March 4th 2020
MA484 Problem Day 2

1 Problem 2

Remember that an ideal in R is a subset $I \subset R$ which contains 0, is closed under addition, and "absorbs products," that is, if $r \in I$ and $x \in R$ then $rx \in I$. The easiest ideals are the principal ideals, which are just the set of all multiples of some fixed element $a \in R$:

$$I = Ra = (a) = \{ra \mid r \in R\}$$

The next-easiest ideals are the finitely-generated ones, where

$$I = \{r_1 a_1 + r_2 a_2 + \ + r_k a_k \mid ri \in R\}$$

for some finite set of $a_1, a_2, ..., a_n \in R$. Let k be a field and let $R = k[x]$. Show that any ideal $I \subset R$ is principal. (If $I = \{0\}$, find an element $a \in I$ of minimal degree and prove that $I = Ra$.) A domain in which every ideal is principal is called a principal ideal domain, or PID. The most important examples are $\mathbb{Z}$ and $k[x]$ when k is a field.

Proof:

To show that any ideal $I \subset R$ is principal, we must show that it is generated by one element in I. We start by considering if I is the zero ideal.

If $I = \{0\}$, then we have that $I = \{ar \mid r \in R\}$ and $a = 0$. This shows that this is a principal ideal in R.

If I is non-zero, we want to pick a polynomial $g(x) \in I$ of lowest degree, and want to show that the ideal I is the ideal generated by $g(x)$. This is to say

$$I = \ < g(x) >$$

Our next step is to take another element of $f(x) \in I$ (which is a polynomial) and divide it by our polynomial of minimal degree, $g(x)$. Using the division algorithm for polynomials, we have

$$f(x) = g(x)q(x) + r(x)$$

where $g(x), q(x), r(x)$ are all polynomials in I, and degree $r(x) < g(x)$
Rearranging our equation, we see that

$$r(x) = f(x) - g(x)q(x)$$

and $f(x) \in I$, and $g(x)q(x) \in I$ because $g(x) \in I$. Thus, we see that $r(x) \in I$. Now we see that because $r(x)$ has degree strictly less than $g(x)$, it must be that $r(x)$ is the zero polynomial because we defined $g(x)$ to have *minimal degree*. This shows that $g(x)$ generates all elements of I, and thus I is a principal ideal, which concludes the proof.

2 Problem 3

An ideal $I \subset R$ is called maximal if $I = R$ and there are no ideals "between" I and R: if J is an ideal and $I \subset J \subset R$ then either $I = J$ or $I = R$. Show that I is maximal if and only if R/I is a field.

Proof:

This is an if and only if so we must verify two directions. We start with the forward direction.

$(\Rightarrow)$

Assume that I is maximal. We want to show that R/I is a field. To show that R/I is a field, we want to show that it has multiplicative inverses.

Let $b + I \in R/I$ be an arbitrary element of R/I, where $b \in R$. Assume that this element is non-zero, because zero has no multiplicative inverse. Because $b + I \neq 0$, we know that $b \notin I$. We now create the set

$$B = \{br + a \mid r \in R, a \in I\}$$

Claims about B: We now claim that this set B is an ideal of R that properly contains I. Additionally, we also claim that $B = R$, and $1 \in B$.

B contains I because if we let $r = 0$, then all elements of B look like elements of I. B properly contains I because $b \in B$ and $b \notin I$. Additionally, B is an ideal because adding any two elements in B gives an element in B, and it absorbs products.

We now want to show that our arbitrary element $b + I$ has an inverse. Because I is maximal, and B properly contains I, we now know that $B = R$. In particular, $1 \in B$. Thus, we can write

$$1 = bc + a \qquad c \in R, \ a \in I$$

So in R/I, we have

$$1 + I = bc + a + I$$

But I absorbs a because $a \in I$. So we are left with

$$1 + I = bc + I = (b + I)(c + I)$$

Notice that $1 + I$ is the identity element of R/I, so thus we have shown that our arbitrary element of R/I has a multiplicative inverse! Thus, R/I is a field and this direction of the implication is verified.

$(\Leftarrow)$

Assume that R/I is a field. We want to show that I is maximal. We once again consider our set B that we defined above. We have already shown that B properly contains I. Our new task is to now show that $B = R$.

We once again consider our arbitrary element $b + I \in R/I$ where $b \in B, b \notin I$. Because $b + I \in R/I$, it has a multiplicative inverse, let us call it $c + I$. Now we multiply the two to get the identity in R/I.

$$(b + I)(c + I) = (bc + I) = 1 + I$$

Thus, we can conclude that $bc - 1 \in I$ via rearranging and using the properties of ideals. Our new goal is to show that $1 \in B$, because if this is true, then B is the whole ring R. Because $bc - 1 \in I$, we have that

$$1 - bc + (bc) = 1 \in B$$

Thus, we now have that $1 \in B$, so it must be that $B = R$. This shows that I is maximal and the proof is complete. We have now verified both directions of the implication, and thus the if and only if holds.

3 Problem 4

An ideal $I \subset R$ is called prime if $ab \in I$ implies that either $a \in I$ or $b \in I$. Show that I is prime if and only if R/I is a domain.

Proof:

Because this is an if and only if statement, we must verify both directions. We start with the forward direction.

$(\Rightarrow)$

Assume that I is a prime ideal. We want to show that R/I is a domain.

