1) Given a ring R with 1, then: $(-1)^2 - 1 = -1(-1+1)$ ✓

5

$= -1(0)$ ✓

$= 0.$ ✓

Due to the uniqueness of inverses over group operations, $(-1)^2 = 1$. ✓ Furthermore, given a unit $u \in R$, then there exists $x \in R$ such that $ux = 1 = (-1)^2$. Thus: $ux = (-1)^2 ux = 1$, ✓ implying $(-1)ux = -1$. ✓ Right multiplying by -1 shows $(-1)ux(-1) = (-1)^2 = 1 = -u(-x)$. Therefore, $-u$ is a unit in R ✓

Ex 2

5 Subrings of $\mathbb{Q}$: Let R =

a) set of rational #s w/ odd denominators (when written in lowest terms)

yes. $\frac{1}{1} \in R$. Also, if $\frac{p}{q}, \frac{p_2}{q_2} \in R$,

closed under sub:

$$\frac{p}{q} - \frac{p_2}{q_2} = \frac{pq_2 - p_2q}{qq_2}$$ and qq_2 is odd. ✓

Moreover, any reductions will take away an odd factor of qq_2 and the reduction of qq_2 will still be odd. ✓

good.

closed under mult:

$\frac{p}{q}\frac{p_2}{q_2} \in R$ b/c qq_2 is odd and $\frac{p_2}{q}, \frac{p}{q_2}$ will reduce to some #/odd #. ✓

5

5. Let B be a Boolean ring and let a, b $\in B$. Observe: $-a = (-a)^2 = a \ \forall a \in B$, then, $(a+b) \in B$ so, $(a+b)^2 = (a+b)^2 = a^2 + ab + ba + b^2 \Rightarrow (a-a^2)+(b-b^2) = ab + ba$ $\Rightarrow ba = -ab = ab$, thus, $ab = ba$, so B is commutative $\square$. Perfect

Exercise 4. Let K be a field. A *discrete valuation* on K is a function $v : K^\times \to \mathbb{Z}$ satisfying

(i) $v(ab) = v(a) + v(b)$ for all $a, b \in K^\times$ (*i.e.*, v is a homomorphism [think logarithm!]),

(ii) v is surjective, and

(iii) $v(x + y) \geqslant \min\{v(x), v(y)\}$ for all $x, y \in K^\times$ with $x + y \neq 0$.

The set $\mathcal{O}_v = \{x \in K^\times \mid v(x) \geqslant 0\} \cup \{0\}$ is called the *valuation ring* of v.

(a) Prove that $\mathcal{O}_v$ is a subring of K containing 1.

(b) Prove that for each $x \in K^\times$, x or x^{-1} is in $\mathcal{O}_v$.

(c) Prove that an element x is a unit of $\mathcal{O}_v$ if and only if $v(x) = 0$.

Proof. Let $a, b \in K$ such that $v(a), v(b)$ greater than or equal to 0. $v(a + b) \geqslant \min\{v(a), v(b)\}$ so $v(a + b)$ is greater than or equal to zero.✓ $v(ab) = v(a) + v(b)$ so $v(ab)$ is greater than or equal to 0.✓ So $\mathcal{O}_v$ is closed over addition and multiplication. $v(1) = v(-1) + v(-1) = 0$, so $v(-1) = 0$, so we have inverses. $v(a * 1) = v(a) = v(a) + v(1)$, so $v(1) = 0$, so $\mathcal{O}_v$ is a subring with 1. ✓

$v(1) = v(xx^{-1}) = v(x) + v(x^{-1}) = 0$, so $v(x) = -v(x^{-1})$. Assuming $v(x) \neq 0$, then either $v(x)$ is positive and so in $\mathcal{O}_v$, or $v(x^{-1})$is. If $v(x) = 0$, then both are, I assume we mean inclusive or here.✓

Assume $v(x) = 0$, then $v(x^{-1}) = 0$, so both are within $\mathcal{O}_v$, so x is a unit. ✓

Assume x and x^{-1} are in $\mathcal{O}_v$, then $v(x) \geqslant 0$ and $v(x^{-}1) \geqslant 0$. If $v(x) > 0$, since $v(x) = -v(x^{-1})$, $v(x^{-1}) < 0$. So, by contradiction, $v(x) = 0$. ✓ □

