ or $b \in I$, thus by definition I is prime. QED

Ideal Extra Material

• Prop: I is maximal then I is prime
Proof: R commutative w/ 1 & I maximal ideal $\Rightarrow$ R_I is a field, but a field is an int. domain. So I is prime by the above proposition. QED

↓
Converse isn't true (Recall (x) in $\mathbb{Z}[x]$).



• Let R be a ring w/ 1 (not comm.) & I is a proper ideal of R, then $\exists$ a maximal ideal containing I
Informal Proof: Use Zorn's Lemma. Let $\mathcal{A}$ be the proper ideals of R containing I. So $\mathcal{A}$ is a poset ordered by set inclusion. Suppose $\mathcal{C}$ is an increasing chain of ideals in $\mathcal{A}$. Index $\mathcal{C}$ by C & consider $\bigcup_{\beta \in C} I_\beta = \bigcup \{I_\beta : I_\beta \in \mathcal{C}\}$.

cont.

by prop. cont.

- Observe that if $r \in \bigcup_{\alpha \in \mathcal{C}} I_\alpha$ iff $r \in I_\alpha$ where $I_\alpha \in \mathcal{C}$.
So if $r, s \in \mathcal{C}$ $\exists$ β ∋ $r, s \in I_\beta$, an ideal, so rs & $r-s \in$ ...
& if $c \in R$, then $s \in I_\beta$, an ideal, so $sc \in I_\beta \subseteq \bigcup_{\alpha \in \mathcal{C}} I_\alpha$, so the "union" is an ideal.
If $1 \in \bigcup_{\alpha \in \mathcal{C}} I_\alpha$, then $\exists$ β ∋ $1 \in I_\beta$, not possible since I_β is ...

Segue into territory of GC Domains

- Last week, they were in $\mathbb{Z}$. We want to generalize this into Comm. rings w/ 1.

Review — You should know this.

If $a, b \in \mathbb{Z}$, both can't be 0, then $\exists$ $d \in \mathbb{N}$ ∋ $\gcd(a,b) \in (a)$

- To define "gcd" of pairs of elts in R commutative w/ 1, we need the defining "second property" of "gcd" in $\mathbb{Z}$ & we need "$a \mid b$".

- Def: $a, b \in R$, $a \neq 0$ if $\exists$ $c \in R$ ∋ $ac = b$, then "$a \mid b$".

Ex

In $\mathbb{Z}[x]$ ① $x-1 \mid x^2-1$ → true
② $x \mid x^2+1$ → false

- Observe that $a \mid b \Rightarrow b \in (a)$ & by commutativity, $b \in (a) \Rightarrow a$
$a \mid b \Leftrightarrow (b) \subseteq (a)$

Def: d is the gcd of a & b if the least prin. ideal containing a & b (equivalent containing (a) & (b) is (d)).

eg: gcd of x & 2 in $\mathbb{Z}[x]$ is 1

- Euclidean domains

Def: A norm N of a ring R is a function
$N : R \to \{0\} \cup \mathbb{N}$

• A Euclidean domain norm N satisfies for $b \neq 0$ & $a \in R$, $\exists$ $q, r \in R$ s.t. $a = bq + r$ with either $r = 0$ or $N(b) > N(r)$.

- A int. domain w/ a Euclidean domain norm is a Euclidean domain.

ex $\mathbb{R}[x]$ $N(f(x)) = \deg(f(x))$

ex $\mathbb{Z}$ w/ $N(\mathbb{Z}) = |\mathbb{Z}|$

ex F is a field

$N(u) = 0$ $\forall u \in F$

↳ Proof: Given $b \in F - 0$ & $a \in F$, $a = ab^{-1}(b) + 0$, thus we're done.

Prop: Every Euclidean domain is a principle ideal domain. (Fair game for Final) — we'll get here next time.

(after Final)

R com w/ 1

$a, b \in R$, $a \neq 0$, $a \mid b$ means $\exists\ c \in R$ s.t. $ac = b$.

Observe:

$a \mid b \Rightarrow b \subseteq (a) \Rightarrow (b) \subseteq (a)$

• If R is an int. domain, $(a) = (b)$ iff $\exists\ u \in R^*$ (units) $ua = b$

• GCD in R com w/ 1

d is a gcd of a & b if (d) is least principal ideal containing a & b. eg. 1 is gcd of 2 & x in $\mathbb{Z}[x]$!!

