Median 29.25 (73%)
Ave 26.7 (67%)

Key

Vanderpool

TMath 403

Spring 2024

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] If p is prime, then there is only one finite ring of order p.

False. (.5) Consider $\mathbb{Z}_5$. (which has order 5)

start (.5)
def of ring (.5)
order p/other def (.5)
found counter ex (1)

We can define two different kinds of multiplication:
let $a, b \in \mathbb{Z}_5$

Ring 1: $a \cdot b = a \cdot b \bmod 5$

Ring 2: $a \cdot b = 0$

(note: this would be true if the statement was about groups)

2. [3] Let R be a ring and $x \in R$. If x is not a unit, then x is a zero divisor.

False. (.5) Consider $\mathbb{Z}_5[x] = \{a_0 + a_1x^1 + \dots + a_nx^n \mid a_i \in \mathbb{Z}_5,\ n \in \mathbb{N}\}$
(the set of polynomials in x with coefficients in $\mathbb{Z}_5$)

start (.5)
def of unit (.5)
def of zerodivisor (.5)
found counter ex (1)

Note x is not a unit b/c $\nexists\, p(x) \in \mathbb{Z}_5[x]$ so that $x \cdot p(x) = 1$
Note also x is not a zero divisor

3. [3] Let R be a ring with unity/one. Show if $\phi : R \to S$ is a ring homomorphism then $\phi(1)$ is idempotent.

True (.5) Recall $\alpha \in R$ is idempotent if $\alpha \cdot \alpha = \alpha$.

start (.5)
idempotent def (.5)
ring homom (.5)
logic (1)

Since $\phi : R \to S$ is a ring homomorphism
$\phi(a \cdot b) = \phi(a)\phi(b) \quad \forall a, b \in R$.
Since R is a ring with unity, $\exists\ 1 \in R \ni 1 \cdot a = a\ \forall a \in R$.
Observe $\phi(1) = \phi(1 \cdot 1)$ b/c 1 is mult. identity
$= \phi(1)\phi(1)$ b/c ϕ is ring. homom
So $\phi(1) = [\phi(1)][\phi(1)] \Rightarrow \phi(1)$ is idempotent.

4. [8] For each of the terms below, determine if the term is used to describe an element, a set, both, or neither. Then provide examples for each.

		element?	set?
an example	abelian	no	yes, groups work $C_5 = \{r \mid r^5 = 1\}$
+2	unit	1.5 yes in $\mathbb{Z}_5$, 2 is a unit b/c $2 \cdot 3 = 1$ in $\mathbb{Z}_5$	.5 no (although close to R having unity or mult. identity)
+2	zero divisor	1.5 yes in $\mathbb{Z}_{12}$, 6 is a zero div b/c $6 \cdot 2 = 0$ but $6 \neq 0$	.5 no
+2	kernel	.5 no	yes 1.5 let $\varphi: \mathbb{Z}_5 \to \mathbb{Z}_5$, $1 \mapsto 1$, $\operatorname{Ker}\varphi = \{0\}$ b/c $\varphi(0) = 0$
+2	prime	1 yes in $\mathbb{Z}$, 5 is prime b/c only divisors are 1 and 5	1 yes an ideal can be prime in $\mathbb{Z}_{12}$ $(2) = \{2, 4, 6, 8, 10, 0\}$ b/c if $a \cdot b \in (2)$ then either $a \in (2)$ or $b \in (2)$

5. Consider $R = \mathbb{Z}_9 \times \mathbb{Z}_3$.

(a) [3] Find an ideal I, so that R/I is a ring but not a field. Justify your answer.

start (+.5)
ideal (+.5)
not field (+.5)
justify (+1)
notation (+.5)

$I = ((0,1))$ note I is not a maximal ideal b/c $((0,1)) \subset ((3,1))$

note $R/I \cong \mathbb{Z}_9$ which is a ring b/c I is an ideal but not a field b/c

$(3+I)\cdot(3+I) = 9 + I = I$

$\Rightarrow$ there are zero divisors $\Rightarrow$ $3+I$ is not a unit.

(b) [3] Find an ideal I, so that R/I is a field. Justify your answer.

start (+.5)
field (+.5)
justify (+1)
notation (+.5)
~~Sense~~ (+.5)

$I = ((1,0))$ note I is maximal so R/I will be a field

In particular $R/I \cong \mathbb{Z}_3$ which is a commutative ring where all elements are units.

