MATH 113 MIDTERM EXAM 4.10PM-6PM
PROFESSOR PAULIN

DO NOT TURN OVER UNTIL INSTRUCTED TO DO SO.
CALCULATORS ARE NOT PERMITTED
REMEMBER THIS EXAM IS GRADED BY A HUMAN BEING. WRITE YOUR SOLUTIONS NEATLY AND COHERENTLY, OR THEY RISK NOT RECEIVING FULL CREDIT
THIS EXAM WILL BE ELECTRONICALLY SCANNED. MAKE SURE YOU WRITE ALL SOLUTIONS IN THE SPACES PROVIDED. YOU MAY WRITE SOLUTIONS ON THE BLANK PAGE AT THE BACK BUT BE SURE TO CLEARLY LABEL THEM

Name: ______________________________

This exam consists of 7 questions. Answer the questions in the spaces provided.

1. (25 points) (a) Carefully define what it means for a set G to be a group.
Solution:

A group is a set G equipped with a binary operation

$* \; G \times G \to G$ s.t.
$(g, h) \mapsto gh$

1/ $(gh)k = g(hk) \quad \forall g, h, k \in G$ (associativity)

2/ $\exists e \in G$ s.t. $ge = eg = g \quad \forall g \in G$ (Identity)

3/ Given $g \in G$, $\exists h \in G$ s.t. $gh = hg = e$ (Inverses)

(b) Prove that the identity is unique in a group G.
Solution:

Let $e, e' \in G$ both behave as an identity $\Rightarrow$

$e = ee' = e'$

(c) Let G be a group and $H \subset G$. Define what it means for H to be a subgroup.

Solution:

$H \subset G$ is a subgroup if

1/ $e \in H$

2/ $g \in H \Rightarrow g^{-1} \in H$

3/ $g, h \in H \Rightarrow gh \in H$

(d) Let $H \subset G$ be a subgroup. Prove the following is an equivalence relation:

$$x \sim y \iff x^{-1}y \in H$$

Solution:

1/ $e \in H \Rightarrow x^{-1}x \in H \ \forall x \Rightarrow x \sim y$ (Reflexive)

2/ $x \sim y \Rightarrow x^{-1}y \in H \Rightarrow (x^{-1}y)^{-1} = y^{-1}x \in H$

$\Rightarrow y \sim x$ (symmetric)

3/ $x \sim y, y \sim z \Rightarrow x^{-1}y, y^{-1}z \in H$

$\Rightarrow (x^{-1}y)(y^{-1}z) = x^{-1}(yy^{-1})z = x^{-1}z \in H$

$\Rightarrow x \sim z$ (transitive)

2. (25 points) Let G be a group.

(a) Define what it means for a subgroup $N \subset G$ to be normal.

Solution:

N normal in $G \iff \forall n \in N, g \in G, \; gng^{-1} \in N$

(b) If $N \subset G$ is a normal subgroup, prove that the binary operation

$$\begin{aligned} \phi : G/N \times G/N &\longrightarrow G/N \\ (xN, yN) &\longrightarrow (xy)N \end{aligned}$$

is well-defined, i.e. independent of coset representative choices.

Solution:

Let $x_1, x_2, y_1, y_2 \in G$ s.t. $x_1 N = x_2 N$ and $y_1 N = y_2 N$

$\iff x_1^{-1} x_2, \; y_1^{-1} y_2 \in N$

$(x_1 y_1)^{-1}(x_2 y_2) = y_1^{-1} x_1^{-1} x_2 y_2 = y_1^{-1}(x_1^{-1} x_2) y_1 \, y_1^{-1} y_2$

$x_1^{-1} x_2 \in N \Rightarrow y_1^{-1}(x_1^{-1} x_2) y_1 \in N$ and $y_1^{-1} y_2 \in N$

$\Rightarrow (x_1 y_1)^{-1}(x_2 y_2) \in N \Rightarrow x_1 y_1 N = x_2 y_2 N$.

