Exam 1 Stats. Total 28 points

	Undergrad	grad
Ave	20	26.8
Med	23	26.5
Dev	7.4	1

Recall: Let S be a set.

[partitions of S] $\longleftrightarrow$ [equiv. relations on S]

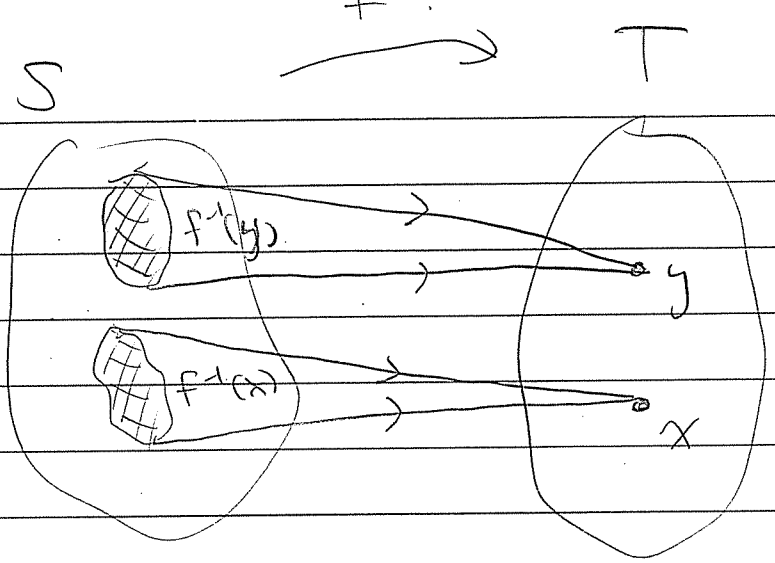
Add one more:
Any map of sets $f: S \to T$ defines an equivalence on the domain S

$$a \sim b \iff f(a) = f(b).$$

The $\sim$-classes are called fibers of f.

$$f^{-1}(t) := \{s \in S : f(s) = t\} \subseteq S.$$

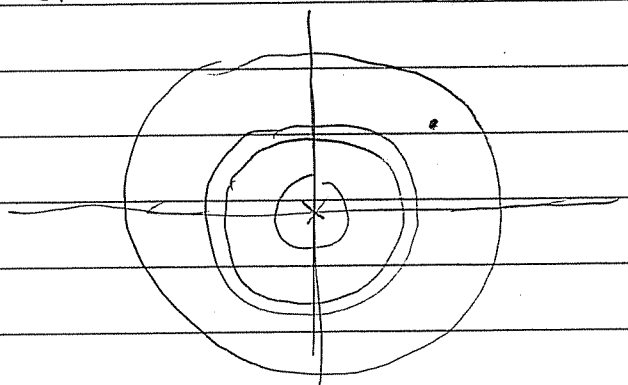
Warning: $f^{-1}(t)$ is a set. $\subseteq S$
If f is invertible then $f^{-1}(t)$ has only one element (called $f^{-1}(t)$).



Pic.

fibers
partition S

eg consider absolute value map $\mathbb{C}^\times \to \mathbb{R}^\times$.
Fibers are circles



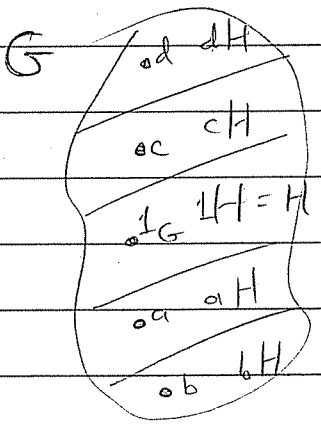
$\mathbb{C}^\times$ partitioned into circles

Recall: Given $H \leq G$ subgroup define

$$a \sim b \iff a^{-1}b \in H$$

$\sim$-classes are called (left) cosets of H.

$$[a] = \{ b \in G : a \sim b \}$$
$$= \{ b \in G : a^{-1}b \in H \}$$
$$= \{ b \in G : a^{-1}b = h \text{ for some } h \in H \}$$
$$= \{ b \in G : b = ah \text{ for } h \in H \}$$
$$= \{ ah : h \in H \}$$
$$= aH$$



Cosets Partition G:

Let G/H = set of (left) H-cosets.

Claim: For all $a \in G$, the map $f(g) = ag$ is a bijection $H \to aH$

Corollary: If $H \leq G$ are finite then

$$|G/H| = |G| / |H|$$

(Lagrange's Theorem 2.8.9)

Next Idea: The set G/H might have more structure....

group?, space?, manifold?, etc.

sub-

eg Consider the group of matrices

$$H = \left\{ \begin{pmatrix} * & * & \cdots & * \\ 0 & & & \\ \vdots & & * & \\ 0 & & & \end{pmatrix} \right\} \leq GL_n(\mathbb{R})$$

$$GL_n(\mathbb{R})/H = \mathbb{RP}^{n-1}$$

real projective space

a lot of structure

Another eg. Modular Arithmetic

Fix $n \in \mathbb{Z}$. Given $a, b \in \mathbb{Z}$ say

$$a \equiv b \bmod n \iff n \mid -a+b$$

EQUIVALENCE RELATION

$$\iff -a+b \in n\mathbb{Z} \quad (a^{-1}b \in H)$$

$$\iff b \in a+n\mathbb{Z} \quad (b \in aH)$$

Temporary Notation: Given $a \in \mathbb{Z}$.

$$\overline{a} := a+n\mathbb{Z} = \{a+nk : k \in \mathbb{Z}\}$$

$$= \{\ldots, a-2n, a-n, a, a+n, a+2n, \ldots\}$$

Hence

$\mathbb{Z}/n\mathbb{Z} = \{\bar{0}, \bar{1}, \bar{2}, \ldots, \overline{n-1}\}$
the set of $n\mathbb{Z}$ - cosets (left? right?)

