

Solutions to Homework 8

1. Show that the ideals (y) and $(x, y) \subset \mathbb{Q}[x, y]$ is prime.

Solution: First, let $\varphi: \mathbb{Q}[x, y] \rightarrow \mathbb{Q}[x]$ be the homomorphism given by plugging in $y = 0$:

$$\varphi \left(\sum_{i,j} a_{ij} x^i y^j \right) = \sum_i a_{i0} x^i.$$

Clearly this is surjective, and $\varphi(y) = 0$, so $(y) \subset \ker \varphi$. For the reverse inclusion, if $\varphi(f) = 0$ for some $f = \sum a_{ij} x^i y^j$, then $a_{i0} = 0$ for all i , so we can write $f = yg$ where

$$g = \sum_{i \geq 0, j \geq 1} a_{ij} x^i y^{j-1}.$$

Thus $\mathbb{Q}[x, y]/(y) \cong \mathbb{Q}[x]$, which is an integral domain, so (y) is prime.

Next, let $\psi: \mathbb{Q}[x, y] \rightarrow \mathbb{Q}$ be the homomorphism given by plugging in $x = 0$ and $y = 0$:

$$\psi \left(\sum_{i,j} a_{ij} x^i y^j \right) = a_{00}.$$

Clearly this is surjective, and $\psi(x) = \psi(y) = 0$, so $(x, y) \subset \ker \psi$. For the reverse inclusion, if $\psi(f) = 0$ for some $f = \sum a_{ij} x^i y^j$, then $a_{00} = 0$, so we can write $f = xg + yh$ where

$$g = \sum_{i \geq 1, j \geq 0} a_{ij} x^{i-1} y^j$$

and

$$h = \sum_{j \geq 1} a_{0j} y^{j-1}.$$

Thus $\mathbb{Q}[x, y]/(x, y) \cong \mathbb{Q}$, which is an integral domain, so (x, y) is prime.

2. Let R be the ring of continuous functions on \mathbb{R} . Show that the ideal $I = \{f \in R : f(t) = 0 \text{ for all } t \in [0, 1]\}$ is not prime.

Solution: Let f be a function with $f(0) \neq 0$ and $f(t) = 0$ for $t \geq \frac{1}{2}$, and let g be a function with $g(1) \neq 0$ and $g(t) = 0$ for $t \leq \frac{1}{2}$. For example, we could take

$$f(t) = \max\{0, \frac{1}{2} - t\} \quad g(t) = \max\{0, t - \frac{1}{2}\}.$$



Then $fg = 0 \in I$, but $f \notin I$ and $g \notin I$.

3. Let $R = \mathbb{Z}[\sqrt{-3}]$, and consider the elements $\sqrt{-3}$, $1 + \sqrt{-3}$, and $2 + \sqrt{-3}$ in R . In each case, show that $R/r \cong \mathbb{Z}/k$ for some integer k . Deduce that two of these elements are prime and the other is not.

Solution:

- $\sqrt{-3}$ is prime. Observe that the isomorphism

$$\mathbb{Z}[\sqrt{-3}] \cong \mathbb{Z}[x]/(x^2 + 3)$$

takes $\sqrt{-3}$ to \bar{x} . Thus

$$R/\sqrt{-3} \cong \mathbb{Z}[x]/(x^2 + 3, x) \cong \mathbb{Z}[x]/(3, x) \cong \mathbb{Z}/3,$$

which is an integral domain. To justify the claim $(x^2 + 3, x) = (3, x)$, note that $x^2 + 3 \in (3, x)$ and $x \in (3, x)$, so $(x^2 + 3, x) \in (3, x)$, and similarly both the generators of $(3, x)$ are in $(x^2 + 3, x)$, so $(3, x) \subset (x^2 + 3, x)$.

