Key

Midterm | **TMath 402** | Winter 2016

True/False: If the statement is false, give a counterexample.
If the statement is *always* true, give a brief explanation of why it is (not *just* an example!).

1. [3] (§0) Suppose a, b, $c \in \mathbb{Z}$ such that $a|c$ and $b|c$, then $(ab)|c$.

False (+1)

Let $a=4$, $b=6$, and $c=12$

notice $4|12$ and $6|12$

but $a \cdot b = 24 \nmid 12$.

start (+.5)
divisibility (+.5)
counter ex (+1)

2. [3] (§1) Let a, b, and c be elements of D_4 where D_4 is the group of order 8. If $ab = bc$ then $a = c$.

False (+1)

Let V be a flip over the vertical axis $\left(\begin{bmatrix} 1 & 2 \\ 3 & 4 \end{bmatrix} \xrightarrow{F} \begin{bmatrix} 2 & 1 \\ 4 & 3 \end{bmatrix} \right)$
similarly let H be a flip over the horiz. axis and R_{90} be a rotation by $90°$ counter clockwise

$$\begin{bmatrix} 1 & 2 \\ 3 & 4 \end{bmatrix} \xrightarrow{V} \begin{bmatrix} 2 & 1 \\ 4 & 3 \end{bmatrix} \xrightarrow{R_{90}} \begin{bmatrix} 1 & 3 \\ 2 & 4 \end{bmatrix} = \begin{bmatrix} 1 & 2 \\ 3 & 4 \end{bmatrix} \xrightarrow{R_{90}} \begin{bmatrix} 2 & 4 \\ 1 & 3 \end{bmatrix} \xrightarrow{H} \begin{bmatrix} 1 & 3 \\ 2 & 4 \end{bmatrix}$$

but $H \neq V$

start (+.5)
D_4 group (+.5)
counter ex (+1)

3. [3] (§0) Define a relation R on the set $\{0, a, b, c\}$ so that $0R0$, $0Ra$, aRa, $aR0$, bRb, $bR0$, and cRc. The relation R defines an equivalence relation.

False (+1)

Notice $bR0$ but $0 \not R b$
so R is not symmetric

start (+.5)
def of eq. relation (+.5)
reason (+1)

4. [3] (§4) Let G be a group and $G = \langle x \rangle$ If g, $h \in G$, then there exists $m \in \mathbb{Z}$ such that $x^m g = h$.

True (+1)

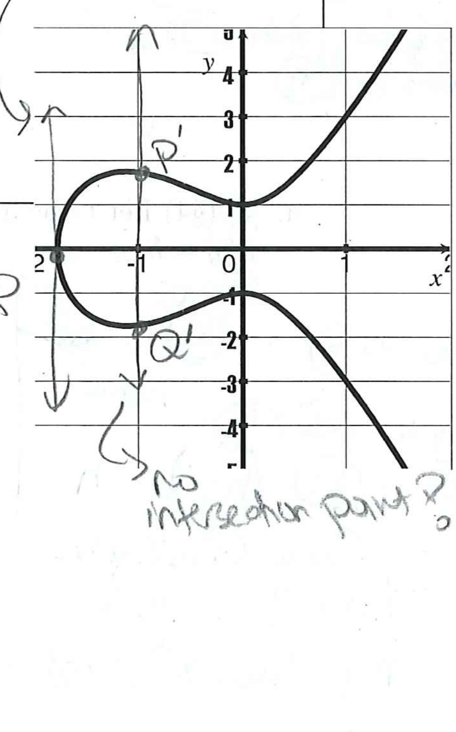
Since $G = \langle x \rangle$ and $g \in G$, $\exists\, r \in \mathbb{Z} \ni g = x^r$.
Similarly since $h \in G$, $\exists\, s \in \mathbb{Z} \ni h = x^s$.
Notice $h = x^s = x^{s-r} x^r = x^{s-r} g$
If $s \geq r$ our $m = s-r$.
If $r > s$ then $h = (x^{-1})^{|s-r|} g$
Since $(x^{-1})^{|s-r|} \in G$ $\exists\, m \ni x^m = (x^{-1})^{|s-r|}$
So $h = x^m g$

or
notice $(hg^{-1})g = h$
Since G is cyclic $\exists\, m \in \mathbb{Z}$ so that $x^m = hg^{-1}$ thus $x^m g = h$ //

start (+.5)
cyclic def (+.5)
got it (+1)

5. [9] (§2) For each of the sets and operations below, fill in the entries with yes or no. If no, briefly explain why. If yes, briefly describe the process you used to reach that anwer.