$[\mathbb{Z} : n\mathbb{Z}] = n$ = # cosets
index of $n\mathbb{Z} \leq \mathbb{Z}$.

Q: What structure does $\mathbb{Z}/n\mathbb{Z}$ have?
Idea: TRY to add & multiply cosets.

$\bar{a} + \bar{b} := \overline{a+b}$? Can we do this?
$(a+n\mathbb{Z}) + (b+n\mathbb{Z}) := (a+b) + n\mathbb{Z}$

$\bar{a}\bar{b} := \overline{ab}$?
$(a+n\mathbb{Z})(b+n\mathbb{Z}) = (ab) + n\mathbb{Z}$

What could go wrong?

eg. Let $n = 12$. So $\bar{7} = \overline{19}$ & $-\bar{2} = \overline{10}$

Then $\bar{7} + -\bar{2} = \overline{7-2} = \overline{5}$
OR $\bar{7} + -\bar{2} = \overline{19} + \overline{10} = \overline{29}$

Q: $\overline{5} = \overline{29}$?
Does choice of coset rep matter?

Lemma 2.9.6. Fix $n \in \mathbb{Z}$.
If $\bar{a} = \bar{a'}$ and $\bar{b} = \bar{b'}$ Then

(1) $\overline{a+b} = \overline{a'+b'}$

(2) $\overline{ab} = \overline{a'b'}$

We say $+, \times$ are Well-Defined.

Proof: Let $\bar{a} = \bar{a'}$ and $\bar{b} = \bar{b'}$ so
$a' = a + rn$ and $b' = b + sn$ for some $r, s \in \mathbb{Z}$.
Then (1) $a' + b' = a + b + (r+s)n$
$\Rightarrow \overline{a'+b'} = \overline{a+b}$ and (2)
$a'b' = (a+rn)(b+sn)$
$= ab + (as + rb + rns)n$
$\Rightarrow \overline{a'b'} = \overline{ab}$ ▨

In Fact: $(\mathbb{Z}/n\mathbb{Z}, +, \times)$ is a ring.

i.e.
- $(\mathbb{Z}/n\mathbb{Z}, +)$ is a (abelian) group
- $(\mathbb{Z}/n\mathbb{Z}, \times)$ is a semigroup (monoid)
  - maybe no inverses.
- $\forall\, a, b \in \mathbb{Z}/n\mathbb{Z}$,
  $a(b+c) = ab + ac$
  a Distributive Rule

eg for $n = 6$. (drop bars)

+	0	1	2	3	4	5
0	(0)	1	2	3	4	5
1	1	2	3	4	5	(0)
2	2	3	4	5	(0)	1
3	3	4	5	(0)	1	2
4	4	5	(0)	1	2	3
5	5	(0)	1	2	3	4

Group! (enough 0's)

		*				*
×	0	1	2	3	4	5
0	0	0	0	0	0	0
* 1	0	(1)	2	3	4	5
2	0	2	4	0	2	4
3	0	3	0	3	0	3
4	0	4	2	0	4	2
* 5	0	5	4	3	2	(1)

NOT a group (not enough 1's)

special rows & columns.

×	1	5
1	1	5
5	5	1

Group! called $(\mathbb{Z}/6\mathbb{Z})^\times$

New HW3. Due date TBA

Def: A ring is a tuple $(R, +, \times, 0, 1)$ such that

- $(R, +, 0)$ is abelian group
- $(R, \times, 1)$ is semigroup (associative with identity 1).
- $\forall a, b, c \in R$ have
  $a(b+c) = ab + ac$
  $(a+b)c = ac + bc$

Notation: Fix $n \in \mathbb{Z}$. Then let

$\bar{a} = a + n\mathbb{Z}$ left/right cosets.

$\mathbb{Z}/n\mathbb{Z} = \{\bar{0}, \bar{1}, \ldots, \overline{n-1}\}$

Can be made into a ring by defining

$$\left.\begin{aligned} \bar{a} + \bar{b} &:= \overline{a+b} \\ \bar{a}\,\bar{b} &:= \overline{ab} \end{aligned}\right\} \forall a, b \in \mathbb{Z}.$$

(Lemma 2.9.6 says this is legal.)

Claim: $(\mathbb{Z}/n\mathbb{Z}, +, \times, \bar{0}, \bar{1})$ is a ring.

Proof: omitted. ///

Notation: Given a ring $(R, +, \times, 0, 1)$ let

$R^\times :=$ set of $\times$-invertible elements
($1 \in R^\times$ since $1 \times 1 = 1$).

Fact: $(R^\times, \times, 1)$ is a group.
The "group of units" of R.

