110A HW4

Warren Kim

Winter 2024

Question 1

Let F be a field, and consider the polynomial ring $F[x, y]$ with two variables. Show that $I = (x, y)$ is not a principal ideal (i.e., it cannot be generated by a single element).

Response

Proof: Suppose for the sake of contradiction that $I = (x, y)$ is a principal ideal. Then, there exists a polynomial $z(x, y) \in F[x, y]$ such that $I = (z(x, y))$. By definition, there exist polynomials $a(x, y), b(x, y) \in F[x, y]$ such that $x = a(x, y)z(x, y), y = b(x, y)z(x, y)$. Since x and y are independent of each other, their only common divisors are constants. This implies that either $z(x, y)$ is a constant polynomial or $z(x, y)$ is not a common divisor for x, y. If $z(x, y)$ is a constant, it cannot generate non-constant polynomials. That is, it cannot generate (x, y). If $z(x, y)$ is not a common divisor for x and y, it cannot be a generator by definition. In either case, we have a contradiction. Therefore, (x, y) is not a principal ideal. $\square$

Question 2

Let R be a ring, and let $I_1, \cdots, I_k$ be ideals. Show that the following sets are ideals:

1. $I_1 + \cdots + I_k = \{i_1 + \cdots + i_k | i_j \in I_j\}$
2. $I_1 \cap I_2 \cap \cdots \cap I_k$

Response

1. $I_1 + \cdots + I_k = \{i_1 + \cdots + i_k | i_j \in I_j\}$ is an ideal.

   Proof: Let R be a ring, and $I_1, \cdots, I_k$ be ideals.

   (a) $0 \in I_1 + \cdots + I_k$. Since I_j is an ideal, $0 \in I_j$ so we get $0 + \cdots 0 = 0 \in I_1 + \cdots + I_k$.

   (b) Closure under addition. Take two elements $a, b \in I_1 + \cdots + I_k$. We can rewrite a, b as, $a = p_1 + \cdots + p_k$ and $b = q_1 + \cdots + q_k$ for $p_j, q_j \in I_j$. Then $a + b = (p_1 + \cdots + p_k) + (q_1 + \cdots + q_k) = (p_1 + q_1) + \cdots + (p_k + q_k)$, and since $p_j + q_j \in I_j$ for all $j \leq k$, we get $a + b \in I_1 + \cdots + I_k$, so $I_1 + \cdots + I_k$ is closed under addition.

   (c) $-a \in I_1 + \cdots + I_k$. Let $a := a_1 + \cdots + a_k \in I_1 + \cdots + I_k$. Since I_j is an ideal, there exists $-a \in I_j$, so we get $-a_1 + \cdots + -a_k = -(a_1 + \cdots + a_k) = -a \in I_1 + \cdots + I_k$.

   (d) Absorbing property. Take any $a \in I_1 + \cdots + I_k$. We can rewrite a as, $a = p_1 + \cdots + p_k$ for $p_j \in I_j$. Consider an element $r \in R$. Then, $ar = (p_1 + \cdots + p_k)r = p_1 r + \cdots + p_k r$. Similarly, $ar = r(p_1 + \cdots + p_k) = rp_1 + \cdots + rp_k$. Since I_j is an ideal, $p_j r, rp_j \in I_j$, so $ar \in I_1 + \cdots + I_k$. Therefore, $I_1 + \cdots + I_k$ satisfies the absorbing property.

   Because $I_1 + \cdots + I_k$ satisfies (a) - (d), $I_1 + \cdots + I_k$ is an ideal. $\square$

2. $I_1 \cap \cdots \cap I_k$ is an ideal.

   Proof: Let R be a ring, and $I_1, \cdots, I_k$ be ideals.

   (a) $0 \in I_1 \cap \cdots \cap I_k$. Since I_j is an ideal, $0 \in I_j$, so $0 \in I_1 \cap \cdots \cap I_k$.

   (b) Closure under addition. Take two elements $a, b \in I_1 \cap \cdots \cap I_k$. Then since each I_j is an ideal, they are closed under addition. So, $a + b \in I_1 \cap \cdots \cap I_k$ because $a + b \in I_j$. Therefore, $I_1 \cap \cdots \cap I_k$ is closed under addition.

   (c) $-a \in I_1 \cap \cdots \cap I_k$. Take any $a \in I_1 \cap \cdots \cap I_k$. Then, since I_j is an ideal, $-a \in I_j$, so $-a \in I_1 \cap \cdots \cap I_k$.

