

Recall you may use a two-sided 8.5" by 11" sheet of notes (or surface with equal area) with what ever you like written or typed on it. Additionally, a non-internet accessing calculator, or Desmos Test Mode can be used.

(note: pg 5 #8 was very challenging - they'd never seen anything like it. I saw in final exam the class collaborated on it.)

Show your work for the following problems to earn full marks.

- 1. [3] Prove or provide a counterexample for the following statement: Let S_{10} be the permutation group on ten elements. For all $\sigma \in S_{10}$, $\sigma^{10} = ()$, where $()$ is the identity permutation.

Counterexample:

False (+.5)

consider $\sigma = (123)(45678) \in S_{10}$

note that the order of σ is $3 \cdot 5 = 15$ so

$\sigma^{10} \neq ()$

def of S_{10} (+1)

permutation + raised to 10 (+1)

logic/reason (+.5)

- 2. [3] Prove or provide a counterexample for the following statement: We can define a ring structure on the set $R = \{a + b\sqrt{5} | a, b \in \mathbb{Z}\}$.

Proof: R has an abelian group structure

(+.5) with $(a+b\sqrt{5}) + (c+d\sqrt{5}) = (a+c) + (b+d)\sqrt{5}$

(+1) Note the unit is $0 + 0\sqrt{5}$, inverses $-(a+b\sqrt{5}) = -a - b\sqrt{5}$

Closed b/c \mathbb{Z} is closed $(a+b\sqrt{5}) + (c+d\sqrt{5}) = (a+c) + (b+d)\sqrt{5}$

(+1) Multiplicative structure distributes nicely

with $(a+b\sqrt{5}) \cdot (c+d\sqrt{5}) = (ac + b^2 \cdot 5) + (ad + bc)\sqrt{5}$

logic/reason (+.5)

- 3. Consider $\theta : D_4 \rightarrow \mathbb{Z}_4$ defined by $\theta(r^k f) = k$.

- (a) [2] If θ is a homomorphism, find $\theta(f)$. Show your computations/justification.

$\theta(f) = \theta(r \circ f) = 0$ (+1)

$\theta(f) = \theta(r f r^2 f r^3) = \theta(r f) + \theta(r^2 f) + \theta(r^3) = 1 + 2 + 1 = 0 \pmod{4}$

recheck (+.5)

- (b) [2] Can θ be extended to define a homomorphism? Justify your answer.

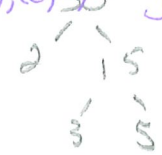
We trace the elements to make sure structure is preserved.

$e \mapsto 0 \quad f \mapsto 0$

scratch & computations (+1)

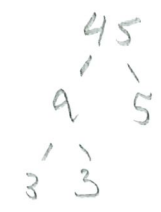
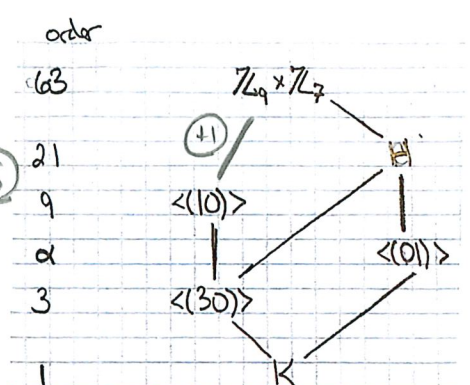
No? (+.5)

$\langle (3,1) \rangle = \{ (3,1), (6,2), (9,3), (12,4), (15,5), (18,6), (21,7), (24,8), (27,9), (30,10), (33,11), (36,12), (39,13), (42,14), (45,15) \}$



4. Consider the partial subgroup lattice for $\mathbb{Z}_9 \times \mathbb{Z}_7$ shown to the right.

recognize $(+1,5) \rightarrow K = \{ (0,0) \}$
 so $\langle (0,0) \rangle$ works $(+1,5)$
 relation $(+1,5)$
 $(1,5) \rightarrow$ b/c of containment of steps
 $(+1) \rightarrow$ can use $\langle (3,0), (0,1) \rangle$



(b) [2] Find a generating set for the subgroup denoted with H .

(c) [1] What number should α be replaced with in the order column?

7 b/c $\langle (0,1) \rangle = \{ (0,1), (0,2), (0,3), (0,4), (0,5), (0,6), (0,0) \}$
 $(+1)$

(d) [1] One edge is missing. Add the missing edge to the subgroup lattice.