Claim: $(\mathbb{Z}/n\mathbb{Z})^\times = \{\bar{a} : 0 \le a < n, \gcd(a,n) = 1\}$

Proof: Note that

$\bar{a}$ is invertible
$\iff \exists \bar{b}, \ \bar{a}\bar{b} = \overline{ab} = \bar{1}$
$\iff \exists b \in \mathbb{Z}, \ ab \equiv 1 \mod n$
$\iff \exists b, k \in \mathbb{Z} \ \ 1 = ab + nk$
$\iff \gcd(a,n) = 1$
↑ cor 2.3.6

eg $(\mathbb{Z}/10\mathbb{Z})^\times = \{\bar{1}, \bar{3}, \bar{7}, \bar{9}\}$

Table:

$\times$	1	3	7	9
1	(1)	3	7	9
3	3	9	(1)	7
7	7	(1)	9	3
9	9	7	3	(1)

abelian. :)

Is $(\mathbb{Z}/10\mathbb{Z})^\times$ cyclic?

$3 = 3$

$3^2 = 9$

$3^3 = 3 \cdot 9 = 7$

$3^4 = 3 \cdot 7 = \underline{1} = 3^0$

generators

So $(\mathbb{Z}/10\mathbb{Z})^\times = \langle \bar{3} \rangle = \langle \bar{7} \rangle$

$\neq \langle \bar{9} \rangle$

$\neq \langle \bar{1} \rangle$

Is it "easy" to divide in $(\mathbb{Z}/n\mathbb{Z})^\times$?

eg. Compute $\bar{12}^{-1}$ in $(\mathbb{Z}/31\mathbb{Z})^\times$.

Want to solve $12x + 31y = \underline{1}$

Examine (x, y, r) where $12x + 31y = r$.

	x	y	r
(1)	1	0	12
(2)	0	1	31
(3) = (2) − 2(1)	−2	1	7
(4) = (1) − (3)	3	−1	$\bar{5}$
(5) = (3) − (4)	−5	2	2
(6) = (4) − 2(5)	13	−5	$\underline{1}$

$12 \cdot 13 + 31(-5) = \underline{1}$ ✓

Hence $\overline{12}\cdot\overline{13} = \overline{12\cdot 13}$

$= \overline{1 - 31\cdot 5}$

$= \overline{1} - \overline{31\cdot 5}$

$= \overline{1}$ ○

$\overline{12}^{-1} = \overline{13}$ in $(\mathbb{Z}/31\mathbb{Z})^\times$.

Define: $\varphi(n) := |(\mathbb{Z}/n\mathbb{Z})^\times|$.

Euler's φ-function

("totient" function)

$$\varphi(n) = \|\{a \in \mathbb{Z} : 0 \le a < n,\ \gcd(a,n) = 1\}\|$$

Corollary ("Euler's Theorem") Fix $n \in \mathbb{Z}$. Then $\forall a \in \mathbb{Z}$ with $\gcd(a,n) = 1$ we have

$$a^{\varphi(n)} = 1 \bmod n$$

Proof: Consider $\bar{a} \in (\mathbb{Z}/n\mathbb{Z})^\times$ and let $r = |\langle \bar{a} \rangle|$. Lagrange says $|\langle \bar{a} \rangle|$ divides $|(\mathbb{Z}/n\mathbb{Z})^\times|$ hence $\varphi(n) = rk$. Finally.

$$\overline{a^{\varphi(n)}} = \bar{a}^{\varphi(n)} = \bar{a}^{rk} = (\bar{a}^r)^k$$

$$= (\bar{1})^k = \overline{1^k} = \overline{1}$$

∎

Corollary (Fermat's little Theorem)
Given $p \in \mathbb{Z}$ prime and $p \nmid a$ we have

$$a^{p-1} = 1 \bmod p.$$

Proof: $\varphi(p) = p - 1$ 

Q: $\varphi(100) = ?$

Given random $1 \le n \le 100$.
Prob $(2 \mid n) = 1/2$ ⇕ independent events?
Prob $(5 \mid n) = 4/5$.

So (?) $\varphi(100) = 100\left(1 - \frac{1}{2}\right)\left(1 - \frac{1}{5}\right)$
$= 40$ ✓

Guess

$$\varphi(n) = n \prod_{\substack{p \mid n \\ p \text{ prime}}} \left(1 - \frac{1}{p}\right)$$

Can we prove this?

Yes.

Given groups G, H define the direct product group

$$G \times H = \{(g,h) : g \in G, h \in H\}$$

with operation $(g_1,h_1)(g_2,h_2) = (g_1g_2, h_1h_2)$.

Note: $|G \times H| = |G||H|$.

Let $a + n\mathbb{Z} = [a]_n$

Theorem (Chinese Remainder Theorem) Let $n, m \in \mathbb{Z}$ be coprime. Then the map

$$\varphi : \mathbb{Z}/mn\mathbb{Z} \to \mathbb{Z}/m\mathbb{Z} \times \mathbb{Z}/n\mathbb{Z}$$
$$[a]_{mn} \mapsto ([a]_m, [a]_n)$$

is an isomorphism of rings.

$$\mathbb{Z}/mn\mathbb{Z} \approx (\mathbb{Z}/m\mathbb{Z}) \times (\mathbb{Z}/n\mathbb{Z})$$
as rings

Proof: HW 3.7

Corollary: Given $m, n \in \mathbb{Z}$ coprime,

$$(\mathbb{Z}/mn\mathbb{Z})^\times \approx (\mathbb{Z}/m\mathbb{Z})^\times \times (\mathbb{Z}/n\mathbb{Z})^\times$$
as groups

Cor: Given $m, n \in \mathbb{Z}$ coprime, have

$$\varphi(mn) = \varphi(m)\varphi(n).$$

(φ is a "multiplicative function")

Cor: $\forall n \in \mathbb{Z}$,

$$\varphi(n) = n \prod_{\substack{p \mid n \\ p \text{ prime}}} \left(1 - \frac{1}{p}\right)$$

Proof: Factor $n = p_1^{e_1} p_2^{e_2} \cdots p_r^{e_r}$.

