

Algebra II - Spring - HW8 - June 1, 2021

Mandatory:

(1) If $n, m \in \mathbb{N}$, let us say that $n \leq m$ if and only if n divides m . Show that the relation \leq is a partial order on \mathbb{N} . Is the set $\{2, 3, 4, 5\}$ a chain?

Proof. We need to show that this relation is the reflexive, antisymmetric, and transitive in order to be a partial order on \mathbb{N} .

Reflexive: Let $n \in \mathbb{N}$. We know $n \leq n$ is true since $n \mid n \implies nk = n$, where k will just be 1 and we know 1 is in the set of natural numbers.

Antisymmetric: Let $n, m \in \mathbb{N}$. We know that if $n \leq m$ that implies that $n \mid m$ which means there exists $d \in \mathbb{N}$ such that $nd = m$. Now if $m \leq n$ that implies $m \mid n$ which means there exists $b \in \mathbb{N}$ such that $mb = n$. Now plugging in the first expression into the second one for m we get,

$$mb = n$$

$$ndb = n$$

This statement can only hold if both d and b are equal to 1. Which implies that $m = n$. Thus this relation is antisymmetric.

Transitivity: Let $x, y, z \in \mathbb{N}$. Where $x \leq y$ and $y \leq z$. Like before that would imply $xd = y$ and $yb = z$. So plugging in the first equality into the second one for y we get,

$$yb = z$$

$$xdb = z$$

We know that $db = c$ where c is some natural number since d, b were natural numbers and the natural numbers are closed under multiplication, so we get $xc = z \implies x \leq z$. Thus this relation is transitive.

Therefore this relation is a partial order on \mathbb{N} . □

The given set is not a chain. One reason is immediately we see that $2 \leq 3$ doesn't hold based on our given relation and there actually is no relation between 3 and any of the other given elements. Meaning it doesn't satisfy the required conditions and thus not a chain.

(2) Let R be a commutative ring with $1 \neq 0$. The *Jacobson radical* of R , denoted $J(R)$, is defined as the intersection of all maximal ideals of R . In symbols:

$$J(R) := \bigcap_{M=\text{maximal ideal of } R} M.$$

Prove that $J(R)$ is a proper ideal of R , and determine $J(\mathbb{Z})$.

Proof. I believe in a previous homework we proved that the intersection of ideals is an ideal, but I'll show it again with the following.

Obviously this is non empty since in class we learned that for this type of ring there always exists a maximal ideal.

Let $a, b \in J(R)$. We want to show that $a - b \in J(R)$. We know though that since $a, b \in J(R)$ are in all maximal ideals of R then by definition of them being ideals we know that $a - b \in M$ for all M . Therefore it is also in $J(R)$.

Let $r \in R$ and $a \in J(R)$ we want to show $ra \in J(R)$, but like the reasoning before since a is in every maximal ideal of R then by definition of them being ideals $ra \in M$ for all M and thus $ra \in J(R)$.

Thus this forms an ideal. The reason this is a proper ideal is that by definition maximal ideals have to be proper, and since none of these ideals contain the whole ring it's the intersection can never create the whole ring thus this ideal is proper as well. \square

$J(\mathbb{Z})$. We know that the all maximal ideals of \mathbb{Z} have the form $p\mathbb{Z}$ where p is prime. Since for each p the set $p\mathbb{Z}$ is just all multiples of p . So for an element to exist in every maximal ideal of \mathbb{Z} it would mean that it is divisible by all possible primes. Since the number of primes is infinite the only integer that can satisfy that requirement would be 0. Thus $J(\mathbb{Z}) = \{0\}$.

(3) Recall that the *Gaussian integers* $\mathbb{Z}[i]$ is the following subring of \mathbb{C} :

$$\mathbb{Z}[i] := \{a + bi : a, b \in \mathbb{Z}\}.$$

Use the fact that $(1+i)(1-i) = 2$ to show that the ideal of $\mathbb{Z}[i]$ generated by 2 is not a prime ideal.

