110A HW6

Warren Kim

Winter 2024

Question 1

Consider $\mathbb{Z}$, and let $p \in \mathbb{Z}$ be nonzero. Show that (p) is a prime ideal if and only if p is prime.

Response

Proof: Let $p \in \mathbb{Z}$ be nonzero.
$(\implies)$ Suppose that (p) is a prime ideal. Consider $ab \in (p)$. This means that $p \mid ab$ since we can represent $ab = pr$ for some $r \in \mathbb{Z}$. If $ab \in (p)$, then by definition either $a \in (p)$ or $b \in (p)$. If $b \in (p)$, then we are done, so suppose not. Then $a \in (p)$; that is, $p \mid a$. Since the following two statements

1. p is prime.

2. If $p \mid ab$, then $p \mid a$ or $p \mid b$.

are equivalent and $a, b \in \mathbb{Z}$ were arbitrary, p is prime.

$(\impliedby)$ Suppose that p is prime. Suppose $p \mid ab$. Then by definition, either $p \mid a$ or $p \mid b$. Without loss of generality, suppose $p \mid a$ and consider $(p) \subseteq \mathbb{Z}$. Then $ab \in (p)$ since $p \mid ab$. But since $p \mid a$, $a \in (p)$. Since $a, b \in \mathbb{Z}$ were arbitrary, (p) is a prime ideal.

Since we proved both directions, (p) is a prime ideal if and only if p is prime. $\square$

Question 2

Let $R = \mathbb{Z}/1024$, and consider the principal ideal $I = ([2]) \subseteq R$. Show that I is maximal.

Response

Proof: Let $R = \mathbb{Z}/1024$ and consider the principal ideal $I = ([2]) \subseteq R$. Then $1 \notin I$, so $I \subsetneq R$ is a proper ideal. Note that $([2])$ contains all even[1] elements of $\mathbb{Z}/1024$. Suppose we have some ideal $J \subseteq R$ such that $J \supsetneq I$. Then there exists $[a] \in J$ such that a is odd. Since J contains I, $[2] \in J$. Then $[a] - [2] \in J$ is also odd[2]. We also have that $[2q] \in I$ for $q \in \mathbb{Z}$, so $[a] - [2q] \in J$. Since a is odd, we can represent $a := 2k + 1$ for some $k \in \mathbb{Z}$. Put $k := q$. Then $[a] - [2q] = [2q + 1 - 2q] = [1] \in J$. Since $[1] \in J$, this implies that $J = R$. Thus, I is a maximal ideal. $\square$

1: Take $[a] \in ([2])$. Then $[a] = [2p] = [2][p] \in ([2])$ for some $p \in \mathbb{Z}$, so a is an even number by definition.

2: $[a] - [2] \in J$ is also odd since we can write $a = 2k + 1$ for some $k \in \mathbb{Z}$, so $[2k + 1] - [2] = [2k + 1 - 2] = [2(k - 1) + 1]$ is an odd number by definition.

Question 3

Let $f : R \to S$ be surjective, and let $P \subseteq S$ be a prime ideal. Show that $f^{-1}(P) \subseteq R$ is a prime ideal.

Response

Proof: Suppose $f : R \to S$ is a surjective ring homomorphism and $P \subseteq S$ is a prime ideal. Then define $f^{-1}(P) \subseteq R$ to be the preimage of S under f; i.e. $f^{-1}(P) := \{x \in R : f(x) \in S\}$. Using the fact that "*if $J \subseteq S$ is any ideal, then $f^{-1}(J) = \{x \in R \mid f(x) \in J\}$ is also an ideal of R*" from class, we have that $f^{-1}(P)$ is an ideal since P is an ideal. Pick $a, b \in R$ such that $ab \in f^{-1}(P)$. Then either $a \in f^{-1}(P)$ or $b \in f^{-1}(P)$. Now since $ab \in f^{-1}(P)$ by assumption, we have that $f(ab) = f(a)f(b) \in P$. Since P is a prime ideal, we have that either $f(a) \in P$ or $f(b) \in P$; i.e. either $a \in f^{-1}(P)$ or $b \in f^{-1}(P)$ by definiton of the preimage. Since $a, b \in R$ were arbitrary, $f^{-1}(P)$ is a prime ideal. $\square$

Question 4

Let $f : R \to S$ be surjective, and let $M \subseteq S$ be a maximal ideal. Show that $f^{-1}(M) \subseteq R$ is maximal.

Response

Proof: Let $f : R \to S$ be a surjective ring homomorphism, and let $M \subseteq S$ be a maximal ideal. Then define $f^{-1}(M)$ to be the preimage of M under f; i.e. $f^{-1}(M) := \{x \in R : f(x) \in S\}$. Using the fact that "*if $J \subseteq S$ is any ideal, then $f^{-1}(J) = \{x \in R \mid f(x) \in J\}$ is also an ideal of R*" from class, we have that $f^{-1}(M)$ is an ideal since M is an ideal. Consider an ideal $N \subseteq R$ such that $f^{-1}(M) \subsetneq N \subseteq R$. Then $f(N)$ is an ideal of S since

1. Take $c, d \in f(N)$. Since f is surjective, there exist $a, b \in R$ such that $f(a) = c, f(b) = d$. Then since N is an ideal, it is closed under subtraction so $f(a - b) = f(a) - f(b) = c - d \in f(N)$.

2. Take $b \in f(N)$ and $s \in S$. Then since f is surjective, there exists $r, a \in R$ such that $f(r) = s, f(a) = b$. Since N is an ideal, $ar, ra \in N$ so $f(ar) = f(a)f(r) = bs \in f(N)$ and $f(ra) = f(r)f(a) = sb \in f(N)$.

3. Since N is an ideal, $0_R \in N$. Since f is a ring homomorphism, $f(0_R) = f(0_S)$. Then $0_S = f(0_R) \in f(N)$.

(1) - (3) are satisfied.

Now, consider $f(f^{-1}(M))$. Then $f(f^{-1}(M)) \subseteq M$ since if we take $f(a) \in f(f^{-1}(M))$, then $f(a) \in M$ because $a \in f^{-1}(M)$. Now since f is surjective, for all $y \in M$, there exists $x \in R$ such that $f(x) = y$. But $x \in f^{-1}(M)$ since $f(x) = y \in M$, so $f(f^{-1}(M)) \supseteq M$. Thus, $f(f^{-1}(M)) = M$.

Since M is maximal, either $f(N) = S$ or $f(N) = f(f^{-1}(M)) = M$. If $f(N) = S$, then since f is surjective, this means that N maps onto all of S, so $N = R$. If $f(N) = f(f^{-1}(M)) = M$, then $N \subseteq f^{-1}(M)$, a contradiction. So, $f^{-1}(M)$ is a maximal ideal. $\square$