Key

Vanderpool

TMath 402

Autumn 2022

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] (§2.2) Let a and b be integers and p be a prime number. If p divides ab, then either p divides a or p divides b.

(+1) True

logic (+1)

Without loss of generality assume p does not divide a, then it suffices to show p divides b.
Note since p is prime and p does not divide a, $\gcd(p,a)=1$.
So $\exists\ r,s \in \mathbb{Z} \ni 1 = rp + sa$.
Note then $1(b) = (rp+sa)b = rpb + sab$. Since p divides ab p divides sab. Certainly p divides rpb. Thus p divides rpb+sab or b.

2. [3] (§3.2) All groups are abelian/commutative.

False (+1)

Consider $D_4 = \{r, s \mid e = r^4 = s^2 \text{ and } srs = r^{-1}\}$
since $srs = r^{-1} \Rightarrow sr = r^{-1}s$
so s does not commute with r.

(.5) looking for counter ex
(+1) found counter ex
(1.5) Clarity/explanation

Consider S_{10} or the symmetric group on 10 elements.
Notice $(123)(12) = (13)(2)$ but
$(12)(123) = (1)(23)$ which are not equal

3. [3] (§5.1) Let $\sigma \in S_{12}$. Then $\sigma^{12} = ()$.

False (+1)

Consider $(123)(45678) \in S_{12}$
Notice the order of (123) is 3 and the order of $(45678) = 5$.

(.5) looking for counter ex
(+1) Know order prop/def
(.5) got one

Thm's from class $\Rightarrow$ the order of $(123)(45678) = 3 \cdot 5$ or 15.
Since $12 < 15$, by definition of order we know
$[(123)(45678)]^{12} \neq ()$

Free Response: Show your work for the following problems. The correct answer with no supporting work will receive NO credit.

4. [9] For each of the sets and operations below, determine if they define a group. If no, briefly explain why. If yes, briefly describe the process you used to reach that answer.

Sets S & Operator $\star$	Is a Group?
a) $\mathbb{Z}_{10}$ $\star$ is multiplication under modulo 10	(+.5) No - If $\star$ is multiplication we need 1 to be the identity. (+.5) Notice $0 \in \mathbb{Z}_{10}$ but $\nexists$ multiplicative inverse for 0
(+.5) since (+.5) prop of group	(+1) using binary op. defined
b) $\{a, b, c, d\}$ $\star$ is defined by (table below)	(+.5) No - We need an identity. It looks like b should be the identity b/c the b^{th} row (indicating $b\alpha = \alpha$ for all α) But the circled spot indicates $cb \neq c$ and $db \neq d$. (+.5) We are missing a two sided identity
(+.5) since (+.5) prop of group	(+1) reading Cayley Table
c) Set generated by r and s subject to the relations $e = r^{10} = s^2$ and $srs = r^{-1}$ where e is the identity.	Yes? This is D_{10} as defined in the text (Ch 5.2) So recognizing it can work. OR Closure - get b/c defined in terms of generators Identity - get with r^{10} inverses - $s^2 = e \Rightarrow s$ is own inverse $r^{10} = e \Rightarrow$ we can build r's

Table for b):

$\star$	a	b	c	d
a	b	a	d	c
b	a	b	c	d
c	c	d	b	a
d	d	c	a	b

5. [2] Choose a set (any set you want!) and define a (non-trivial) equivalence relation on it. (Non-trivial means that every element is not in its own equivalence class nor that all elements are in the same equivalence class.)

Set (+.5)

equivalence relation (+.5)

well defined / understandable (+1)

6. Consider the integers $\mathbb{Z}$ with the the binary operator of addition. Let α be an integer. Define $\alpha\mathbb{Z} = \{\alpha k | k \in \mathbb{Z}\}$.

written additively

(a) [4] (§3.3) Show $5\mathbb{Z}$ is a subgroup of $\mathbb{Z}$.

work with $\alpha\mathbb{Z}$ (+.5)

We use a property and show $5\mathbb{Z} \neq \emptyset$ and if $g, h \in 5\mathbb{Z}$, then $g-h \in 5\mathbb{Z}$.

use def/prop of subgp (+1.5)

Notice $0 \in 5\mathbb{Z}$. So $5\mathbb{Z} \neq \emptyset$.

notation/consistent (+.5)

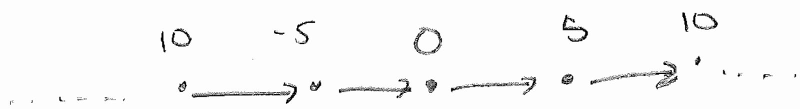
Let $h \in 5\mathbb{Z}$. Then $\exists\, k \in \mathbb{Z} \ni h = 5k$. Notice $-5k$ is the inverse to h because $h + (-5k) = 5k - 5k = 0$ (recalling the group is additive). Thus $h \in 5\mathbb{Z}$.

