110A HW5

Warren Kim

Winter 2024

Question 1

Let R be a ring and $I \subseteq R$ be an ideal. Let $J \subseteq R$ be an ideal such that $I \subseteq J$, and let $\overline{J} \subseteq \overline{R} = R/I$ be an ideal.

1. Show that $\pi^{-1}(\pi(J)) = J$ and $\pi(\pi^{-1}(\overline{J})) = \overline{J}$. [Recall $\pi : R \to R/I$ is the canonical projection.]

2. Let $\overline{J} = \pi(J)$. Let $\pi : R \to R/I$ and $\phi : \overline{R} \to \overline{R}/\overline{J}$ be canonical projections. Show that $\ker(\phi \circ \pi) = J$.

Response

Proof: Let R be a ring and $I \subseteq R$ be an ideal. Let $J \subseteq R$ be an ideal such that $I \subseteq J$, and let $\overline{J} \subseteq \overline{R} = R/I$ be an ideal.

(1) $\boldsymbol{\pi^{-1}(\pi(J)) = J}$**:** Let $a \in \pi^{-1}(\pi(J))$. Then by definition of the pre-image under π, there exists $x \in J$ such that $\pi(a) = \pi(x) \in \pi(J)$, or $a + I = x + I$, which implies that $a - x \in I \subseteq J$, so $a \in J$. Since a was arbitrary, $\pi^{-1}(\pi(J)) \subseteq J$. Now let $b \in J$. Then by definition, $\pi(b) = b + I$. Then, $\pi^{-1}(\pi(b)) = \pi^{-1}(b + I)$ but by definition of the pre-image, $\pi^{-1}(b + I) = b \in \pi^{-1}(\pi(J))$. Since b was arbitrary, $J \subseteq \pi^{-1}(\pi(J))$. Since we have $\pi^{-1}(\pi(J)) \subseteq J$ and $\pi^{-1}(\pi(J)) \supseteq J$, $\pi^{-1}(\pi(J)) = J$.

$\boldsymbol{\pi(\pi^{-1}(\overline{J})) = \overline{J}}$**:** Let $a + I \in \pi(\pi^{-1}(\overline{J}))$. Then there exists $x \in R$ such that $x \in \pi^{-1}(\overline{J})$ and $\pi(x) = a + I \in \overline{J}$. Since a was arbitrary, $\pi(\pi^{-1}(\overline{J})) \subseteq \overline{J}$. Now let $b + I \in \overline{J}$. Then by definition, $b + I$ is in the image of J under π, so $b \in \pi^{-1}(\overline{J})$. Then $\pi(\pi^{-1}(b + I)) = \pi(b) = b + I \in \pi(\pi^{-1}(\overline{J}))$. Since $b + I$ was arbitrary, $\overline{J} \subseteq \pi(\pi^{-1}(\overline{J}))$. Since $\pi(\pi^{-1}(\overline{J})) \subseteq \overline{J}$ and $\pi(\pi^{-1}(\overline{J})) \supseteq \overline{J}$, $\pi(\pi^{-1}(\overline{J})) = \overline{J}$.

(2) Let $\overline{J} = \pi(J)$. Let $\pi : R \to R/I$ and $\phi : \overline{R} \to \overline{R}/\overline{J}$ be canonical projections. Take $a \in J$. Then $\phi \circ \pi(a) = \phi(\pi(a)) = \phi(a + I) = (a + I) + \overline{J}$, but since $a + I \in \overline{J}$, we have that $(a + I) + \overline{J} = 0 + \overline{J} \in \ker(\phi \circ \pi)$. Since a was arbitrary, $J \subseteq \ker(\phi \circ \pi)$. Now take any $b \in R$ such that $\phi \circ \pi(b) = 0 + \overline{J}$. Then, $(b + I) + \overline{J} = 0 + \overline{J}$. Then by definition, $b + I \in \overline{J} = \pi(J)$ by assumption. Then $b + I$ is the image of J under π, so $b \in \pi^{-1}(\overline{J}) = \pi^{-1}(\pi(J)) = J$. Since b was arbitrary, $\ker(\phi \circ \pi) \subseteq J$. Since $J \subseteq \ker(\phi \circ \pi)$ and $J \supseteq \ker(\phi \circ \pi)$, $J = \ker(\phi \circ \pi)$. $\square$

Question 2

Let $m, n \in \mathbb{Z}$ be nonzero. Show that $(m, n) = 1$ if and only if $\mathbb{Z}/mn \cong \mathbb{Z}/m \times \mathbb{Z}/n$.

Response

Proof: $(\implies)$ Let $m, n \in \mathbb{Z}$ be nonzero such that $\gcd(m, n) = 1$. Then we can represent $mx + ny = 1$ for some $x, y \in \mathbb{Z}$. Pick $R = \mathbb{Z}$, $I = (m)$, and $J = (n)$. Then we can write $(m)x + (n)y = (1) = \mathbb{Z}$ for some $x, y \in \mathbb{Z}$. So, $I + J = R$, and by the Chinese Remainder Theorem for isomorphisms, we have $R/(I \cap J) \simeq (R/I) \times (R/J)$. But since $I + J = R$, we have $I \cap J = IJ$, so $R/IJ \simeq (R/I) \times (R/J)$. Substituting I, J, R, we get $\mathbb{Z}/mn \simeq \mathbb{Z}/m \times \mathbb{Z}/n$.

