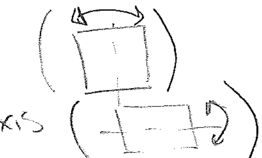
Final Key TMath 402 Winter 2016

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] (§1) Let D_4 be the dihedral group of order 8. For all a, b, and c in D_4, if $ab = bc$, then $a = c$.

State (+.5)
D_4 group (+.5)
Counter ex (+1)

false (+1)

Let F be a flip over the vertical axis 
and H be a flip over the horizontal axis
Let R_{90} be a rotation by 90° counterclockwise

$H R_{90} = R_{90} V$ but $H \neq V$.

2. [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 $x^m g = h$.

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

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 $h = x^s = x^{s-r} x^r = x^{s-r} g$

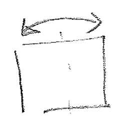
If $s \geq r$ our $m = s - r$.
If $r > s$ then $h = (x^{-1})^{|s-r|} g$

3. [3] (§9) If H is a normal subgroup of a group G, then $ghg^{-1} = h$ for all $h \in H$ and $g \in G$.

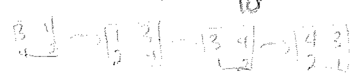
State (+.5)
normal def (+1)
sense (+.5)

false (+1)

Let R_i be rotations counterclockwise i degrees

Note $\{R_0, R_{90}, R_{180}, R_{270}\} \triangleleft D_4$, let F = 

But $F R_{90} F^{-1} = F R_{90} F = R_{270} \neq R_{90}$



or

4. [3] (§13) Let a and b belong to a commutative ring. If ab is a zero divisor, then a or b is a zero divisor.

true (+1)

State (+.5)
def of zero divisor (+1)
logic/sense (+.5)

Since ab is a zero divisor, $\exists$ c in the ring such that $(ab)c = 0$.
Since the ring is commutative we know $acb = 0$.
By associativity either $(ac) \cdot b = 0$ or $a(cb) = 0$
$\Rightarrow$ either b is a zero divisor or a is.

5. (§2, 12 & 13) For each below, find a set and binary operator(s) that satisfies the criteria given, if one exists. If no set exists, explain why.

(a) [3] a ring, but not a field

(+1) well defined set and operators

(+.5) meet conditions

(+1) def of 2 properties/ conditions

(b) [3] an integral domain, but not a ring

(c) [3] a ring, but not a group

(d) [3] a group but not an abelian group

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. Consider S_5, the group of permutations on five elements.

(a) [2] (§5 & 3) Let $H = \{\sigma \in S_5 | \sigma(5) = 1\}$. Determine if $H \leq S_5$ and justify your answer.

sense (+1)
def of subgroup (+1)

Notice the identity $\notin H$ so H is not a subgroup of S_5.

(b) [4] (§5, 7, & 3) Define a subgroup N of S_5 such that $[S_5 : N] = \cancel{6}\ 20$. Justify your choices.

size of S_5 (+.5)
index (+.5)
size of N (+1)
well defined (+.5)
is subgp (+1)
got H (+.5)

Recall $|S_5| = 5 \cdot 4 \cdot 3 \cdot 2 \cdot 1$

Since $[S_5 : N] = \frac{|S_5|}{|N|}$ we know $N = \frac{5 \cdot \cancel{4} \cdot 3 \cdot 2 \cdot 1}{\cancel{20}}$

We need to find a group of order 6 or $3 \cdot 2 \cdot 1$

Let $N = \{\sigma \in S_5 \mid \sigma(1) = 1 \text{ and } \sigma(2) = 2\}$

Notice N is a subgroup since $N = \text{stab}(1) \cap \text{stab}(2)$ (recalling $\text{stab}(i)$ is a subgroup & the intersection of 2 subgroups is a subgroup), and $|N| = 3 \cdot 2 \cdot 1 = 6$.

well defined (+1)
def of eq. rel (+1)
justification (+1)

(c) [3] (§0) Note that S_5 is itself a set (the set of permutations on five elements). Devise an equivalence relation on S_5 and justify your answer.

(Trivial answer) Let R be defined so that $(1) R a$ $\forall a \in S_5$, ie. all elements in S_5 are equivalent to the identity.
We can verify reflexive, symmetric & transitive properties but since everything is equivalent to the identity its boring.