Alternatively, consider the surjective homomorphism $\varphi: R \rightarrow \mathbb{Z}/3$ given by $\varphi(a + b\sqrt{-3}) = a \pmod{3}$. Then $\varphi(\sqrt{-3}) = 0$, so $(\sqrt{-3}) \subset \ker \varphi$. For the reverse inclusion, suppose that $\varphi(a + b\sqrt{-3}) = 0$; then $a \equiv 0 \pmod{3}$, so we can write $a = 3c$ for some $c \in \mathbb{Z}$. Then

$$a + b\sqrt{-3} = 3c + b\sqrt{-3} = (b - c\sqrt{-3}) \cdot \sqrt{-3}.$$

Now the first isomorphism theorem gives $R/\sqrt{-3} \cong \mathbb{Z}/3$.

- $1 + \sqrt{-3}$ is not prime. We have

$$R/(1 + \sqrt{-3}) \cong \mathbb{Z}[x]/(x^2 + 3, x + 1) \cong \mathbb{Z}[x]/(4, x + 1) \cong \mathbb{Z}/4,$$

which is not an integral domain. To see that $(x^2 + 3, x + 1) = (4, x + 1)$, note that $x^2 + 3 = (x - 1)(x + 1) + 4 \in (4, x + 1)$ and $4 = (x^2 + 3) - (x - 1)(x + 1) \in (x^2 + 3, x + 1)$. Also we have used the fact that $\mathbb{Z}[x]/(x + 1) \cong \mathbb{Z}$, which we saw in lecture.

Alternatively, consider the surjective map $\varphi: R \rightarrow \mathbb{Z}/4$ given by $\varphi(a + b\sqrt{-3}) = a - b \pmod{4}$. This is a homomorphism because $(-1)^2 \equiv -3 \pmod{4}$. We have $\varphi(1 + \sqrt{-3}) = 0$, so $(1 + \sqrt{-3}) \subset \ker \varphi$. For the reverse inclusion, suppose that $\varphi(a + b\sqrt{-3}) = 0$, so we can write $a - b = 4c$ for some $c \in \mathbb{Z}$. Then $(b + c - c\sqrt{-3})(1 + \sqrt{-3}) = (b + 4c) + b\sqrt{-3} = a + b\sqrt{-3}$, so $a + b\sqrt{-3} \in (1 + \sqrt{-3})$.

- $2 + \sqrt{-3}$ is prime. We have

$$R/(2 + \sqrt{-3}) \cong \mathbb{Z}[x]/(x^2 + 3, x + 2) \cong \mathbb{Z}[x]/(7, x + 2) \cong \mathbb{Z}/7,$$

which is an integral domain. To see that $(x^2 + 3, x + 2) = (7, x + 2)$, note that $x^2 + 3 = (x - 2)(x + 2) + 7$.

Alternatively, consider the surjective map $\varphi: R \rightarrow \mathbb{Z}/7$ given by $\varphi(a + b\sqrt{-3}) = a - 2b \pmod{7}$. This is a homomorphism because $(-2)^2 \equiv -3 \pmod{7}$. We have $\varphi(2 + \sqrt{-3}) = 0$, so $(2 + \sqrt{-3}) \subset \ker \varphi$. For the reverse inclusion, suppose that $\varphi(a + b\sqrt{-3}) = 0$, so we can write $a - 2b = 7c$ for some $c \in \mathbb{Z}$. Then $(b + 2c - c\sqrt{-3})(2 + \sqrt{-3}) = (2b + 7c) + b\sqrt{-3} = a + b\sqrt{-3}$, so $a + b\sqrt{-3} \in (2 + \sqrt{-3})$.

4. Let R be a commutative ring, let $I, J \subset R$ be ideals, and let $P \subset R$ be a prime ideal. Show that if $IJ \subset P$ then $I \subset P$ or $J \subset P$.

Solution: Observe that the following is equivalent to the definition of a prime ideal: for all $a, b \in R$, if $ab \in P$ and $a \notin P$, then $b \in P$. Similarly, the statement of the problem is equivalent to saying that for all ideals $I, J \subset R$, if $IJ \subset P$ and $I \not\subset P$ then $J \subset P$.

Suppose that $IJ \subset P$ and $I \not\subset P$. Then we can choose an $i \in I$ with $i \notin P$. Now for all $j \in J$ we have $ij \in IJ \subset P$, and $i \notin P$, so $j \in P$. Thus $J \subset P$.