Problem 5: Fix a prime p and define $v_p : \mathbb{Q}^{\times} \to \mathbb{Z}$ by $v_p(a/b) = \alpha$ where $a/b = p^{\alpha} \cdot c/d$ where $p \nmid c$ and $p \nmid d$.

a) Prove v_p is a valuation

(i) Let $a, a' \in \mathbb{Q}^{\times}$. Then there exist $c, c', d, d', \alpha, \alpha' \in \mathbb{Z}$ such that $p \nmid c, p \nmid c', p \nmid d, p \nmid d'$ and

$$a = p^{\alpha} \frac{c}{d} \quad \text{and} \quad a' = p^{\alpha'} \frac{c'}{d'}$$

Then

$$\begin{aligned} v_p(a \cdot a') &= v_p\left(p^{\alpha} \cdot \tfrac{c}{d} \cdot p^{\alpha'} \tfrac{c'}{d'}\right) \\ &= v_p\left(p^{\alpha+\alpha'} \cdot \left(\tfrac{cc'}{dd'}\right)\right) \\ &= \alpha + \alpha' \qquad (\text{since } c, c', d, d' \nmid p) \\ &= v_p(a) + v_p(a') \end{aligned}$$

(ii) Let $n \in \mathbb{Z}$. Then $p \nmid 1$? so let $a = p^n$

$$v(a) = v(p^n) = n \checkmark$$

Consequently, v_p is surjective.

(iii) Suppose, without loss of generality, that $\alpha \leq \alpha'$. Then

$$\begin{aligned} v(a+a') &= v\left(p^{\alpha} \tfrac{c}{d} + p^{\alpha'} \tfrac{c'}{d'}\right) \\ &= v\Big(p^{\alpha}\underbrace{\left(\tfrac{c}{d} + p^{\alpha'-\alpha} \tfrac{c'}{d'}\right)}_{\text{has a power of } p \geq 0 \text{ since the addition won't have a power of } p \text{ in the denominator}}\Big) \\ &= \alpha + (\text{unknown positive}) \geq \alpha = \min\{v(a), v(a')\} \checkmark \end{aligned}$$

good.

Thus v_p is a valuation.

b) Prove that $\mathcal{O}_{v_p} = \{a/b \in \mathbb{Q} \mid (p,b) = 1\}$. Let $x = a/b$ be irreducible, and also $a/b = p^{\alpha} c/d$ where $c, d \in \mathbb{Z}$.

$$\begin{aligned} x \in \mathcal{O}_{v_p} &\iff v(x) \geq 0 \\ &\iff v(a/b) \geq 0 \\ &\iff p \nmid b \quad (\text{if } p \mid b,\ p \nmid a \text{ so } \alpha \text{ is negative}) \\ &\iff (p,b) = 1 \checkmark \end{aligned}$$

□

c) ~~Part~~ e, Determine what rational numbers constitute $\mathcal{O}_{v_p}^{\times}$, the units in $\mathcal{O}_{v_p}$.

Answer By exercise 4 part c we know the units of $\mathcal{O}_{v_p}$ are elements of $\mathbb{Q}^{\times}$ such that $v(x) = 0$. Well letting $x = \frac{a}{b} p^{\alpha}$ ~~$\frac{c}{d}$~~ $c, d \nmid p$
$\boxed{\text{irreducibe}}$

$$v(x) = 0 \Longleftrightarrow \alpha = 0$$

$$\Longleftrightarrow a \nmid p \text{ and } b \nmid p$$ ✓

$$\Longleftrightarrow (a,p) = 1, (a,b) = 1, (b,p) = 1$$ ✓ □

5

6. We would like to show that for $M = \sum a_i g_i \in \mathbb{Z}G$, $MN = NM$. $MN = (a_1g_1 + a_2g_2 + \ldots a_ng_n) \times (g_1 + g_2 + g_3 + \ldots g_n)$. The k^{th} coefficient of this product will be $\sum_{g_ig_j=g_k} a_i$ ✓ for any k between 1 and n. $NM = (g_1 + g_2 + \ldots g_n) \times (a_1g_1 + a_2g_2 + \ldots a_ng_n)$, with the k^{th} coefficient being $\sum_{g_ig_j=g_k} a_j$. ✓ We need to show that this comes to the same thing. Observe that $(a_1g_1 + a_2g_2 + \ldots a_ng_n) \times (g_1 + g_2 + g_3 + \ldots g_n) = (a_1g_1g_1 + a_1g_1g_2 + \ldots + a_1g_1g_n + \ldots)$, so each a_i is distributed across all possible products g_ig_j. Therefore, the sums are the same, and the coefficients of the k^{th} product are the same in MN and NM for all possible k. ✓

Explanation could tightened.