Proof. Well we know that the ideal generated by 2 is the following,

$$I = (2) = \{2r : r \in \mathbb{Z}[i]\} = \{2a + 2bi : a, b \in \mathbb{Z}\} \tag{1}$$

Which is just the set of elements with even coefficients. Which means that $(1+i), (1-i) \notin I$. Applying the fact given though, we see that their product equals 2, and 2 is indeed in the set. Which means this fails to satisfy the requirements to be a prime ideal, since neither of the 2 elements we multiplied are in the set, but their product produced an element in the set. \square

(4) Let A and B be commutative rings both with 1 and let $f : A \rightarrow B$ be a unital ring homomorphism. If P is a prime ideal of B , prove that

$$f^{-1}(P) = \{a \in A : f(a) \in P\}$$

is a prime ideal of A .

Proof. First we know this is non empty since from clas we know every ideal contains 0 and thus $f^{-1}(P)$ will contain 0

Let's take $x, y \in f^{-1}(P)$ by definition this means that $f(x), f(y) \in P$. We know P to be an ideal, so by definition we know $f(x) + f(y) \in P$. Thanks to the ring homomorphism we also know that $f(x) + f(y) = f(x + y)$ which means $x + y \in f^{-1}(P)$.

Let $x \in f^{-1}(P)$ and $a \in A$. We know that $f(x) \in P$ and because P is an ideal, we have it that $f(a) \cdot f(x) \in P$. Like before thanks to the ring homomorphism we know $f(a)f(x) = f(ax)$ which means $ax \in f^{-1}(P)$. With these two conditions we just proved $f^{-1}(P)$ is an ideal.

Now take $x \cdot y \in f^{-1}(P)$ we know $f(xy) \in P$, and by the ring homomorphism we then know $f(x)f(y) \in P$. Thus by definition either $f(x)$ or $f(y)$ are in P . This gives us that either x or y are in $f^{-1}(P)$.

Therefore $f^{-1}(P)$ is a prime ideal. □

Optional:

(5) Give an example to show that the result of problem (4) is not true if “prime ideal” is replaced with “maximal ideal.”

(6) Let $p \in \mathbb{N}$ be a prime. Consider the following subset of the rationals:

$$\mathbb{Z}_{(p)} := \left\{ \frac{a}{b} \in \mathbb{Q} : \gcd(a, b) = 1 \text{ and } p \nmid b \right\}.$$

In words, $\mathbb{Z}_{(p)}$ is the set of rational numbers $x \in \mathbb{Q}$ such that when x is written in lowest terms, say $x = \frac{a}{b}$, then p does not divide b .

(a) Show that $\mathbb{Z}_{(p)}$ is a subring of \mathbb{Q} . (The ring $\mathbb{Z}_{(p)}$ is called the *localization of \mathbb{Z} at (p)* .)

(b) Use the usual bar notation for the elements of $\mathbb{Z}/p\mathbb{Z}$; that is, write $\bar{k} = k + p\mathbb{Z}$ for each $k \in \mathbb{Z}$. Define a map

$$\begin{aligned} \phi : \mathbb{Z}_{(p)} &\rightarrow \mathbb{Z}/p\mathbb{Z} \\ x &\mapsto \bar{a} \cdot (\bar{b})^{-1} \text{ if } x = \frac{a}{b}. \end{aligned}$$

Prove that ϕ is a well-defined, unital, and surjective ring homomorphism. Deduce that

$$p\mathbb{Z}_{(p)} = \left\{ \frac{a}{b} \in \mathbb{Q} : \gcd(a, b) = 1, p \nmid b, \text{ and } p \mid a \right\}$$

is a maximal ideal of $\mathbb{Z}_{(p)}$.

(c) Show that $p\mathbb{Z}_{(p)}$ is the *unique* maximal ideal of $\mathbb{Z}_{(p)}$.