5. Let $\varphi: R \rightarrow S$ be a surjective homomorphism of commutative rings, let $P \subset S$ be a prime ideal, and let

$$I = \varphi^{-1}(P) = \{r \in R : \varphi(r) \in P\}.$$

Show that I is a prime ideal.

Solution: For completeness, let us first argue that I is an ideal. If $i_1, i_2 \in I$ then $\varphi(i_1), \varphi(i_2) \in P$, so $\varphi(i_1) + \varphi(i_2) \in P$ because P is an ideal, so $\varphi(i_1 + i_2) \in P$ because φ is a homomorphism, so $i_1 + i_2 \in I$. Similarly, if $i \in I$ and $r \in R$ then $\varphi(i) \in P$, so $\varphi(ri) = \varphi(r)\varphi(i) \in P$, so $ri \in I$.

Next we argue that I is prime. Let $r_1, r_2 \in R$, and suppose that $r_1 r_2 \in I$. Then $\varphi(r_1)\varphi(r_2) = \varphi(r_1 r_2) \in P$, so $\varphi(r_1) \in P$ or $\varphi(r_2) \in P$ because P is prime, so $r_1 \in I$ or $r_2 \in I$.

6. In lecture, after giving a somewhat informal proof that every PID is a UFD, we said that a more formal proof should be broken into the following steps. Write good, clean proofs of two of these statements.

- (a) Let $I_1 \subseteq I_2 \subseteq I_3 \subseteq \dots$ be a chain of ideals. Then

$$I = I_1 \cup I_2 \cup I_3 \cup \dots$$

is an ideal.

Proof: First let $a, b \in I$. Then $a \in I_k$ for some k , and $b \in I_l$ for some l . If $k \leq l$ then $I_k \subset I_l$, so $a \in I_l$, so $a + b \in I_l$ because I_l is an ideal, so $a + b \in I$. Similarly, if $l \leq k$ then $I_l \subset I_k$, so $a + b \in I_k \subset I$.

Next let $a \in I$ and $r \in R$. Then $a \in I_k$ for some k , so $ra \in I_k$ and $ar \in I_k$ because I_k is an ideal, so $ar, ra \in I$.

- (b) Let R be a ring in which every ideal is finitely generated: that is, for every ideal $I \subset R$ there are $a_1, \dots, a_n \in R$ such that $I = (a_1, \dots, a_n)$. Then there is no infinite increasing chain of ideals $I_1 \subsetneq I_2 \subsetneq I_3 \subsetneq \dots$. Equivalently, any chain $I_1 \subseteq I_2 \subseteq I_3 \subseteq \dots$ eventually stabilizes: that is, there is a k such that $I_k = I_{k+1} = I_{k+2} = \dots$. (The converse is also true. Such a ring is called *Noetherian*.)

Proof: We prove the second statement, that every chain eventually stabilizes.

Let $I = I_1 \cup I_2 \cup I_3 \cup \dots$. By part (a), I is an ideal, so write $I = (a_1, \dots, a_n)$ with $a_1, \dots, a_n \in R$. For each a_i we have $a_i \in I_{k_i}$

for some k_i . Let $k = \max\{k_1, \dots, k_n\}$. Then for every i we have $I_{k_i} \subset I_k$, so $a_i \in I_k$. Thus $(a_1, \dots, a_n) \subset I_k$. Thus $I \subset I_k \subset I_{k+1} \subset I_{k+2} \subset \dots \subset I$, so $I_k = I_{k+1} = I_{k+2} = \dots = I$.

- (c) Let R be a Noetherian ring. Then for every $r \in R$ there are irreducible elements $r_1, r_2, \dots, r_m \in R$ such that $r = r_1 r_2 \cdots r_m$. (We do not make any claim about uniqueness of this factorization.)

Proof: I should have specified that r is not a unit.