6. Use the first three letters of your first name to build a polynomial of the form $a_0 + a_1x + a_2x^2$ in $\mathbb{Z}_3[x]$. Specifically, use the table below to let a_0 be the number that corresponds to the first letter in your first name. For Ruth then "R" would set $a_0 = 0$. Let a_1 be the number that corresponds to the second letter and a_2 correspond to the third letter. For Ruth then $a_1 = 0$ and $a_2 = 2$, thus the polynomial for Ruth is $0 + 0x + 2x^2$.

1	A	D	G	J	M	P	S	V	Y
2	B	E	H	K	N	Q	T	W	Z
0	C	F	I	L	O	R	U	X	

(a) [1] Let $p(x)$ represent the polynomial of the form $a_0 + a_1x + a_2x^2$ corresponding with your first name. Write down $p(x)$.

R $\Rightarrow a_0 = 0$ So $0 + 0x + 2x^2$

U $\Rightarrow a_1 = 0$

T $\Rightarrow a_2 = 2$

(b) [2] Find a representative of x^3 in $\mathbb{Z}_3[x]/(p(x))$ with degree less than 2.

use ideal (+1)

$x^3 = x(x^2)$

$2x^2 \in (2x^2)$ note $x^2 = (2\cdot 2)x^2 \in (2x^2)$

$\Rightarrow$ in $\mathbb{Z}_3[x]/(p(x))$ $x^3 = x(x^2) \in (2x^2)$ so $x^3 \sim 0$

(c) [4] how many elements does $\mathbb{Z}_3[x]/(p(x))$ have? Justify your answer.

start (+.5)
sense/notation (.5) (+1)

Note $x^2 \in (2x^2) \Rightarrow$ cannot have elements of order 2 or higher

$\Rightarrow$ elements will look like

(+1) $a_0 + a_1x$ where $a_0, a_1 \in \mathbb{Z}_3$

(+1) $\Rightarrow$ there are $3\cdot 3$ or 9 elements:

unique representatives are:

$0 \quad 1 \quad 2 \quad x \quad x+1 \quad x+2 \quad 2x \quad 2x+1 \quad 2x+2$

7. Consider:

Theorem 1. *Let I and J be ideals in a ring R. Then $I \cap J$ is an ideal in R.*

(a) [2] Find an example I, J, and R that helps verify Theorem 1.

R (+.5)
ideals (+.5)
work (+.5)
sense/notation (+.5)

in $\mathbb{Z}_{12}$ let $I = (3) = \{3, 6, 9, 0\}$
$J = (2) = \{2, 4, 6, 8, 10, 0\}$

Notice $I \cap J = \{6, 0\} = (6)$
which is an ideal.

(b) [8] Prove Theorem 1.

start (+.5)
def of ideal (+1.5)
element intro (+.5)
general cases/commutative (-1)
sense/notation (+.5)

Writing Prove (+4)

We check the definition of an ideal:

Subgroup: Recall I and J are also subgroups b/c they are ideals

1) Closure: Let $x, y \in I \cap J$. We wts $x + y \in I \cap J$.
Since I is a subgroup under $+$, $x + y \in I$.
Similarly for $J \Rightarrow x + y \in J$. Thus $x + y \in I \cap J$.

2) Identity: Since I and J are subgroups $\exists\, 0 \in I$ and $0 \in J$
$\Rightarrow 0 \in I \cap J$

3) Inverses: Since I is a subgroup, $\forall x \in I$, $\exists -x \in I$
Similarly for $J \Rightarrow \forall x \in I \cap J$, $x^{-1} \in I \cap J$.

Subring: Recall I and J are also subrings b/c they are ideals

1) Mult. closure: Let $x, y \in I \cap J$. We wts $x \cdot y \in I \cap J$.
Since I is a subring under mult, $x \cdot y \in I$.
Similarly for $J \Rightarrow x \cdot y \in J$. Thus $x \cdot y \in I \cap J$.

Ideal: Let $x \in I \cap J$ and $a \in R$. We wts $ax, xa \in I \cap J$.
Since I is an ideal we know $ax \in I$ and $xa \in I$.
Similarly b/c J is an ideal we know $ax \in J$ and $xa \in J$.
Thus $ax \in I \cap J$ and $xa \in I \cap J$. //

note R was not given to us as commutative