Sets S & Operator $\star$	Forms a Group	Abelian Group
a) $\{1, i, j, k, -1, -i, -j, -k\}$ $$\begin{array}{ccccccccc} \star & 1 & i & j & k & -1 & -i & -j & -k \\ 1 & 1 & i & j & k & -1 & -i & -j & -k \\ i & i & -1 & -k & j & -i & 1 & k & -j \\ j & j & k & -1 & -i & -j & -k & 1 & i \\ k & k & -j & i & -1 & -k & j & -i & 1 \\ -1 & -1 & -i & -j & -k & 1 & i & j & k \\ -i & -i & 1 & k & -j & i & -1 & -k & j \\ -j & -j & -k & 1 & i & j & k & -1 & -i \\ -k & -k & j & -i & 1 & k & -j & i & -1 \end{array}$$ work (+1)	gp def (+.5) yes (+.5) closure ✓ inverses exist for each ✓ identity is 1 ✓ assoc is tricky to see but there	abelian def (+.5) no (+.5) notice $i*j=k$ but $j*i=-k$
b) $\left\{\begin{pmatrix} a & 0 \\ 0 & b \end{pmatrix} \middle\vert\, ab \neq 0 \,\&\, a, b \in \mathbb{R}\right\}$ $\star$ is matrix multiplication work (+1)	gp def (+.5) yes (+.5) closure ✓ inverse to $\begin{pmatrix} a & 0 \\ 0 & b \end{pmatrix}$ is $\begin{pmatrix} \frac{b}{ab} & 0 \\ 0 & \frac{a}{ab} \end{pmatrix}$ ✓ identity $\begin{pmatrix} 1 & 0 \\ 0 & 1 \end{pmatrix}$ ✓ assoc b/c matrices ✓	yes (+.5) abelian def (+.5) $\begin{pmatrix} a & 0 \\ 0 & b \end{pmatrix}\begin{pmatrix} c & 0 \\ 0 & d \end{pmatrix} = \begin{pmatrix} ac & 0 \\ 0 & bd \end{pmatrix}$ $\begin{pmatrix} c & 0 \\ 0 & d \end{pmatrix}\begin{pmatrix} a & 0 \\ 0 & b \end{pmatrix} = \begin{pmatrix} ca & 0 \\ 0 & db \end{pmatrix}$
b) $\{(x, y) \in \mathbb{R}^2 \mid y^2 = 3x^3 + 5x^2 + 1\}$ (graph shown to the right) $\star$ Let $P, Q \in S$. If $P \neq Q$ draw the line between P & Q. The line will intersect with S at a third point, call it C. Then $P \star Q = C$ If $P = Q$, draw the line tangent to the curve. The tangent line with intersect S at a second point, call it C. Then $P \star Q = C$ work (+1)	no (+.5) 'use' (+.5) clear (+.5) a C doesn't always exist? no closure also: no identity	no (+.5)



Free Response: Show your work for the following problems. The correct answer with no supporting work will receive NO credit.
(If you use a calculator, be sure to tell me.)

6. (§3) Let G be a group and $g \in G$.

(a) [2] Which is larger: the order of G or the order of g. Justify your answer.

def of $|G|$ (+.5)
def of $o(g)$ (+.5)
reasoning (+.5)

(+.5) $|G|$ is larger than $o(g)$.
Recall $o(g)$ is the integer $n \ni g^n = e$ where e is the identity.
Note for all $1 \leq i \leq n$ $g^i \in G$ so g^i is counted when counting the number of elements in G, ie. when finding $|G|$

(b) [3] When is $|G| = o(g)$? (In Gallian's notation: $|G| = |g|$.) Justify your answer.

start (+.5)
notation (+.5)
general (+.5)
get it / reasoning (+.5)

(+1) When g generates G.

Notice $|\langle g \rangle| = |\{g, g^2, g^3, g^4, \ldots\}| = o(g)$
So $|G| = o(g) \iff |G| = |\langle g \rangle|$
Since $g \in G$, the groups G & $\langle g \rangle$ have the same binary operator so G and $\langle g \rangle$ are the same group?

7. [6] (§3) Let G be an Abelian group with identity e and let m be a fixed integer. Show the set of all elements in G that are solutions to $x^m = e$ is a subgroup of G. In symbols show that $\{g \in G | g^m = e\} \leq G$. Let $H = \{g \in G | g^m = e\}$

start (+.5)
subgp def/test (+1)
actually does test (+2)
abstraction (+.5)
notation (+1)
sense/logic (+1)

We will verify the conditions for a set to be a subgroup for H

Non Empty: Notice $e^m = \overbrace{e * e * \cdots * e}^{m \text{ times}} = e$ so e is a solution $\Rightarrow e \in H$.

Closure: Let $g, h \in H$ we wts $g \cdot h \in H$.
Since $g \in H$ we know $g^m = e$. Similarly $h \in H \Rightarrow h^m = e$.
Consider $(gh)^m = g^m h^m$ b/c G is abelian
$= e * e$
$= e$
Thus gh is a solution to $x^m = e \Rightarrow gh \in H$.

Identity: we verified the identity was in H in the non-empty argument.

Inverses: Let $g \in H$, we wts $g^{-1} \in H$.
Since $g \in H$, $g^m = e$ (†) Since G is a group $(g^m)^{-1} \in G$
So (†) can become $e = (g^m)^{-1} \Rightarrow e = (g^{-1})^m$
So $g^{-1} \in H$.

8. (§4) Let $G = \mathbb{Z}_{338}$ under addition modulo ~~60~~ 338.

(a) [1] Find $|G|$. 338 (+1)

(b) [3] List three elements of order 26 in G.

relationship w/ gcd (+.5)
factored 338 (+.5) rule
supporting work (+.5)

$o(2) = 169 = \dfrac{338}{\gcd(2,338)}$

338 → 2, 169; 169 → 13, 13

we want $n \ni o(n) = 26 = \dfrac{338}{\gcd(n,338)}$

$\Rightarrow \gcd(n,338) = \dfrac{338}{26} = 13$

So 13 (+.5) b/c $\gcd(13,338) = 13$

39 (+.5) b/c $\gcd(39,338) = 13$

65 (+.5), 91, 117 etc

(c) [4] Write down the subgroup lattice for $\mathbb{Z}_{338}$

found all sbgps (+3)
ordered correctly (+1)

$\langle 1 \rangle$

$\langle 2 \rangle$ $\langle 13 \rangle$

$\{26, 54, 80, 106, 130, 156, 182, \ldots, 0\} = \langle 26 \rangle$ $\langle 169 \rangle = \{169, 0\}$

$\langle 0 \rangle$