(Trivial answer) Let S be defined so x is only related to itself.
Reflexive: xSx by definition of S
Symmetric: if $xSy \Rightarrow x = y$ so ySx ✓
Transitive: if xSy and ySz then $x = y$ and $y = z$ by def of S, thus xSz ✓

(interesting answers) Let S be defined so $x \sim y$ if $x(1) = y(1)$ ie send 1 to same place

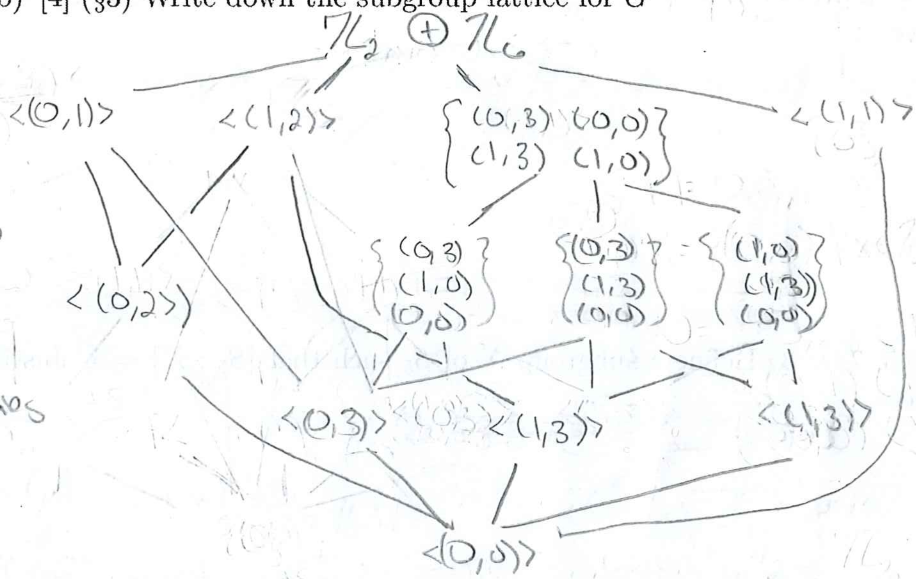
The proof could be showing S_5 is partitioned

7. Let $G = \mathbb{Z}_2 \oplus \mathbb{Z}_6$ under addition modulo 2 in the first coordinate and addition modulo 3 in the second.

(a) [1] (§2) Find $|G|$. $2 \cdot 6 = 12$

(b) [4] (§3) Write down the subgroup lattice for G

trivial sbgp (+.5)
Containments (+1)
+.5 for each proper sbgp up to (+2.0) i.e. 4 sbgps
(+.5) no redundancies



Note: $\{(0,3),(0,0),(1,3),(1,0)\}$ has no generator

(c) [2] (§7) Identify the distinct cosets of $\langle(0,2)\rangle$ in G.

Note $\langle(0,2)\rangle = \{(0,2),(0,4),(0,0)\}$
So there will be $12/3$ or 4 cosets (+.5)

$\langle(0,2)\rangle = \{(0,2),(0,4),(0,0)\}$
$(1,0)+\langle(0,2)\rangle = \{(1,2),(1,4),(1,0)\}$ (+.5)
$(1,1)+\langle(0,2)\rangle = \{(1,3),(1,5),(1,1)\}$ (+.5)
$(0,1)+\langle(0,2)\rangle = \{(0,3),(0,5),(0,1)\}$ (+.5)

(d) [4] (§6 & 9) What group is $\mathbb{Z}_2 \oplus \mathbb{Z}_6/\langle(0,2)\rangle$ isomorphic to? Prove it.

(+1) $\mathbb{Z}_2 \oplus \mathbb{Z}_2$ We'll use the 1st isomorphism theorem

Define $\varphi: \mathbb{Z}_2 \oplus \mathbb{Z}_6 \to \mathbb{Z}_2 \oplus \mathbb{Z}_2$
$(1,0) \mapsto (1,0)$
$(0,1) \mapsto (0,1)$ (+1)

Notice φ is onto and $\mathrm{Ker}\,\varphi = \{(a,b) \mid a=0, b=0 \bmod 2\}$ (+1)
$= \langle(0,2)\rangle$