$(\impliedby)$ Let $\mathbb{Z}/mn \simeq \mathbb{Z}/m \times \mathbb{Z}/n$. Suppose for the sake of contradiction that $d = \gcd(m, n) > 1$. Since $\mathbb{Z}/mn \simeq \mathbb{Z}/m \times \mathbb{Z}/n$, there exists a bijection $f : \mathbb{Z}/mn \to \mathbb{Z}/m \times \mathbb{Z}/n$. Recall $([m]_m, [n]_n) = ([0]_m, [0]_n) \in \mathbb{Z}/m \times \mathbb{Z}/n$. Then since f is bijective, there exists $x \in \mathbb{Z}/mn$ such that $f([x]_{mn}) = ([0]_m, [0]_n)$. Put $x := d \cdot \min\{m, n\}$. Without loss of generality, assume $n < m$. Then $f([x]_{mn}) = f([dn]_{mn}) = ([dn]_m, [dn]_n) = ([0]_m, [0]_n)$ since $d \mid m$ and $d \mid n$ by definition. Because $d < m$, $[dn]_{mn} = [x]_{mn} \neq [0]_{mn}$. Since $\ker(f) \neq \{0\}$, f is not injective and therefore not bijective, a contradiction.

Since we showed $(\implies)$ and $(\impliedby)$, $(m, n) = 1$ if and only if $\mathbb{Z}/mn \simeq \mathbb{Z}/m \times \mathbb{Z}/n$. $\square$

Question 3

Let R be a (commutative) ring and $I_1, I_2, I_3 \subseteq R$ be ideals such that $I_1 + I_3 = R$ and $I_2 + I_3 = R$. Show that $(I_1 \cap I_2) + I_3 = R$.

Response

Proof: Let R be a commutative ring ant $I_1, I_2, I_3 \subseteq R$ be ideals such that $I_1 + I_3 = R$ and $I_2 + I_3 = R$. $\boldsymbol{(I_1 \cap I_2) + I_3 \subseteq R}$**:** Take $a \in (I_1 \cap I_2) + I_3$. Then since $I_1 + I_3 = R$ and $I_2 + I_3 = R$, $a \in R$ since $a \in I_1 + I_3 = R$ and $a \in I_2 + I_3 = R$.

$\boldsymbol{R \subseteq (I_1 \cap I_2) + I_3}$**:** Pick any $x \in R$. Since $I_1 + I_3 = R$ and $I_2 + I_3 = R$, there exist $a \in I_1$, $b \in I_2$, $c, d \in I_3$ such that $a + c = 1$ and $b + d = 1$. Then

$$\begin{aligned} 1 &= (a+c)(b+d) \\ &= ab + ad + cb + cd \\ 1 &= ab + ((ad + cb) + cd) \end{aligned}$$

Then $ab \in I_1 \cap I_2$ because $a \in I_1$, we have $ab \in I_1$, and similarly, $b \in I_2$. Also, $(ad + cb) + cd \in I_3$ since $cd \in I_3$, so $ab + ((ad + cb) + cd \in (I_1 \cap I_2) + I_3$. Then multiplying by x on both sides, we get $x(ab) + x((ad + cb) + cd) = x \in (I_1 \cap I_2) + I_3$.

Since $(I_1 \cap I_2) + I_3 \subseteq R$ and $(I_1 \cap I_2) + I_3 \supseteq R$, $(I_1 \cap I_2) + I_3 = R$. $\square$

Question 4

Let R be a (commutative) ring and let $I_1, I_2, I_3 \subseteq R$ be ideals. Suppose that $I_i + I_j = R$ for $i \neq j$. Let a_1, a_2, a_3 be any ideals. Show that there is some $x \in R$ such that

$$\begin{aligned} x &\equiv a_1 \mod I_1 \\ x &\equiv a_2 \mod I_2 \\ x &\equiv a_3 \mod I_3 \,. \end{aligned}$$

Response

Proof: Let R be a commutative ring and let $I_1, I_2, I_3 \subseteq R$ be ideals where $I_i + I_j = R$ for $i \neq j$. Let $a_1, a_2, a_3 \in R$. Then $I_1 + I_2 = R$, $I_1 + I_3 = R$, and $I_2 + I_3 = R$, so

$$\begin{aligned} (I_2 \cap I_3) + I_1 = R \\ (I_1 \cap I_3) + I_2 = R \\ (I_1 \cap I_2) + I_3 = R \end{aligned}$$

from (**Question 3**). Then there exist

$$\begin{aligned} p \in I_1, q \in I_2 \cap I_3 \text{ such that } p + q = 1_R \\ r \in I_2, s \in I_1 \cap I_3 \text{ such that } r + s = 1_R \\ u \in I_3, v \in I_1 \cap I_2 \text{ such that } u + v = 1_R \end{aligned}$$

Define $x := a_1(qu) + a_2(ps) + a_3(rv)$. Then

$$\begin{aligned} x = a_1(qu) + a_2(ps) + a_3(rv) &\equiv a_1(qu) \pmod{I_1} && ps \in I_1, rv \in I_1 \cap I_3 \subseteq I_1 \\ x = a_1(qu) + a_2(ps) + a_3(rv) &\equiv a_2(ps) \pmod{I_2} && rv \in I_2, qu \in I_2 \cap I_3 \subseteq I_2 \\ x = a_1(qu) + a_2(ps) + a_3(rv) &\equiv a_3(rv) \pmod{I_3} && qu \in I_3, ps \in I_1 \cap I_3 \subseteq I_3 \end{aligned}$$

Here, $q \equiv 1 \pmod{I_1}$ since $p \equiv 0 \pmod{I_1}$. Similarly, $u \equiv 1 \pmod{I_1}$ since $v \equiv \pmod{I_1}$. So, $qu \equiv 1 \pmod{I_1}$. A simliar argument can be made for ps and rv. Then we get

$$\begin{aligned} x &\equiv a_1 \pmod{I_1} \\ x &\equiv a_2 \pmod{I_2} \\ x &\equiv a_3 \pmod{I_3} \end{aligned}$$

$\square$