(e) [2] Could $\mathbb{Z}_9 \times \mathbb{Z}_7$ form a field with component-wise addition and multiplication reduced by the appropriate modulo? Why or why not?

def of field $(+1)$
 No, the element $(3,0)$ has no multiplicative inverse $(+1,5)$
 The unit is $(1,1)$ but $\nexists \alpha \in \mathbb{Z}_7$ so that $\alpha \cdot 0 = 1 \in \mathbb{Z}_7$

5. Consider a homomorphism $\phi : \mathbb{Z}_{30} \rightarrow \mathbb{Z}_{45}$.

(a) [3] What are the possible sizes for the image of ϕ ? Clearly provide justification and reasoning.

$(+1)$ [Lde by Lagrange $\text{im } \phi \leq \mathbb{Z}_{45} \Rightarrow |\text{im } \phi| | 45 \Rightarrow |\text{im } \phi| \in \{1, 3, 5, 9, 15, 45\}$
 $(+1)$ [By FHT $\text{im } \phi \cong \mathbb{Z}_{30} / \text{ker } \phi \Rightarrow |\text{im } \phi| = [\mathbb{Z}_{30} : \text{ker } \phi]$ by def of index
 $\Rightarrow |\text{im } \phi| = \frac{30}{|\text{ker } \phi|} \Rightarrow (\text{im } \phi) | 30 \Rightarrow |\text{im } \phi| \in \{1, 2, 3, 5, 6, 10, 15, 30\}$

(b) [4] How many different homomorphisms can be defined for ϕ with $\text{ker}(\phi) = \{0, 15\}$.

start $(+1,5)$
 $(+1)$ [By FHT and Lagrange (and (a)) if $|\text{ker } \phi| = 2$ then $|\text{im } \phi| = 30 \div 2 = 15$
 $\Rightarrow \text{im } \phi = \langle \frac{45}{\text{gcd}(15,45)} \rangle = \langle \frac{45}{15} \rangle = \langle 3 \rangle$
 $= \{ 3, 6, 9, 12, 15, 18, 21, 24, 27, 30, 33, 36, 39, 42, 0 \}$

for both true true
 $\{1, 3, 5, 45\}$

$(+1)$ [The homomorphism is completely defined by image of 1 so

6. Let $X = \{1, 2, 3, 4, 5\}$ and let S be the set of all permutations on X .

(a) [5] Let $\alpha = (1, 2, 4)$ and $\beta = (1, 5)$. Find the following:

i. α as a product of transpositions

(41) $\alpha = (124) = (14)(42)$ or $(12)(14)$

(these are several answers for this)

ii. α^{-1}

(41) $\alpha^{-1} = (421)$ or (214) or (142)

note $(124)(142) = (1)(2)(4) = (142)(124)$

iii. $\alpha \circ \beta$

$(124)(15) = (1245)$ (41)

Composition in correct direction (4.5)

iv. Does α and β commute? Justify your answer.

$\beta \circ \alpha = (15)(124) = (1524) \neq \alpha \circ \beta$ so do not commute (4.5)

(b) [4] Define a subset $H = \{\sigma \in S \mid \sigma(3) = 3\}$. That is, all permutations that do not move 3 (or stabilize 3). For example, α from part (a) is in H since 3 is not moved.

Provide a formal proof that H is a subgroup of S .

Proof: We will verify H is a group in its own right. Use $H \subseteq S_S$ so H inherits associativity. We will check for an identity, inverses, and closure.

• Identity: Note that (1) does not move any elements so 3 is fixed by $(1) \Rightarrow (1) \in H$.

• Inverses: Let $\sigma \in H$ then σ keeps 3 in place. Since $\sigma^{-1}\sigma = (1)$ and σ does not move 3 we know σ^{-1} must also leave 3 alone. Thus: $\sigma^{-1} \in H$.

• Closure: Let $\sigma, \tau \in H$ then consider $\sigma\tau$.

Consider $\sigma\tau$ acting on 3.

Note σ does not move 3, and then τ does not either thus $\sigma\tau$ does not move 3.

$\Rightarrow \sigma\tau \in H$

proof complete (44)

7. Use the provided Cayley graph of a group G to answer the following:

(a) [1] How many generators are used in the Cayley graph?

2

(b) [2] Simplify $ts^2tst^2st^3sts^2$ to a form on the Cayley graph.

(+) Follow the arrows

identity and identities/letters

(c) [2] Find the inverse of $ts^2tst^2st^3sts^2$

(+) on the Cayley graph (+) st
 (+) we need a path back from st to 1

(+) tts works

note there are multiple answers?