↳ better structure: we'd like $d = \gcd(a, b)$ to guarantee that $(d) = (a) + (b)$

- Defn: Euclidean domain:

integral domain having a norm $N: R \to \mathbb{N} \cup \{0\}$ s.t. if $b \in R - \{0\}$, $a \in R$ $\exists$ q, r s.t. $a = bq + r$,

Ex) $(\mathbb{Z}, +, \cdot, 0)$

$N(z) = |z|$. $\mathbb{R}[x]$ $N(q(x)) = \deg(a(x))$

↑ field F

- Suppose a, b as on previous page. R is Eucl.

$a = bq + r$

case 1): $r = 0$

$(a) * (b) = (a)$

case 2) $a = qb + r$

$b = q_1 r + r_1$

$r = q_2 r_1 + r_2$

$r_1 = q_3 r_2 + r_3$

so ... $r_{n-1} = q r_n (+0)$

Well $(a) + (b) = (r) + (b)$: $a = qb + r$

& $(r) + (b) = (r_1) + (r)$: $b = q_1 r + r_1$

we want to $(a) + (b) = (r) + (b) = (r_1) + (r)$

so $= \ldots = (r_{n-1}, r_n) = (r_n)$

so $(a) + (b) = (r_n)$

& r_n is the least principal ideal following containment. So when we have a Euclidean domain we can satisfy that if $d = \gcd(a, b)$, then $(d) = (a) + (b)$.

basis for internet security.

could be on final

- R is a Euclidean Domain $\Rightarrow$ R is a PID

Proof:

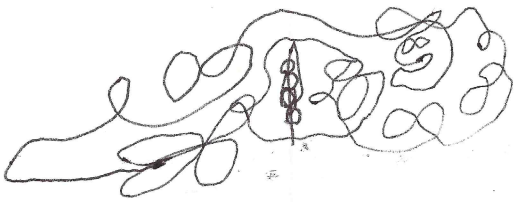
Let I be an ideal. If I is the trivial ideal, $I = \{0\}$, then I is principal $(I = (0))$, if $I = R = (1)$.

So assume I is not trivial & proper. Let $k \in I - \{0\}$. If $N(k) = 0$, then by the Lemma k is a unit, so $I = R$.

We have $\forall\, i \in I - \{0\}$, $N(i) > 0$. By well ordering, $\exists$ a least elt. in $\{N(k) : k \in I - \{0\}\}$. Let $b \in I - \{0\}$ s.t. $N(b)$ is minimal in the above set.

Claim: $(b) = I$,

Let $a \in I$, so $\exists\, q, r \in R$ w/ $a = bq + r$, & $r = 0$ or $N(b) > N(r)$. But $r \in I$, from which $r = 0$ follows b/c $N(b)$ is minimal. $Q.E.D.$



• PID's

We know the definition, see previous stuff.

We showed that in comm. rings w/ 1 that maximal ideals are prime.

perfect problem for final.

- R is a PID & $I=(b)$ is prime, then I is maximal.

Proof:

Suppose $I=(b)$ is prime, & $I \subseteq J$ where J is an ideal. J is principal $\Rightarrow J=(k)$ for some $k \in R$. So $(b) \subseteq (k)$ & (b) is prime.

Since $(b) \subseteq (k) \Rightarrow \exists\ l \in R \ni kl=b$.

Since (b) is prime, either $k \in (b)$ or $l \in (b)$

One of these leads to $I=J$, the other to $R=J$, & that completes the proof. This part needs to be proven by us.

- R is comm. w/ 1, R[x] is a PID $\Rightarrow$ R is a field.

Notice $\Rightarrow$ R[x] is a Euclidean domain.

Proof:

Suppose R[x] is a PID ... so it's an integral domain,

Notice $R \hookrightarrow R[x]$, so R has no zero divisors, so R is an int. domain.

Consider (x). Since R is an int. domain, (x) is a prime ideal.

Claim: Since R is an int. domain, (x) is a prime ideal.

Proof of claim: Indeed if $\exists\ s(x), t(x)^{n(x)} \in R[x]$, $s(x)\,t(x)=x\,u(x)$, then $s(0)\,t(0)=0 \Rightarrow s(0)$ or $t(0)=0$

$\Rightarrow s(x)$ or $t(x)$ is in (x) (is a prime ideal).

We have that $R[x]/(x) \cong R$

But (x) being prime $\Rightarrow$ (x) is maximal,

But by previously proven:

$R \cong \frac{R[x]}{(x)}$ is a field.

QED

we also liked this proof

Review 3rd Isomorphism Thms for groups & rings.