✓

$\{g_ig_j = g_k\}$ is the same as $\{g_ig_j = g_{k'}\}$ for all k, k'.

9

7. Suppose for contradiction that $\mathbb{Q}[x] \cong \mathbb{Z}[x]$. Then there would exists $\varphi : \mathbb{Q}[x] \to \mathbb{Z}[x]$ where φ is a ring isomorphism. We know that $\varphi(1) =$

5

Note that if $\mathbb{Q}[x] \cong \mathbb{Z}[x]$, then given a function $\sum_{i=0}^{n} a_i x^i \in \mathbb{Q}[x]$, $\varphi(\sum_{i=0}^{n} a_i x^i) = \varphi(\sum_{i=0}^{n} \frac{a_i}{2} x^i + \sum_{i=0}^{n} \frac{a_i}{2} x^i)$

$$= \varphi(\sum_{i=0}^{n} \frac{a_i}{2} x^i) + \varphi(\sum_{i=0}^{n} \frac{a_i}{2} x^i)$$

$$= 2\varphi(\sum_{i=0}^{n} \frac{a_i}{2} x^i).$$

since φ is surjective, it must be the case that $2 \mid m \ \forall m \in \mathbb{Z}[x]$.

Since this is not the case, by noting odd constant functions in $\mathbb{Z}[x]$, $Z[x] \cong Q[x]$ ✓

good

5

8. In checking whether or not any given set is an ideal, it is necessary to check that the set is a subring and that it is closed under multiplication by arbitrary elements of the ring. This means that we need to check that it is closed under subtraction by elements within the set, and by multiplication by arbitrary elements, which compresses the ideal criterion check and the second component of the subring check into one step. → You keep saying "subtraction" revisit your notes to see that we define additive inverses, and reduce "subtraction" to addition of additive inverses. This tidies up the axiomatization.

It is closed under subtraction because $(3a_0 + a_1x + ... + a_nx^n) - (3b_0 + b_1x + ...b_nx^n) = 3(a_0 - b_0) + ...$ It is also closed under multiplication for any polynomial, b - $ab = ba = 3a_0b_0 + ...$ Thus this is a ~~subring.~~ ideal ✓

(b) This is not an ideal. It is not closed under multiplication by any polynomial b. If $a \in \mathbb{Z}[x]$ has $3a_2x^2$, then the relevant coefficient of ab is $a_0b_2 + a_1b_1 + 3a_2b_0$, which is not necessarily a multiple of 3. ✓

(c) This is closed under subtraction, because for all components from 0 to 2, $0 - 0 = 0$. It is also closed under multiplication. In the constant term, for a in our set, and $b \in \mathbb{Z}[x]$, $a_0b_0 = 0b_0 = 0$. Then $a_0b_1 + a_1b_0 = 0b_1 + 0b_0 = 0$ and $a_0b_2 + a_1b_1 + a_2b_0 = 0$. Going the other way, $b_0a_0 = 0$, $b_00 + b_10 = 0$, and $b_00 + b_10 + b_20 = 0$. Thus the product on both sides is the same, and the first three terms are 0. So closure is demonstrated for arbitrary b. The set is therefore an ideal. ✓

✓ (d) This is not an ideal either. For a in the set, and b an arbitrary integer polynomial the first term of ab is $a_0b_1 + a_1b_0$. $a_1 = 0$ by our condition, but a_0 is not necessarily zero, nor is b_1. This is the coefficient for x, which is an odd term. Therefore this set is not an ideal.