(+1) Thus by the 1st isomorphism theorem $\exists$ an isomorphism $\bar{\varphi}$ between $\mathbb{Z}_2 \oplus \mathbb{Z}_2$ and the factor group $\mathbb{Z}_2 \oplus \mathbb{Z}_6/\langle(0,2)\rangle$

$$\begin{tikzcd} \mathbb{Z}_2 \oplus \mathbb{Z}_6 \arrow[r, "\varphi"] \arrow[d, "\pi"] & \mathbb{Z}_2 \oplus \mathbb{Z}_2 \\ \mathbb{Z}_2 \oplus \mathbb{Z}_6/\langle(0,2)\rangle \arrow[ur, dashed, "\bar{\varphi}"'] & \end{tikzcd}$$

or

Or could show the Cayley tables of both groups
(+1) for $\mathbb{Z}_2 \oplus \mathbb{Z}_2$ (+2) Cayley for factor group (+1) Cayley of $\mathbb{Z}_2 \oplus \mathbb{Z}_2$

8. Consider the set of polynomials with real coefficients $\mathcal{P}$ with the binary operator of addition. Define a map ϕ that takes a polynomial to its derivative. (+.5)

understood ϕ (+.5) def's (+.5) → not on 1-1 so can't be automorphism

(a) [3] Determine if ϕ is a homomorphism, an isomorphism, or an automorphism. Prove your conclusion.

(+.5) ϕ is a homomorphism b/c $\phi(a_nx^n+a_{n-1}x^{n-1}+\dots+a_0)+\phi(b_nx^n+b_{n-1}x^{n-1}+\dots+b_0)$

$= a_n n x^{n-1}+a_{n-1}(n-1)x^{n-2}+a_1+b_n n x^{n-1}+b_{n-1}(n-1)x^{n-2}+\dots+b_1$

(+.5) not an isomorphism b/c $\phi(2x+7)=\phi(2x)$ i.e. not one-to-one

(+.5) $= \phi(a_nx^n+a_{n-1}x^{n-1}+\dots+a_0+b_nx^n+b_{n-1}x^{n-1}+\dots+b_0)$

i.e. derivative of a sum is the sum of the derivatives

(b) [3] (§10) Identify $\ker\phi$.

$\ker\phi=\{a_nx^n+\dots+a_0 \mid (a_nx^n+\dots+a_1x+a_0)'=0\}$ def of ker (+.1)

$=\{a_nx^n+\dots+a_0 \mid a_n n x^{n-1}+\dots+a_1x=0\}$ particular case (+1) got it (+1)

$=\{a_nx^n+\dots+a_0 \mid a_n=a_{n-1}=0=a_1\} = \{a_0 \mid a_0\in\mathbb{R}\}$ constants?

9. [5] Choose *ONE* of the following. Clearly identify which of the two you are answering and what work you want to be considered for credit.
No, doing both questions will not earn you extra credit.

(a) (§7) Suppose G is a finite group of order n and m is relatively prime to n. If $g \in G$ and $g^m = e$, prove that $g = e$.

(b) (§6) Find the order of $\text{Aut}(\mathbb{Z}_n)$ where n is a fixed positive integer. Prove your result.

Style (+1) abstract (+1)

(a)

(+.1) Notice since $g^m=e$, that $o(g)\mid m$.

Consider $\langle g\rangle \leq G$ by LaGrange

(+.1) we know $|\langle g\rangle| \mid |G| \Rightarrow |\langle g\rangle| \mid n$

Because $o(g)=|\langle g\rangle|$ we thus have $o(g)\mid n$.

So $o(g)\mid m$ and $o(g)\mid n$

correct logic (+1) Since $\gcd(m,n)=1$

$o(g)$ must be 1

There is only one element with order 1: the identity.

Thus $g=e$.

style (+1)
abstract (+1)

(b)

Recall $\text{Aut}(\mathbb{Z}_n)=\{\varphi:\mathbb{Z}_n\to\mathbb{Z}_n \mid \varphi \text{ is an iso}\}$

(+1) We will show $|\text{Aut}(\mathbb{Z}_n)|$ is equal to the # of $i \ni \gcd(n,i)=1$.

Note $\mathbb{Z}_n$ is cyclic so to define a homomorphism it suffices to provide the image of 1.

(+1) For φ to be an isomorphism $\varphi(1)$ will need to generate $\mathbb{Z}_n$ so $\langle\varphi(1)\rangle=\mathbb{Z}_n$. It suffices to find $\varphi(1) \ni |\langle\varphi(1)\rangle|=n$.

(+1) Recall $o(\varphi(1))=|\langle\varphi(1)\rangle|$ and $o(\varphi(1))=\dfrac{n}{\gcd(\varphi(1),n)}$

Thus $n=\dfrac{n}{\gcd(\varphi(1),n)}$.

So $\varphi(1)$ can be any element in $\mathbb{Z}_n$ $\ni \gcd(\varphi(1),n)=1$