If r is irreducible then we are done. Otherwise write $r = s_1 s_2$, where $s_1, s_2 \in R$ are not units. If s_1 is irreducible then leave it alone; otherwise write $s_1 = s_{11} s_{12}$ where $s_{11}, s_{12} \in R$ are not units. Similarly, if s_2 is irreducible then leave it alone; otherwise $s_2 = s_{21} s_{22}$. Continue inductively creating a tree like this: if $s_{i_1 i_2 \dots i_k}$ is irreducible then leave it alone; otherwise write $s_{i_1 i_2 \dots i_k} = s_{i_1 i_2 \dots i_k 1} \cdot s_{i_1 i_2 \dots i_k 2}$ where neither factor is a unit. If the resulting tree is finite, then reading off the ends of the branches we get the desired factorization $r = r_1 r_2 \cdots r_m$. We must argue that the tree cannot be infinite.

If the tree is infinite, let $t_0 = r$. If the part of the tree under s_1 is infinite, let $t_1 = s_1$; otherwise the part of the tree under s_2 must be infinite, and we let $t_1 = s_2$. Continue inductively: if $t_k = s_{i_1 i_2 \dots i_k}$, by construction the part of the tree lying under $s_{i_1 i_2 \dots i_k}$ must be infinite, so either the part lying under $s_{i_1 i_2 \dots i_k 1}$ is infinite, or the part lying under $s_{i_1 i_2 \dots i_k 2}$ is infinite, or both. If the part lying under $s_{i_1 i_2 \dots i_k 1}$ is infinite, let $t_{k+1} = s_{i_1 i_2 \dots i_k 1}$; otherwise let $t_{k+1} = s_{i_1 i_2 \dots i_k 2}$.

Now we have a sequence t_0, t_1, t_2, \dots with $t_{k+1} \mid t_k$ and $t_{k+1} \nmid t_k$ (because the other factor of t_{k+1} was not a unit). This gives an infinite increasing chain of ideals $(t_0) \subsetneq (t_1) \subsetneq (t_2) \subsetneq \dots$. But this is impossible because R is Noetherian.

- (d) If R is a principal ideal domain and $r \in R$ is irreducible, then r is prime.

Proof: Let $r \in R$ be irreducible, and suppose that $r \mid ab$ for some $a, b \in R$. Since R is a principal ideal domain, we can write $(r, a) = (c)$ for some $c \in R$. Because $r \in (c)$, we can write $r = cd$ for some $d \in R$. Because r is irreducible, either c is a unit or d is a unit. If d is a unit then $c = rd^{-1}$, so $r \mid c \mid a$. If c is a unit then $(c) = (1)$, so we can write $1 = rx + ay$ for some $x, y \in R$. Multiplying through by b we get $b = rbx + aby$. Since r divides ab

it divides aby , and clearly r divides rbx , so it divides their sum, which is b .

- (e) If R is an integral domain in which every irreducible is prime, factorizations are unique: that is, if we have $r_1r_2 \cdots r_m = s_1s_2 \cdots s_n$ with all r_i and s_i irreducible, then $m = n$, and we can reorder the s_i 's so that there are units u_1, u_2, \dots, u_m with $s_i = u_i r_i$.

Proof: Without loss of generality we can assume that $m \leq n$; otherwise switch the r 's and s 's.

Since r_1 is irreducible, it is prime, so $r_1 \mid s_i$ for some i ; after reordering we can assume that $r_1 \mid s_1$. Write $s_1 = u_1 r_1$. Because s_1 is irreducible and r_1 is not a unit, u_1 must be a unit. Thus we have

$$r_1 r_2 \cdots r_m = u_1 r_1 s_2 \cdots s_n.$$

Because R is an integral domain and $r_1 \neq 0$, we can cancel to get

$$r_2 \cdots r_m = u_1 s_2 \cdots s_n.$$

Continue in the same way, writing $r_i = u_i s_i$ (after rearrangement) and cancelling, until all the r 's are used up:

$$1 = u_1 u_2 \cdots u_m s_{m+1} \cdots s_n.$$

Then the remaining s 's are units, and in particular are not irreducible, so we must have had $n = m$.