   (d) Absorbing property. Take any $a \in I_1 + \cdots + I_k$. Consider an element $r \in R$. Then, since each I_j is an ideal, they satisfy the absorbing property. Therefore, $ar, ra \in I_1 \cap \cdots \cap I_k$ because $ar, ra \in I_j$. Therefore, $I_1 \cap \cdots \cap I_k$ satisfies the absorbing property.

   Because $I_1 \cap \cdots \cap I_k$ satisfies (a) - (d), $I_1 \cap \cdots \cap I_k$ is an ideal. $\square$

Question 3

Let R be a ring, $a \in R$, and $I \subseteq R$ be an ideal. Show that the set $a + I = \{a + x | x \in I\}$ is precisely the congruence class modulo I that contains a. That is, show that $b \equiv a \mod I$ if and only if $b \in a + I$.

Response

Proof: Let R be a ring, $a \in R$, and $I \subseteq R$ be an ideal. Consider the set $a + I = \{a + x \mid x \in I\}$.
($\implies$) Suppose $b \equiv a \pmod{I}$ for some $b \in R$. By definition, $b - a \in I$. Then there exists some $i \in I$ such that $b - a = i$. Therefore, $b = a + i$ for some $i \in I$, so $b \in a + I$.
($\impliedby$) Suppose $b \in a + I$. By definition, there exists some $i \in I$ such that $b = a + i$. Subtracting a from both sides, we get $b - a = i$, which is in I, so $b \equiv a \pmod{I}$. Because both implications were proved, we have that $b \equiv a \mod I$ if and only if $b \in a + I$. $\square$

Question 4

Let $f : R \to S$ be a ring homomorphism, and suppose $I \subseteq R$ is an ideal such that $I \subseteq \ker(f)$. Show that there is a unique homomorphism $\overline{f} : R/I \to S$ such that $f = \overline{f} \circ \pi$.

Response

Proof: Let $f : R \to S$ be a ring homomorphism, and $I \subseteq R$ an ideal such that $I \subseteq \ker(f)$. Consider $\overline{f} : R/I \to S, a + I \mapsto f(a)$. To show that $\overline{f}$ is a homomorphism:

1. Closed under addition. Let $a + I, b + I \in R/I$. Then

$$\begin{aligned}\overline{f}((a+I)+(b+I)) &= \overline{f}((a+b)+I) \\ &= f(a+b) \\ &= f(a)+f(b) \\ \overline{f}((a+I)+(b+I)) &= \overline{f}(a+I)+\overline{f}(b+I)\end{aligned}$$

   so $\overline{f}$ is closed under addition.

2. Closed under multiplication. Let $a + I, b + I \in R/I$. Then

$$\begin{aligned}\overline{f}((a+I)\cdot(b+I)) &= \overline{f}((a\cdot b)+I) \\ &= f(a\cdot b) \\ &= f(a)\cdot f(b) \\ \overline{f}((a+I)\cdot(b+I)) &= \overline{f}(a+I)\cdot\overline{f}(b+I)\end{aligned}$$

   so $\overline{f}$ is closed under multiplication.

3. Preservation of the multiplicative identity. Let $1_{R/I} := 1 + I \in R/I$. Then

$$\overline{f}(1_{R/I}) = \overline{f}(1+I) = f(1) = 1_S$$

   so $\overline{f}$ preserves the multiplicative identity.

So $\overline{f}$ is a ring homomorphism. To show that $f = \overline{f} \circ \pi$, consider $a \in R$. Then

$$\overline{f} \circ \pi(a) = \overline{f}(\pi(a)) = \overline{f}(a+I) = f(a)$$

so $f = \overline{f} \circ \pi$. To show that $\overline{f}$ is unique, suppose we have another homomorphism $g : R/I \to S$ such that $f \neq g$. Then

$$g \circ \pi(a) = g(\pi(a)) = g(a+I) \neq f(a) = \overline{f}(a+I) = \overline{f}(\pi(a)) = \overline{f} \circ \pi(a)$$

so $\overline{f}$ is unique. $\square$

Question 5

Let $a \in \mathbb{R}$ be any real number. Show that the quotient ring $\mathbb{R}[x]/(x-a)$ is isomorphic to $\mathbb{R}$. [hint: you can use, without proof, that a polynomial $p(x)$ has a root a if and only if it can be written $p(x) = (x-a)q(x)$, where $q(x)$ is another polynomial.]