Check each prop (+1.5)

Let $g \in 5\mathbb{Z}$ and consider $g-h$. Since $g \in 5\mathbb{Z}$, $\exists\, l \in \mathbb{Z}$ $\ni g = 5l$. So $g-h = 5l - 5k = 5(l-k)$. Since $l-k \in \mathbb{Z}$ we know $g-h \in 5\mathbb{Z}$, which completes the proof. //

(b) [3] (ModuloActivity) Draw (a partial) Cayley Diagram for $5\mathbb{Z}$.

elements/vertices (+1)
generator/arrows def (+1)
shape/pt # (+1)



where the arrows correspond with adding 5

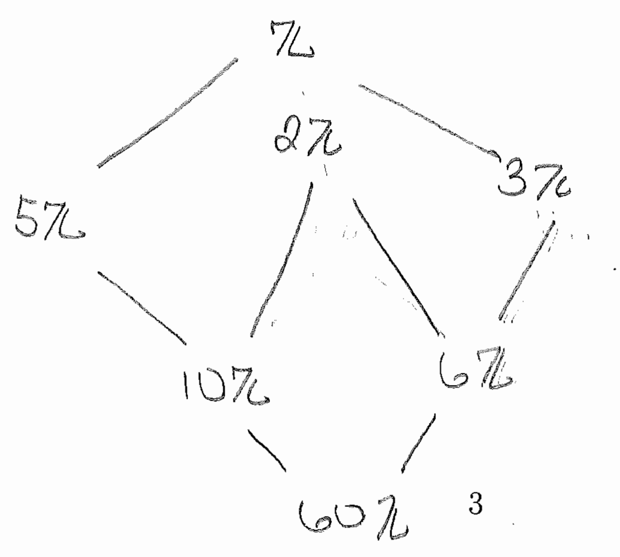
(c) [2] (4.1) Find a subgroup of $5\mathbb{Z}$.

$10\mathbb{Z} = \{ \ldots -20, -10, 0, 10, 20, \}$

(d) [3] Create a partial subgroup lattice for $\mathbb{Z}$. Include $5\mathbb{Z}$ and your answer to part (c) in the lattice.

(+.5) (+.5) Containment (+1.5)

arguable that all these subgroups (generated by primes) are the same 'size' - think cardinality



There are sooo many subgroups one could build in this lattice

(+.5) Start a lattice

7. [8] Choose *ONE* of the following theorems to prove. Clearly identify which of the two you are proving and what work you want to be considered for credit.
No, doing both questions will not earn you extra credit.

Theorem 1. *Let G be a group. Prove that $ba = ca$ implies $b = c$ and $ab = ac$ implies $b = c$ for all elements a, b, and c in G.* ((typo?))

Theorem 2. *Let G be a finite cyclic group with order 20 generated by g . Prove g^n generates G if and only if* $\gcd(n, 20) = 1$.

Thm 1 Proof:

Let $a,b,c \in G$. We will assume the two statements, one after each other.

Assume $ba=ca$. Since G is a group, there exists $a^{-1} \in G$. Act by a^{-1} on the right of the given equation. So:

$ba=ca$

$\Rightarrow (ba)a^{-1}=(ca)a^{-1}$ by associativity

$\Rightarrow b(aa^{-1})=c(aa^{-1})$ by def. of inverse

$\Rightarrow be=ce$ by def. of identity

$\Rightarrow b=c$

Similarly, we assume $ab=ac$. We now act by a^{-1} on the left of $ab=ac$ to find:

$ab=ac$

$a^{-1}(ab)=a^{-1}(ac)$ by assoc

$(a^{-1}a)b=(a^{-1}a)c$

$eb=ec$

$b=c$.

We proved both statements //

Thm 2 Proof:

We will show two directions. First assume $\gcd(n,20)=1$. We want to show $G=\langle g^n \rangle$.

Since $\gcd(n,20)=1$, $\exists\, r,s \in \mathbb{Z} \ni rn+s\cdot 20=1$. Since $G=\langle g\rangle$, we know $g^{20}=e$. So

$(g^n)^r=g^{nr}=g^{nr}e^s=g^{nr}(g^{20})^s=g^{nr+20s}=g$

Thus $g \in \langle g^n \rangle$. Since the generator of G is in the subgroup $\langle g^n \rangle$, we know $\langle g^n \rangle$ must generate all of G. Thus $G=\langle g^n \rangle$.

For the 2nd direction, assume $\langle g^n \rangle = G$. Recall from a Thm in class the order of g^n is $\dfrac{20}{\gcd(n,20)}$. Since g^n generates G, the order must be 20 so $\gcd(n,20)=1$ which is what we wanted to show //

(+1) both statements stated
(+1) state assumptions each time
(+1) group prop/act consistently
(+1) computations

(+1) both directions stated
(+1) state assumptions each time
(+1) order prop/def
(+1) computations

4	3	2	1
well written	good but some math errors or writing that needs addressing	good intuition but at least one serious flaw	I don't understand but I see you worked