Then

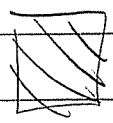
$$\varphi(n) = \varphi(p_1^{e_1})\varphi(p_2^{e_2}) \cdots \varphi(p_r^{e_r}).$$

But $\varphi(p^e) = \left| \{ 1 \le a \le p^e : \gcd(a,p) = 1 \} \right|$

$p \nmid a$

BAD: $\underbrace{p, 2p, 3p, \ldots, p^{e-1}p}_{p^{e-1} \text{ bad elements}} = p^e$.

$$\Rightarrow \varphi(p^e) = \underbrace{p^e}_{\text{all stuff}} - \underbrace{p^{e-1}}_{\text{bad stuff}} = p^e\left(1 - \frac{1}{p}\right).$$



HW 3 due date TBA

START Working

Recall: Given $a, b \in \mathbb{Z}$ coprime.

(i.e. $\gcd(a,b) = 1$

i.e. $a\mathbb{Z} + b\mathbb{Z} = \mathbb{Z}$

i.e. $(a,b) = (1)$)

Choose $n \in \mathbb{Z}$ randomly in range $1, 2, \ldots, N$ (say $N \to \infty$).

Then $\text{Prob}((a,n)=1) = \varphi(a)/a$

$\text{Prob}((b,n)=1) = \varphi(b)/b$

$\text{Prob}((ab,n)=1) = \varphi(ab)/ab$.

Q: $\text{Prob}((a,n)=1 \text{ AND } (b,n)=1) = ?$

A: $\text{Prob}((a,n)=1 \text{ AND } (b,n)=1)$

$= \text{Prob}((ab,n)=1)$ HW 3.4 (MTH 230)

$= \frac{\varphi(ab)}{ab} = \frac{\varphi(a)}{a}\,\frac{\varphi(b)}{b}$

$= \text{Prob}((a,n)=1)\,\text{Prob}((b,n)=1)$

↑ ↑

independent events!

WHY?

Chinese Remainder Theorem: (HW 3.7)

For $a, b \in \mathbb{Z}$ coprime

$$\mathbb{Z}/ab\mathbb{Z} \overset{\text{as rings}}{\approx} \mathbb{Z}/a\mathbb{Z} \times \mathbb{Z}/b\mathbb{Z}$$

Corollary:

$$(\mathbb{Z}/ab\mathbb{Z})^\times \overset{\text{as groups}}{\approx} (\mathbb{Z}/a\mathbb{Z})^\times \times (\mathbb{Z}/b\mathbb{Z})^\times$$

Corollary: $\varphi(ab) = \varphi(a)\varphi(b)$. ☺

Corollary: $\forall n \in \mathbb{Z}$,

$$\varphi(n) = n \prod_{\substack{p \mid n \\ p \text{ prime}}} \left(1 - \frac{1}{p}\right)$$

FUN FACT:

$$\varphi(n) = \sum_{k=1}^{n} \gcd(k, n) \cos\left(\frac{2\pi k}{n}\right)$$

What's left in Chap 2?

Given group hom $\varphi: G \to H$, have $\ker\varphi \leq G$.
Not just any subgroup.

Sp. $a \in \ker\varphi$ i.e. $\varphi(a) = 1_H$.
Then $\forall\, g \in G$ also have $gag^{-1} \in \ker\varphi$ since

$$\begin{aligned}\varphi(gag^{-1}) &= \varphi(g)\varphi(a)\varphi(g^{-1}) \\ &= \varphi(g)\, 1_H\, \varphi(g)^{-1} \\ &= \varphi(g)\varphi(g)^{-1} \\ &= 1_H\end{aligned}$$ ✓

Def: Given $N \leq G$ we say N is normal and write $N \trianglelefteq G$ if

$\forall\, a \in N$, $g \in G$, we have $gag^{-1} \in N$.
"N closed under conjugation by G"

Cor: $\forall$ hom $\varphi: G \to H$, $\ker\varphi \trianglelefteq G$.

Who Cares?
Cosets of $N \trianglelefteq G$ are extra nice.

↓

Prop 2.8.17. Given $H \leq G$, T.F.A.E.

(i) $H \trianglelefteq G$, i.e. $\forall h \in H, g \in G, ghg^{-1} \in H$.
(ii) $\forall g \in G, \quad gHg^{-1} = H$
(iii) $\forall g \in G, \quad gH = Hg$
(iv) Every left H-coset is a right H-coset.

Proof: omitted.

[Note: If G is abelian then every $H \leq G$ is normal. eg $n\mathbb{Z} \trianglelefteq \mathbb{Z}$ $\forall n \in \mathbb{Z}$]

Recall: We gave structure to $\mathbb{Z}/n\mathbb{Z}$ by adding cosets

$$(a+n\mathbb{Z}) + (b+n\mathbb{Z}) := (a+b) + n\mathbb{Z}$$

Well-Defined because given $a+n\mathbb{Z} = a'+n\mathbb{Z}$
$b+n\mathbb{Z} = b'+n\mathbb{Z}$

i.e. $\exists k, l \in \mathbb{Z}$ s.t. $a' = a+nk$, $b' = b+nl$.