✓ (e) Note that the sum of the coefficients for a in our set is $a(1) = 0$, or the polynomial evaluated at 1. Then if b's coefficients also sum to 0, $(a - b)(1) = a(1) - b(1) = 0$. Thus we have closure ✓

under subtraction. Then for any integer polynomial b, $ab(1) = a(1)b(1) = b(1)a(1) = ba(1) = 0$, so the ideal condition is met. This is an ideal. ✓

(f) Let $p(x) = x^2 + 3$ and let $q = 3x$. $p'(0) = 0$, however $(pq)'(x) = 9x^2 + 9$, and $(pq)'(0) = 9$. So the ideal condition is not met. ✓

5

Problem 9. Find all ring homomorphisms $\mathbb{Z} \to \mathbb{Z}/30\mathbb{Z}$. In each case describe the kernel and the image.

Proof. There are 8 ring homomorphisms that I was able to find (you didn't ask for proof that I found all of them, just that I find all of them). $\varphi_1(z) = 0 + 30\mathbb{Z}$ has kernel $\mathbb{Z}$ and image 0. $\varphi_2(z) = 15(z \mathrm{mod} 2) + 30\mathbb{Z}$ has kernel $2\mathbb{Z}$ and image $\{0 + 30\mathbb{Z}, 15 + 30\mathbb{Z}\}$. $\varphi_3(z) = 10(z \mathrm{mod} 3) + 30\mathbb{Z}$ has kernel $3\mathbb{Z}$ and image $\{0 + 30\mathbb{Z}, 10 + 30\mathbb{Z}, 20 + 30\mathbb{Z}\}$. $\varphi_4(z) = 6(z \mathrm{mod} 5) + 30\mathbb{Z}$ has kernel $5\mathbb{Z}$ and image $\{0 + 30\mathbb{Z}, 6 + 30\mathbb{Z}, 12 + 30\mathbb{Z}, 18 + 30\mathbb{Z}, 24 + 30\mathbb{Z}\}$. $\varphi_5(z) = 5(z \mathrm{mod} 6) + 30\mathbb{Z}$ has kernel $6\mathbb{Z}$ and image $\{0+30\mathbb{Z}, 5+30\mathbb{Z}, 10+30\mathbb{Z},$ ✓

$15+30\mathbb{Z}, 20+30\mathbb{Z}, 25+30\mathbb{Z}\}$. $\varphi_6(z) = 3(z\mathrm{mod}10)$ has kernel $10\mathbb{Z}$ and image $\{0+30\mathbb{Z}, 3+30\mathbb{Z}, 6+30\mathbb{Z}, 9+30\mathbb{Z}, 12+30\mathbb{Z}, 15+30\mathbb{Z}, 18+30\mathbb{Z}, 21+30\mathbb{Z}, 24+30\mathbb{Z}, 27+30\mathbb{Z}\}$. $\varphi_7(z) = 2(z\mathrm{mod}15)$ has kernel $15\mathbb{Z}$ and image $\{0+30\mathbb{Z}, 2+30\mathbb{Z}, 4+30\mathbb{Z}, 6+30\mathbb{Z}, 8+30\mathbb{Z}, 10+30\mathbb{Z}, 12+30\mathbb{Z}, 14+30\mathbb{Z}, 16+30\mathbb{Z}, 18+30\mathbb{Z}, 20+30\mathbb{Z}, 22+30\mathbb{Z}, 24+30\mathbb{Z}, 26+30\mathbb{Z}, 28+30\mathbb{Z}\}$. Finally, $\varphi_8(z) = z+30\mathbb{Z}$ ✓ has kernel $30\mathbb{Z}$ and image $\mathbb{Z}/30\mathbb{Z}$. ✓ □

5

Question 10a. Prove that $I + J$ is the smallest ideal containing I and J.

Proof. First, since $0 \in I$ and $0 \in J$, $I \subseteq I + J$ and $J \subseteq I + J$. Second, I believe we showed that $I + J$ is an ideal in class. It's pretty clear. Third, I show that $I + J$ is the smallest ideal containing I and J. Suppose that K is any ideal of R such that $I \subseteq K$ and $J \subseteq K$. Let $i+j$ be an arbitrary element of $I+J$. We know $i, j \in K$ since $I, J \subseteq K$. Moreover, K is an ideal, so it closed under addition, so $i+j \in K$. Therefore $I+J \subseteq K$, and K was any ideal containing I and J, so $I + J$ is the smallest such ideal. ✓ □

Question 10b. Prove that IJ is an ideal contained in $I \cap J$.