(d) [2] Find the left cosets of $\langle t \rangle$

$$\langle t \rangle = \{1, t, t^2, s^2, s^2t, s^2t^2, 1\} \quad (+, 5)$$

$$s\langle t \rangle = \{st, st^2, s^3, s^3t, s^3t^2, s^3\} \quad (+)$$

or $\{st, st^2, s^3, t^2s, ts, s\}$

(+5) note b/c $|G| = 12$ and $|\langle t \rangle| = 6$ there are only two cosets
 (+) have all elements

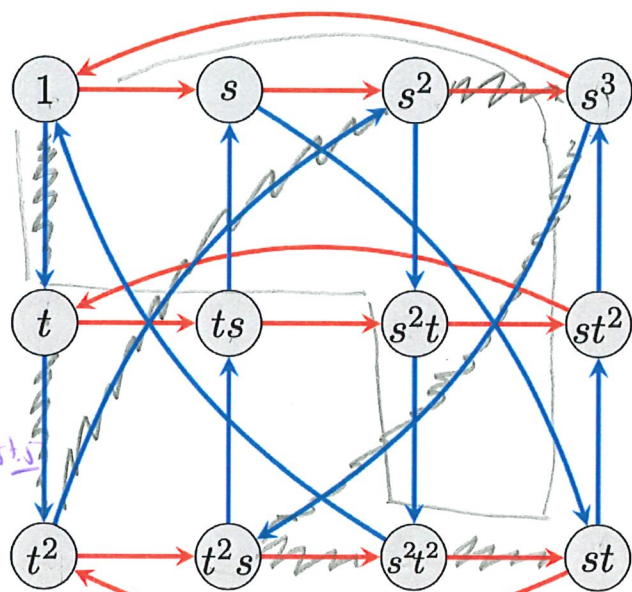
(+5) $\langle t \rangle$ works

Note $[G : \langle t \rangle] = 2$ and we had a well known proof showing if the index is 2 then $\langle t \rangle \trianglelefteq G$.

Also we could just see

$$\langle t \rangle s = \{ts, t^2s, s^3, s^3ts, s^3t^2s, s^3\}$$

$$= \{ts, t^2s, s^3, st^2, st, s\} = s\langle t \rangle \quad \rightarrow \text{checking the}$$



definition of normal (+5)
 used def right (+1)

defined where variables are from (1)

abelian def (1,5)
def of cyclic (1)
in factor group (1)
center / Z(G) (1,5)

8. [8] Recall the center of G is a normal subgroup defined as $Z(G) = \{z \in G \mid zg = gz \forall g \in G\}$. Prove formally that if $G/Z(G)$ is cyclic, then G is abelian.

Pf: Let $a, b \in G$. We will show $a \cdot b = b \cdot a$.

Consider $aZ(G) \in G/Z(G)$ and $bZ(G) \in G/Z(G)$

b/c $G/Z(G)$ is cyclic $\exists x \in G \ni \langle xZ(G) \rangle = G/Z(G)$

That is $\exists n, m \in \mathbb{Z} \ni$

$$aZ(G) = x^n Z(G) \text{ and } bZ(G) = x^m Z(G).$$

That is \exists elements $\bar{\alpha}, \bar{\beta}$ and $\bar{\gamma}, \bar{\delta} \in Z(G) \ni$

$$a\bar{\alpha} = x^n \bar{\alpha} \text{ and } b\bar{\beta} = x^m \bar{\beta}$$

Since G is a group we can left compose with $\bar{\alpha}^{-1}$ and $\bar{\beta}^{-1}$ on the respective equations to get

$$a = x^n \bar{\alpha} \bar{\alpha}^{-1} \text{ and } b = x^m \bar{\beta} \bar{\beta}^{-1}$$

Since $Z(G)$ is a subgroup $\bar{\alpha} \bar{\alpha}^{-1} = \bar{\alpha} \in Z(G)$
and $\bar{\beta} \bar{\beta}^{-1} = \bar{\beta} \in Z(G)$

$$\text{so } a = x^n \bar{\alpha} \text{ and } b = x^m \bar{\beta}. \quad (*)$$

Consider $ab = (x^n \bar{\alpha})(x^m \bar{\beta})$ by (*)
 $= x^n (\bar{\alpha} x^m) \bar{\beta}$ b/c associativity of G
 $= x^n (x^m \bar{\alpha}) \bar{\beta}$ b/c $\bar{\alpha} \in Z(G)$
 $= x^{n+m} \bar{\alpha} \bar{\beta}$ b/c assoc + def of order
 $= x^{m+n} \bar{\alpha} \bar{\beta} = x^m x^n \bar{\alpha} \bar{\beta}$

$\bar{\alpha}, \bar{\beta} \in Z(G)$ & commute

Proof done (14)