Then

$$\begin{aligned} a'+b' &= a+nk+b+nl \\ &= a+b+nk+nl \\ &= a+b+n(k+l) \end{aligned}$$

switch

THE KEY.

$$\Longrightarrow (a'+b')+n\mathbb{Z} = (a+b)+n\mathbb{Z}$$ ☺

Why did this work? ($n\mathbb{Z} \trianglelefteq \mathbb{Z}$)

Let G be any group with $N \trianglelefteq G$.

Define a product on $G/N = \{aN : a \in G\}$ by setting

$$(aN)(bN) := (ab)N$$

Well-Defined?

Suppose $aN = a'N$ and $bN = b'N$

Then $(ab)N = (a'b')N$?

Have $aN = a'N \Rightarrow a^{-1}a' \in N$

$\Rightarrow a' \in aN$

$\Rightarrow \exists\, h \in N,\ a' = ah.$

Similarly, $\exists\, k \in N,\ b' = bk.$

Then $a'b' = ahbk.$ $(= abhk?)$ NO.

[But $h \in N \Rightarrow b^{-1}hb \in N$

$\Rightarrow \exists\, l \in N,\ b^{-1}hb = l \Rightarrow hb = bl$]

So $a'b' = ahbk$

$= ablk. \in (ab)N$

$\Rightarrow (a'b')N = (ab)N$ Well-Defined ✓.

In fact

$$aNbN := \{ ahbk : h, k \in N \}$$
$$= (ab)N$$

Finally,

Definition / Theorem 2.12.2.

Given $N \trianglelefteq G$ the set G/N with well-defined operation $(aN)(bN) = (ab)N$ is a group.

Called a "quotient group".

Proof: closed ✓

identity? $(1N)(aN) = (aN)(1N) = aN$ $\forall aN \in G/N$.

inverses? $\forall\, aN \in G/N$,

$(aN)(a^{-1}N) = (a^{-1}N)(aN) = 1N$

$\Rightarrow (aN)^{-1} = a^{-1}N$

∎

The canonical map

$$\pi : G \to G/N$$
$$a \mapsto aN$$

is a surjective hom.
with $\ker \varphi = N$ because

$$\ker \varphi = \{ a \in G : aN = N \}$$
$$= \{ a \in G : a \in N \}$$
$$= N.$$

Corollary: $H \leq G$ is normal iff

$\exists$ hom $\varphi : G \to G'$ with $\ker \varphi = H$

Proof: If $H = \ker \varphi$ then $H \trianglelefteq G$. ✓
If $H \trianglelefteq G$, consider quotient group G/H
and canonical map $\pi : G \to G/H$
Then $H = \ker \pi$ ▨

First Isomorphism Theorem.
Given hom $\varphi : G \to G'$ we have

$$G/\ker \varphi \overset{\sim}{\to} \operatorname{im} \varphi \leq G'$$

as groups

Proof: Given hom $\varphi: G \to G'$

we need a map $\overline{\varphi}: G/\ker\varphi \to \operatorname{im}\varphi$.

The most obvious choice is

$$\overline{\varphi}(a\ker\varphi) := \varphi(a)$$

Check: hom?

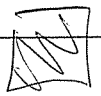
$$\begin{aligned}\overline{\varphi}((a\ker\varphi)(b\ker\varphi)) &= \overline{\varphi}((ab)\ker\varphi)\\ &= \varphi(ab)\\ &= \varphi(a)\varphi(b)\\ &= \overline{\varphi}(a\ker\varphi)\,\overline{\varphi}(b\ker\varphi)\end{aligned}$$ ✓

injective? Suppose $\overline{\varphi}(a\ker\varphi) = \overline{\varphi}(b\ker\varphi)$

i.e. $\varphi(a) = \varphi(b)$. Then $\varphi(a^{-1}b) = 1$

Hence $a^{-1}b \in \ker\varphi \Longrightarrow a\ker\varphi = b\ker\varphi$ ✓

surjective? Easy because $\operatorname{im}\overline{\varphi} = \operatorname{im}\varphi$.



HW 3 due Wed Oct 26.

I will add a few more problems on Wed Oct 19.

Typo:

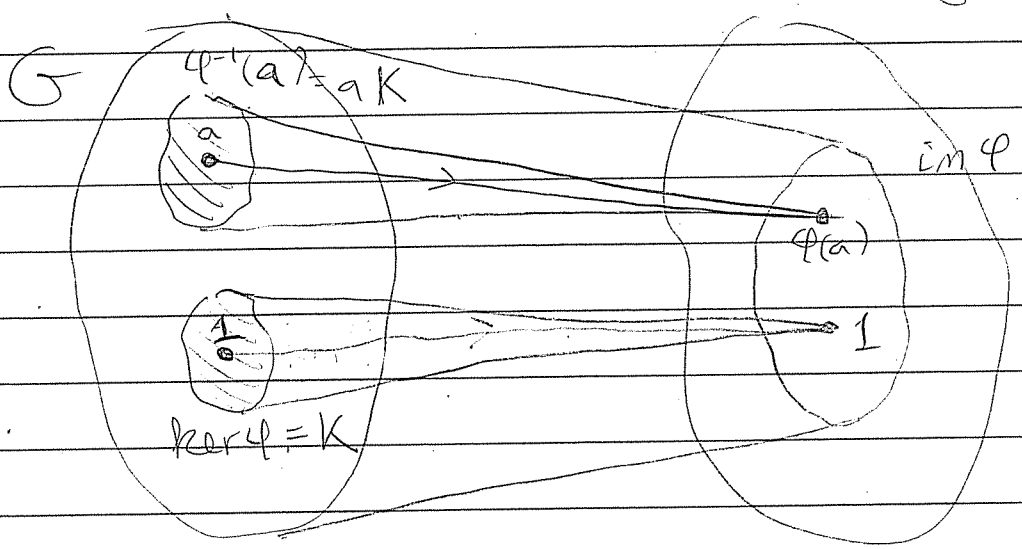
Problem 4. Given $H, K \leq G$.