Response

Proof: Let $a \in \mathbb{R}$ and $\mathbb{R}[x]/(x-a)$ be a quotient ring. Consider $f : \mathbb{R}[x] \to \mathbb{R}$ where $p(x) \mapsto p(a)$. To show that f is a homomorphism:

1. Closed under addition. Let $p(x), q(x) \in \mathbb{R}[x]$. Then

   $$f(p(x) + q(x)) = p(a) + q(a) = f(p(x)) + f(q(x))$$

   so f is closed under addition.

2. Closed under multiplication. Let $p(x), q(x) \in \mathbb{R}[x]$. Then

   $$f(p(x) \cdot q(x)) = p(a) \cdot q(a) = f(p(x)) \cdot f(q(x))$$

   so f is closed under multiplication.

3. Preservation of the multiplicative identity. Let $1_{\mathbb{R}[x]} \in \mathbb{R}[x]$. Then

   $$f(1_{\mathbb{R}[x]}) = 1(a) = 1_{\mathbb{R}}$$

   so f preserves the multiplicative identity.

So f is a ring homomorphism. Take an arbitrary $b \in \mathbb{R}$. Then there is some $p(x) \in \mathbb{R}[x]$ such that $f(p(x)) = b$, so f is surjective. Pick $p(x) \in \ker(f)$. Then $f(p(x)) = p(a) = 0$ is only true when $p(x) = (x-a)q(x)$ where $q(x)$ is another polynomial. So, $\ker(f)$ is generated by the ideal $(x-a)$. By the First Isomorphism Theorem (proven in class), since $f : \mathbb{R}[x] \to S$, we have that $\mathbb{R}[x]/\ker(f) \simeq \mathrm{Im}(f)$. From above, we have that $\ker(f) = (x-a)$ and $\mathrm{Im}(f) = \mathbb{R}$, so $\mathbb{R}[x]/(x-a) \simeq \mathbb{R}$. $\square$

Question 6

Let R be a commutative ring, and let $I, J \subseteq R$ be ideals. Consider

$$IJ = \{i_1j_1 + \cdots + i_nj_n | i_r \in I, j_s \in J, n > 0\}.$$

1. Show that IJ is an ideal.
2. Show that $IJ \subseteq I \cap J$.
3. Show that if $I + J = R$, then $IJ = I \cap J$.

Response

1. IJ is an ideal.

   Proof: Let R be a ring, and $I, J \subseteq R$ be ideals. Then, to show that

   $$IJ = \{i_1j_1 + \cdots + i_nj_n \mid i_r \in I, j_s \in J, n > 0\}$$

   is an ideal:

   (a) $0 \in IJ$. Since I, J are ideals, so $0 \in I, J$, so $0 \cdot 0 = 0 \in IJ$.

   (b) Closure under addition. Take two elements $a, b \in IJ$. We can rewrite a, b as, $a = p_1q_1 + \cdots + p_nq_n$ and $b = u_1v_1 + \cdots + u_nv_n$ for $p_r, u_r \in I, q_s, v_s \in J$. Then

   $$a + b = (p_1q_1 + \cdots + p_nq_n) + (u_1v_1 + \cdots + u_nv_n)$$

   which is a finite sum that can be rewritten in the form $i_1j_1 + \cdots + i_nj_n$ for $i_r \in I, j_s \in J$. Then by definition, $a + b \in IJ$, so IJ is closed under addition.

   (c) $-a \in IJ$. Take $a := i_1j_1 + \cdots + i_nj_n \in IJ$. Since I, J are ideals, we have $-i_k \in I, -j_k \in J$ for $i_k \in I, j_k \in J$, so $-i_1j_1 + \cdots + -i_nj_n = -(i_1j_1 + \cdots + i_nj_n) = -a \in IJ$.

   (d) Absorbing property. Take any $a \in IJ$. We can rewrite a as, $a = i_1j_1 + \cdots + i_nj_n$ for $i_t \in I, j_s \in J$. Consider an element $t \in R$. Then, $at = (i_1j_1 + \cdots + i_nj_n)t = i_1j_1t + \cdots + i_nj_nt$. Similarly, $at = t(i_1j_1 + \cdots + i_nj_n) = ti_1j_1 + \cdots + ti_nj_n$. Since $I, J \subseteq R$ are ideals, $i_rt, ti_r \in I, j_s \in J$, so $ti_rj_s \in IJ$. Similarly, $i_r \in I, j_st, tj_s \in J$, so $i_rj_st \in IJ$. So IJ satisfies the absorbing property.

   Because IJ satisfies (a) - (d), IJ is an ideal. □

2. $IJ \subseteq I \cap J$.