Proof. First I prove that IJ is an ideal. Let $\sum a_ib_i$ and $\sum c_id_i$ be sums in IJ where $a_i, c_i \in I$ and $b_i, d_i \in J$. Then

$$\sum a_ib_i - \sum c_id_i = \sum a_ib_i + \sum(-c_i)d_i \qquad \text{since } I \text{ closed under negation}$$

And the left side is a finite sum of products of I and J, so ✓ it is an element of IJ. So IJ is closed under subtraction. Let $r \in R$ and $\sum a_ib_i \in IJ$. Then

$$r\sum a_ib_i = \sum(ra_i)b_i \checkmark$$

And I is closed under multiplication by r so $ra_i \in I$, so $\sum(ra_i)b_i \in IJ$. Likewise by symmetry, $(\sum a_ib_i)r \in IJ$. ✓ Therefore IJ is closed under multiplication by elements of r. And therefore IJ is an ideal since it is closed under subtraction and closed under left and right multiplication by elements of R. ✓

Second I prove that $IJ \subseteq I \cap J$. IJ is the set of finite sums of products of the form ij with $i \in I$ and $j \in J$. Every product ij is in I and J since I and J are closed under multiplication by elements of R, due to being rings. Moreover, I and J are closed under addition, so the sums are also in both I and J. So all finite sums of products of the form ij with $i \in I$ and $j \in J$ are in $I \cap J$. Therefore $IJ \subseteq I \cap J$. ✓ □

Question 10c. Give an example where $IJ \neq I \cap J$.

Answer. Consider ideals of $\mathbb{Z}$. We know that for $x \in \mathbb{Z}$, (x) is an ideal. (x) contains all elements of $\mathbb{Z}$ that are multiples of x. I claim that $(x)(x) = (x^2)$. Let $a_i, b_i \in \mathbb{Z}$, such SP that xa_i and xb_i are in (x). Then

$$\sum xa_ixb_i = x^2\sum a_ib_i$$

Since a_i and b_i are arbitrary, a_ib_i can be any element of $\mathbb{Z}$, so $x^2\sum a_ib_i$ is an multiple of x^2, precisely an arbitrary element of (x^2). Therefore $(x)(x) = (x^2)$. But $(x^2) \subsetneq (x)$ since for $x \neq 1$, $x \notin (x^2)$. Therefore if we let $I = J = (x)$, then $IJ = (x)(x) = (x^2) \neq (x) = I \cap J$. ✓ or −1 ...

Question 10d. Prove that if R is commutative and if $I + J = R$ then $IJ = I \cap J$.

Proof. It is sufficient to show that $I \cap J \subset IJ$, the opposite inclusion is always case, as proven in part b. Let $x \in I \cap J$. Note that since $R = I + J$, there exists $i \in I$ and $j \in J$ such that $1 = i + j$.

$$\begin{aligned} x &= x1 \\ &= x(i+j) && \text{substitution} \\ &= xi + xj && \text{distributive property} \\ &= ix + xj \checkmark && \text{commutativity} \end{aligned}$$

And since $x \in I$ and $x \in J$, we know $ix \in IJ$ and $xj \in IJ$. And IJ is closed under addition, so $ix + xj \in IJ$, so $x \in IJ$. Therefore $I \cap J \subseteq IJ$. And we know the opposite inclusion from part b, so $IJ = I \cap J$. ✓ □

Problem 11 S

$I \wedge J \subseteq IJ$ ✓

R is a comm ring w/ 1. Prove (x) in $R[x]$ is a prime ideal iff R is an integral domain. Prove (x) is a maximal ideal iff R is a field.

We know that

✓

(x) is a prime ideal $\Longleftrightarrow$ $\frac{R[x]}{(x)}$ is an integral domain.

(x) is a maximal ideal $\Longleftrightarrow$ $\frac{R[x]}{(x)}$ is a field.

but, $\frac{R[x]}{(x)} \cong R$ b/c $(x) = xR[x]$. ✓