(a) If $H \trianglelefteq G$ then $HK \leq G$.

(b) Moreover if $H \cap K = \{1\}$ AND we have $hk = kh$. $\forall h \in H, k \in K$, then $HK \cong H \times K$.
$(h,k) \mapsto hk$.

Where are we ??

Given a group hom $\varphi : G \to G'$, what can we say?



$\ker\varphi \trianglelefteq G$

$K \trianglelefteq G$.

Claim: $\varphi^{-1}(a) = aK = Ka$.

↑ by normality.

Proof of $\varphi^{-1}(a) = aK$.

Let $b \in \varphi^{-1}(a)$ i.e. $\varphi(b) = \varphi(a)$

Then $\varphi(a^{-1}b) = 1 \implies a^{-1}b \in K$

$\implies b \in aK$.

Conversely, let $ak \in aK$ (i.e. $k \in K$).

Then $\varphi(ak) = \varphi(a)\varphi(k) = \varphi(a)1 = \varphi(a)$

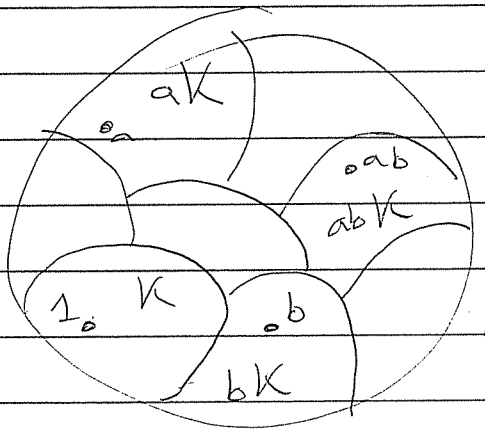
$\implies ak \in \varphi^{-1}(a)$. ∎

Summary (Prop 2.5.8).

Given hom $\varphi: G \to G'$ let $K = \ker\varphi$. T.F.A.E.

- $\varphi(a) = \varphi(b)$
- $a^{-1}b \in K$
- $b \in aK$.
- $bK = aK$. ///.

Fibers of hom $\varphi: G \to G'$ partition G into cosets of $K = \ker\varphi$.



Since $K \trianglelefteq G$, cosets can be multiplied

$(aK)(bK) = (ab)K$

to form a group G/K.

First Isomorphism Theorem.
Every hom $\varphi: G \to G'$ contains an isomorphism.

First make it surjective

$\varphi: G \to \operatorname{im}\varphi$ (easy).

Now make it injective.
How? Why is it not injective? $\ker\varphi \neq \{1\}$.
So get rid of the kernel!

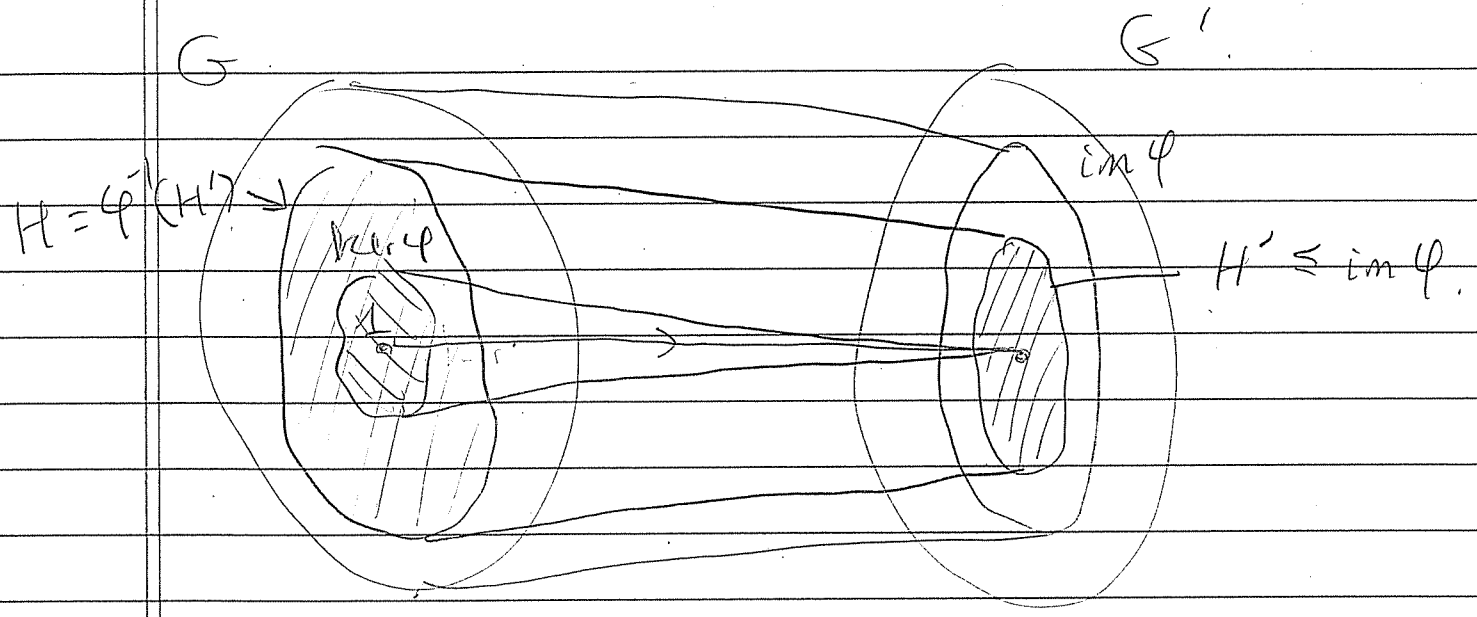
$$\bar{\varphi}: \bar{G} = G/\ker\varphi \longrightarrow \operatorname{im}\varphi$$
$$\bar{\varphi}(a\ker\varphi) := \varphi(a).$$