(c) Prove that G cyclic $\Rightarrow G/N$ cyclic

Solution:

G cyclic $\Rightarrow gp(x) = G$ for some $x \in N \Rightarrow$

$G = \{ x^m \mid m \in \mathbb{Z} \} \Rightarrow G/N = \{ x^m N = (xN)^m \mid m \in \mathbb{Z} \}$

$\Rightarrow gp(xN) = G/N \Rightarrow G/N$ cydic.

3. (25 points) (a) State, without proof, Lagrange's Theorem.

Solution:

Let $H \subset G$ be a subgroup. If $|G| < \infty$ then

$$|H| \,\big|\, |G|$$

(b) Let G be a group and $x, y \in G$ such that $ord(x)$ and $ord(y)$ are coprime. Prove that if $n, m \in \mathbb{Z}$ then

$$x^n = y^m \Rightarrow ord(x)|n \text{ and } ord(y)|m$$

You may use any result from lectures as long as it is clearly stated.

Facts about $ord(x)$ and $ord(y)$:

1. $ord(x) = |gp(x)|$, $ord(y) = |gp(y)|$ and 2. $x^n = e \Leftrightarrow ord(x)|n$, $y^m = e \Leftrightarrow ord(y)|m$

$gp(x) \cap gp(x)$ is a subgroup of both $gp(x)$ and $gp(y)$.
Because their orders are coprime $|gp(x) \cap gp(y)| = 1$

$\Rightarrow gp(x) \cap gp(y) = \{e\}$

$x^n \in gp(x)$, $y^m \in gp(y)$. Hence $x^n = y^m \Rightarrow$
$x^n = y^m = e \Leftrightarrow ord(x)/n$ and $ord(y)|m$.

4. (25 points) Let G be a group and S be a set.

(a) Define the concept of an action of G in S.

Solution:

A group action is a map $\varphi : G \times S \longrightarrow S$ s.t.

$(x, s) \longmapsto x(s)$

1/ $e(s) = s \quad \forall s \in S$

2/ $(xy)(s) = x(y(s)) \quad \forall \quad \in G, s \in S$

(b) Prove that

$$\begin{aligned} \phi : G \times G &\longrightarrow G \\ (g, h) &\longrightarrow ghg^{-1} \end{aligned}$$

gives a group action on G on itself.

Solution:

1/ $e(h) = ehe^{-1} = h \quad \forall h \in G$

2/ $(xy)(h) = (xy)h(xy)^{-1} = x(yhy^{-1})x^{-1}$

$= x(y(h))$

(c) Using this, prove the following: If G is finite then

$$|\{ghg^{-1}|g \in G\}| \text{ divides } |G| \text{ for any } h \in G.$$

You may use any result from the course as long as it is clearly stated.

$\{ghg^{-1} | g \in G\} = orb(h)$ under above action.

Orbit-Stabiliser $\Rightarrow |G| = |Stab(h)| \cdot |orb(h)|$

$\Rightarrow |orb(h)| \,/\, |G| \Rightarrow |\{ghg^{-1} | g \in G\}| \,/\, |G|$

5. (25 points) Show that for $x, y \in Sym_5$, if $ord(x) = ord(y) = 6$, then x and y are conjugate. Is the same true of elements of order 2? You may use any result from the course as long as it is clearly stated.

Solution:

Possible cycle structures in Sym_5:

1, 1, 1, 1, 1 $\leftarrow$ order = 1 (LCM)
1, 1, 1, 2 $\leftarrow$ order = 2
1, 2, 2 $\leftarrow$ order = 2
1, 1, 3 $\leftarrow$ order = 3
1, 4 $\leftarrow$ order = 4
2, 3 $\leftarrow$ order = 6
5 $\leftarrow$ order = 5

Hence $ord(x) = ord(y) \iff x$ and y have the same cycle structure 2, 3.

Fact: x, y have same cycle structure $\iff$ they are conjugate

Hence $ord(x) = ord(y) = 6 \Rightarrow x$ conjugate to y.

$ord(x) = ord(y) = 2 \not\Rightarrow x$ conjugate to y

e.g. (12) and $(12)(34)$.