   Proof: Let R be a ring, and $I, J \subseteq R$ be ideals. Then, from (1), IJ is an ideal in R. Suppose we have an arbitrary element $i_1j_1 + \cdots + i_nj_n \in IJ$. Since $I, J \subseteq R$ are ideals, $i_rj_s \in I$ and $i_rj_s \in J$. That is, $i_rj_s \in I \cap J$. Since $I, J \subseteq R$ are ideals, they are both closed under addition. So, $i_1j_1 + \cdots + i_nj_n \in I \cap J$. Since $i_1j_1 + \cdots + i_nj_n$ was arbitrary, $IJ \subseteq I \cap J$. □

3. If $I + J = R$, then $IJ = I \cap J$.

   Proof: Suppose $I + J = R$. Then $1_I + 1_J = 1_R$. Pick any $a \in I \cap J$. Then, $a = a \cdot 1_R = a \cdot (1_I + 1_J) = a \cdot 1_I + a \cdot 1_J$. Then, $a \cdot 1_I \in I$ because $a, 1_I \in I$. Similarly, $a \cdot 1_J \in J$ because $a, 1_J \in J$. So, $a \cdot 1_I + a \cdot 1_J \in I \cap J$ since $I \cap J$ is an ideal (**Question 2**). Because $a \cdot 1_I + a \cdot 1_J \in I \cap J$ was arbitrary, $I \cap J \subseteq IJ$. From (2), $IJ \subseteq I \cap J$. It follows that $IJ = I \cap J$. □

Question 7

Let R be a commutative ring. Recall that $r \in R$ is nilpotent if there is some $n > 0$ such that $r^n = 0$.

1. Let $Nil(R)$ be the set of nilpotent elements of R. Show that $Nil(R)$ forms an ideal.
2. Show that $R/Nil(R)$ has no nonzero nilpotent elements.

Response

1. Let $Nil(R)$ be the set of nilpotent elements of R. Show that $Nil(R)$ forms an ideal.

   Proof: Let R be a commutative ring.

   (a) $0 \in Nil(R)$. Since R is a ring, $0 \in R$, so $0^n = 0 \in Nil(R)$ for any $n > 0$.

   (b) Closure under addition. Take $a, b \in Nil(R)$. Then, there exist some $n, m > 0$ such that $a^n = b^m = 0$. Consider $(a+b)^p$ where $p = n + m$. Then we have

   $$(a+b)^p = \sum_{k=0}^{p} \binom{p}{k} a^{p-k} b^k$$

   Then, if $k \geq m$, then $b^k = 0$. If $p - k \geq n$, then $a^{p-k} = 0$. Therefore, every term of the expansion $(a+b)^p = 0 \in Nil(R)$, so $a + b \in Nil(R)$.

   (c) $-a \in Nil(R)$. Take $a \in Nil(R)$. Then, there exists some $n > 0$ such that $a^n = 0$. Since R is a ring, there exists $-a \in R$. Consider $(-a)^k$ where $k = n$. Then, $(-a)^k = (-a)^n = (-1)^n a^n = (-1)^n \cdot 0 = 0 \in Nil(R)$.

   (d) Absorbing property. Take $a \in Nil(R)$. Then, there exists some $n > 0$ such that $a^n = 0$. Pick any $r \in R$. Consider $(ar)^k$ where $k = n$. Then, $(ar)^k = (ar)^n = a^n r^n = 0 \cdot r^n = 0 \in Nil(R)$. Similarly, $(ra)^k = (ra)^n = r^n a^n = r^n \cdot 0 \in Nil(R)$.

   Since $Nil(R)$ satisfies (a) - (d), $Nil(R)$ is an ideal. $\square$

2. Show that $R/Nil(R)$ has no nonzero nilpotent elements.

   Proof: Suppose $a + Nil(R) \in R/Nil(R)$ is nilpotent. Then, there exists some $n > 0$ such that $(a + Nil(R))^n = 0 + Nil(R)$. Then, we have

   $$(a + Nil(R))^n = \sum_{k=0}^{n} \binom{n}{k} a^{n-k} Nil(R)^k$$

   Since $Nil(R)$ is an ideal, every term in the expansion that is multiplied by $Nil(R)$ is absorbed. Then, we are left with $a^n + Nil(R) = 0 + Nil(R)$, which implies that $a^n \in Nil(R)$. Then, there exists some $m > 0$ such that $(a^n)^m = 0$. But $(a^n)^m = a^n m = 0$, so it must be true that $a \in Nil(R)$ is nilpotent. Then, we get that $a + Nil(R) = 0 + Nil(R)$. Since $a + Nil(R)$ was arbitrary, this holds for all $a + Nil(R) \in R/Nil(R)$. $\square$