Get an isomorphism $\bar{\varphi}: G/\ker\varphi \to \operatorname{im}\varphi$.

One more observation:
Given surjective hom $\varphi: G \to \operatorname{im}\varphi$,
let $H' \leq \operatorname{im}\varphi$. Define

$$H = \varphi^{-1}(H') = \{a \in G : \varphi(a) \in H'\}.$$

preimage of H'.



Then: • $H \leq G$

Proof: $a, b \in H$ have $\varphi(a), \varphi(b) \in H' \Rightarrow \varphi(ab)$
$= \varphi(a)\varphi(b) \in H' \Rightarrow ab \in H$.

$\varphi(1) = 1 \in H' \Rightarrow 1 \in H$.

$a \in H \Rightarrow \varphi(a) \in H' \Rightarrow \varphi(a)^{-1} = \varphi(a^{-1}) \in H' \Rightarrow a^{-1} \in H$

□

• $K \trianglelefteq H$

Proof: If $k \in K$ then $\varphi(k) = 1 \in H' \Rightarrow k \in H$.
Given $h \in H \leq G$ have $hKh^{-1} = K$

□

We can restrict the map $\varphi : G \to \operatorname{im}\varphi$
to $\varphi|_H : H \to \operatorname{im}\varphi|_H = H'$.
Then we have

$$H/K \cong H'$$

$$hK \longmapsto \varphi(h) \in H'$$

Finally, DEFINE a Lattice $(L, \leq, \wedge, \vee, 0, 1)$.

$(L, \leq)$ partially-ordered set.

$\forall\, x, y \in L$, $x \wedge y$ = greatest lower bound

$x \vee y$ = least upper bound.

$0 \leq x \quad \forall\, x \in L$

$x \leq 1 \quad \forall\, x \in L$. ///

eg Given a set U, let $\wp(U) = \{A \subseteq U\}$.

Then $(\wp(U), \subseteq, \cap, \cup, \emptyset, U)$
is a lattice.

eg Given $n \in \mathbb{Z}$, $n \geq 1$, Let $D(n) = \{1 \leq d \leq n : d \mid n\}$
Then

$$(D(n), \mid, \gcd, \operatorname{lcm}, 1, n)$$

is a lattice.

eg Given group G let $L(G) = \{H \leq G\}$.

Given $H, K \in L(G)$, $H \cap K \in L(G)$

$H \cup K \notin L(G)$.

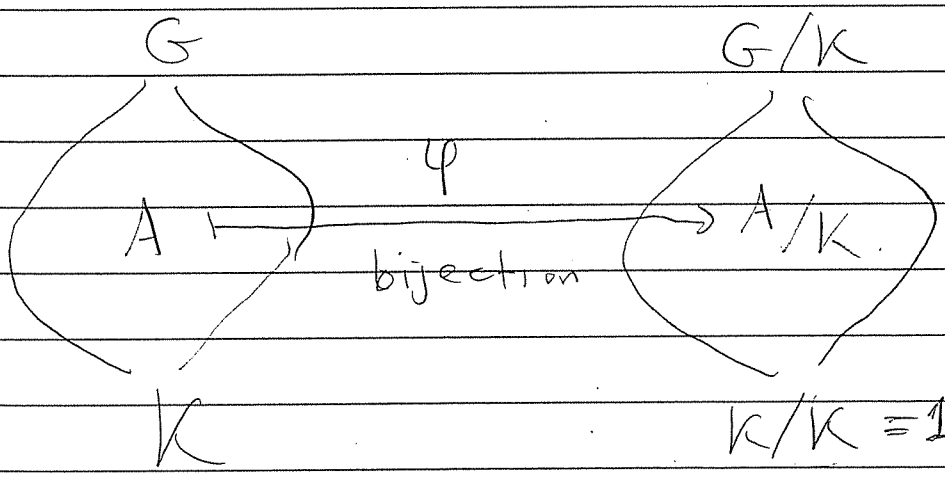
So we define $\langle H, K \rangle = \bigcap_{\substack{G' \leq G \\ G' \supseteq H \cup K}} G'$.

$(L(G), \leq, \cap, \langle \cdot, \cdot \rangle, \{1\}, G)$
is a lattice (the lattice of subgroups).

Big Summary:

(Correspondence Theorem / 4th Isomorphism Theorem / Lattice Isomorphism Theorem)

Given surjective hom $\varphi : G \to \text{im}\varphi$,
let $K = \ker\varphi$ so $\text{im}\varphi \cong G/K$.
Then for any $K \trianglelefteq A \leq G$ define $\varphi(A) \cong A/K$.
Theorem φ is an isomorphism of lattices



i.e (1) $A \leq B \iff \varphi(A) \leq \varphi(B)$

(2) if $A \leq B$ then $[B:A] = [\varphi(B):\varphi(A)]$

(3) $\varphi(\langle A, B\rangle) = \langle \varphi(A), \varphi(B)\rangle$

(4) $\varphi(A \cap B) = \varphi(A) \cap \varphi(B)$

(5) $A \trianglelefteq G \iff \varphi(A) \trianglelefteq \varphi(G) = G/K$.

etc...