6. (25 points) Let G and H be groups.

   (a) Define the concept of a homomorphism from G to H.
   Solution:

A homomorphism is a map $\phi : G \to H$ s.t.

$$\phi(xy) = \phi(x)\phi(y) \quad \forall x, y \in G$$

   (b) State, without proof, the first isomorphism theorem for groups.

   Solution:

Let $\phi : G \to H$ be a homomorphism. Then the induced map

$$\phi : G/\ker\phi \to \operatorname{Im}\phi$$
$$x\ker\phi \mapsto \phi(x)$$

is a well-defined isomorphism.

   (c) Give an example of a non-trivial homomorphism from $\mathbb{Z}/3\mathbb{Z}$ to D_6. You do not need to prove it is a homomorphism.
   Solution:

Let $D_6 = \{e, \sigma, \sigma^2, \sigma^3, \sigma^4, \sigma^5, \tau, \tau\sigma, \tau\sigma^2, \tau\sigma^4, \tau\sigma^5\}$

Define $\phi : \mathbb{Z}/3\mathbb{Z} \to D_6$

$$[a] \mapsto \sigma^{2a}$$

7. (25 points) (a) State the structure theorem for finitely generated Abelian groups.

Solution:

Let G be a f.g. Abelian group. Then G is isomorphic to the direct product of cyclic groups. These groups are either infinite $(\cong (\mathbb{Z},+))$ or prime power order $(\cong (\mathbb{Z}/p\mathbb{Z},+))$. Moreover, up to reordering and isomorphism this decomposition is unique

(b) Using this, show that an Abelian group of order 30 must contain an element of order 5.

Solution:

$30 = 5 \times 2 \times 3$

$|G| = 30$ and G Abelian $\Rightarrow G \cong \mathbb{Z}/5\mathbb{Z} \times \mathbb{Z}/2\mathbb{Z} \times \mathbb{Z}/3\mathbb{Z}$

$\text{ord}([1]_5, [0]_2, [0]_3) = 5 \Rightarrow \exists x \in G$

s.t. $\text{ord}(x) = 5$

(c) Prove that, up to isomorphism, there is only one group of size 100, such that every element has order dividing 10.

$|G| = 100 = 5^2 \cdot 2^2$, Abelian $\Rightarrow$

$$G \cong \mathbb{Z}/5^2\mathbb{Z} \times \mathbb{Z}/2^2\mathbb{Z} \quad \Leftarrow \operatorname{ord}([1]_{5^2}, [1]_{2^2}) = 100 \nmid 10$$

$$\text{or } \mathbb{Z}/5\mathbb{Z} \times \mathbb{Z}/5\mathbb{Z} \times \mathbb{Z}/2^2\mathbb{Z} \quad \Leftarrow \operatorname{ord}([0]_5, [0]_5, [1]_{2^2}) = 4 \nmid 10$$

$$\mathbb{Z}/5^2\mathbb{Z} \times \mathbb{Z}/2\mathbb{Z} \times \mathbb{Z}/2\mathbb{Z} \quad \Leftarrow \operatorname{ord}([1]_{5^2}, [0]_2, [0]_2) = 25 \nmid 10$$

$$\mathbb{Z}/5\mathbb{Z} \times \mathbb{Z}/5\mathbb{Z} \times \mathbb{Z}/2\mathbb{Z} \times \mathbb{Z}/2\mathbb{Z}$$

$$10([a]_5, [b]_5, [c]_2, [d]_2) = ([10a]_5, [10b]_5, [10c]_2, [10d]_2) = ([0]_5, [0]_5, [0]_2, [0]_2)$$

$$\Rightarrow \operatorname{ord}([a]_5, [b]_5, [c]_2, [d]_2) \mid 10$$

$\Rightarrow \mathbb{Z}/5\mathbb{Z} \times \mathbb{Z}/5\mathbb{Z} \times \mathbb{Z}/2\mathbb{Z} \times \mathbb{Z}/2\mathbb{Z}$ is the only group (up to isomorphism) which satisfies the desired properties.

END OF EXAM