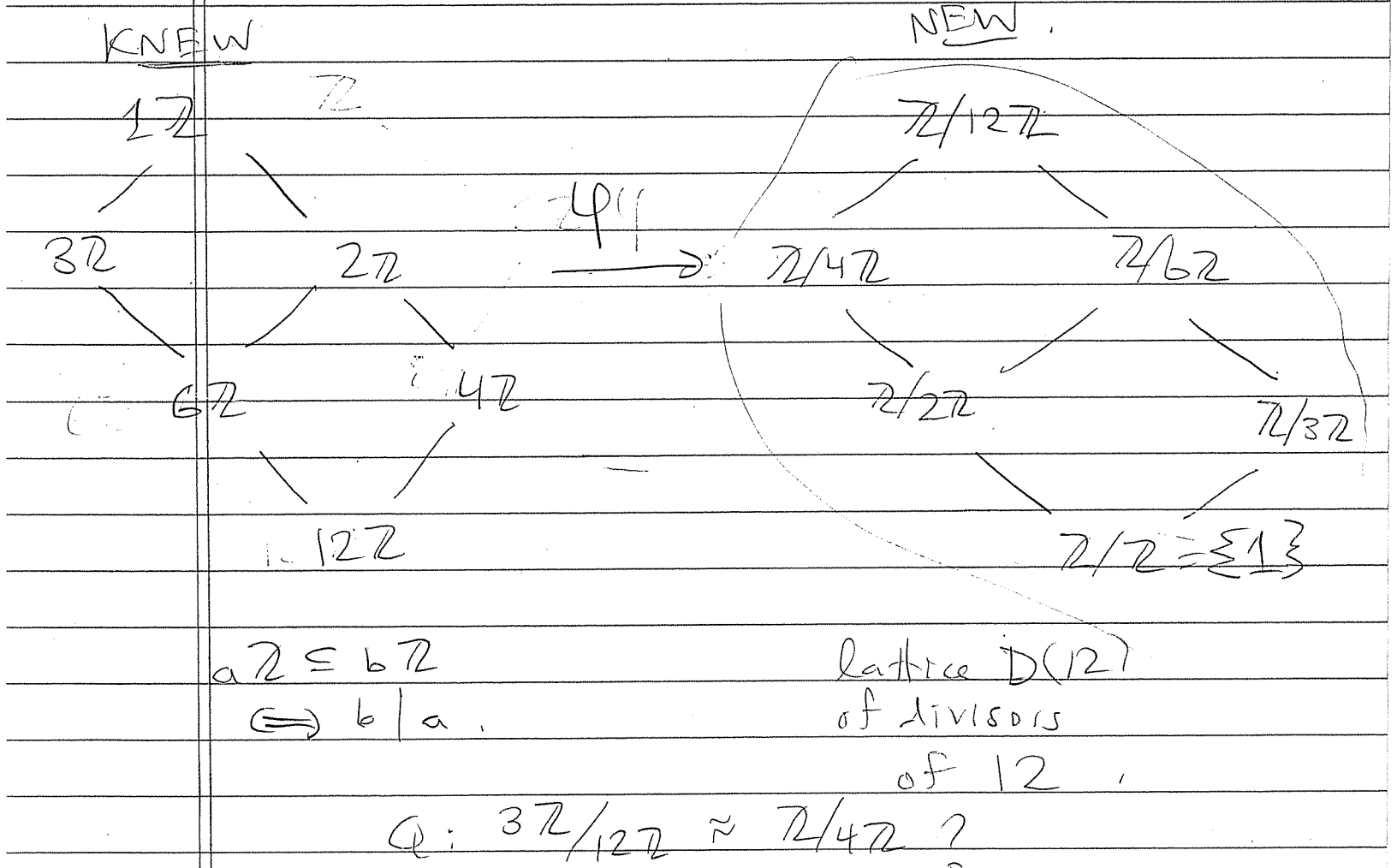
Corollary: Given $n \in \mathbb{Z}$, $n \neq 0$.
Fundamental Theorem of Finite Cyclic Groups

$$L(\mathbb{Z}/n\mathbb{Z}) \approx D(n)$$

as Lattices.

Proof: Consider hom $\varphi : \mathbb{Z} \to \mathbb{Z}/n\mathbb{Z}$
$a \mapsto a + n\mathbb{Z}$
$\ker \varphi = n\mathbb{Z}$.

eg $n = 12$.



$a\mathbb{Z} \subseteq b\mathbb{Z}$
$\iff b \mid a$.

lattice $D(12)$
of divisors
of 12.

Q: $3\mathbb{Z}/12\mathbb{Z} \approx \mathbb{Z}/4\mathbb{Z}$?

Where next?

Bit of vector spaces

Bit of Geometry.

Symmetry = groups acting on things

Icosahedron

For Reference:

2nd Iso. Thm: $H, N \leq G$, $N \trianglelefteq G$

$$\frac{H}{H \cap N} \cong \frac{HN}{N}.$$

3rd. Iso Thm.: $N \trianglelefteq H \trianglelefteq G$.

$$\frac{G/N}{H/N} \cong \frac{G}{H}$$