Because I is a prime ideal, given $ab \in I$, it follows that $a \in I$ or $b \in I$. We now want to show that if we multiply any two elements in R/I and they produce the zero element in R/I, that one of the two things we multiplied with was the zero element in R/I. Consider

$$0 = (x + I)(y + I) = xy + I \qquad x, y \in R$$

Note that the zero element in R/I is I because it has the form $r + I$, where $r \in R$ is 0. Because $xy + I = 0$ in R/I, it must be that $xy \in I$. We can now use the fact that I is a prime ideal, which implies that

$$x \in I \text{ or } y \in I$$

Without loss of generality, let's assume $x \in I$. Thus, it must be that $(x + I) = I$ which is the zero element of R/I. Thus, we have shown that one of the two things we multiplied in R/I to get the zero element was the zero element, and thus R/I has no zero divisors. Thus, R/I is a domain and this direction of the implication is verified.

$(\Leftarrow)$

Assume that R/I is a domain. We want to show that I is a prime ideal. Here, we will essentially do the forward implication in reverse to get this direction.

Consider the product of elements in R/I that produces the zero element in R/I. We will once again use $x, y \in R$ such that

$$0 = (x + I)(y + I) = xy + I$$

Because R/I is a domain, it must be that either $(x + I) = 0$, or $(y + I) = 0$. For either of these to be true, it must be that x or y is an element of I. Thus, we conclude that either $x \in I$ or $y \in I$. Because $xy + I = 0$, we can also conclude that $xy \in I$. Thus, we have that

$$\text{if } xy \in I, \text{ then either } x \in I \text{ or } y \in I$$

This is exactly the definition of a prime ideal, so thus, I is a prime ideal. We have verified both direction, so the if and only if holds and the proof is complete.

4 Problem 5

Show that any maximal ideal is prime. Find an easy example of a prime ideal that is not maximal.

Proof:

This one is quite quick. By Problem 3, we know

$$I \text{ is maximal ideal in } R \;\Leftrightarrow\; R/I \text{ is a field}$$

and we also know from Problem 4 that

$$I \text{ is a prime ideal in } R \;\Leftrightarrow\; R/I \text{ is a domain}$$

Let M be a maximal ideal in a ring R. By Problem 3, we know that R/M is a field. By Problem 4, we know that because a field is an integral domain, that M is a prime ideal of R. Thus, the proof is complete.

To find an example of a prime ideal that is not maximal, we want to look for a domain that is not a field because that is the link we established to prove that maximal ideals are prime ideals. Consider the zero ideal in a domain. Unless the domain is already a field, this ideal will not be maximal because there will be other elements in the ring R. Note that the zero ideal in a domain is prime, so thus, we have found a prime ideal in a ring R that is not maximal.

5 Problem 8

Suppose R is Noetherian, $a \in R, a = 0, a \notin R^x$ (i.e. a is not a unit). Show that there exist irreducibles $\pi_1, \pi_2, ..., \pi_k$ such that $a = \pi_1\pi_2...\pi_k$. In other words, factorizations exist.

Proof:

We will do this by contradiction. Suppose for a contradiction that a cannot be written as the product of irreducibles. Let us define the set of ideals

$$S = \{aR \mid a \text{ cannot be written as a product of irreducibles}\}$$

By the property of Noetherian rings, S has a maximal element. Let us call this maximal element sR. Let us now say that

$$s = xy$$

and neither x nor y is a unit. Note that s must factor because it is not irreducible. Because x, y are not units, the ideals

$$xR,\ yR \;\subsetneq\; sR$$

Because $xy = s$, it follows that xR and yR are not in S. Thus, x and y can be written as the product of irreducibles (i.e. they factor). So we can write them as

$$x = \pi_1 \pi_2 ... \pi_n (u)$$

$$y = \rho_1 \rho_2 ... \rho_k (v)$$

Where u and v are units in R. Thus, we can write S as

$$s = xy = x = \pi_1 \pi_2 ... \pi_n \rho_1 \rho_2 ... \rho_k (uv)$$

and now we have a contradiction because we assumed s *could not* be written as the product of irreducibles. Thus, it must be that in Noetherian rings, all non-zero, non-unit elements can be written as the product of irreducibles in the ring, and the proof is complete.

6 Problem 11

Let $R = \mathbb{Z}[\sqrt{-5}] = \{a + b\sqrt{-5} \mid a, b \in \mathbb{Z}\}$. R is known to be a Noetherian domain. Let $N : R \to \mathbb{Z}$ be the function $N(a + b\sqrt{-5}) = a^2 + 5b^2$. Since this is just the square of the complex absolute value, we know that $N\alpha\beta) = N(\alpha)N(\beta)$. (Of course, it's easy to check that by hand as well.)

a. Show that u is a unit in R if and only if $N(u) = 1$.

b. Show that no element of R has norm 3.

c. Show that no element of R has norm 7.

d. Show that 3, 7, (1+ 2$\sqrt{-5}$), and (1 - 2$\sqrt{-5}$) are all irreducible in R.

e. Check that $3 \times 7 =$ (1 + 2 $\sqrt{-5}$)(1 - 2$\sqrt{-5}$).

f. What does that tell you?

Proof:

This one has a lot of parts.

(a):

$$(\Rightarrow)$$

Assume that u is a unit in R. We want to show that $N(u) = 1$. Because u is a unit, we know that

$$uu^{-1} = 1$$

If we now apply our function N to uu^{-1}, by the properties of N, we get

$$N(uu^{-1}) = N(u)N(u^{-1}) = 1$$

This shows us that $N(u)$ and $N(u^{-1})$ must be factors of 1. The only factors of 1 are 1 and -1, but because N outputs a strictly positive number, it follows that $N(u) = 1$, and thus this direction is verified.

$(\Leftarrow)$

Assume that $N(u) = 1$. We want to show u is a unit in R. We know that the norm is the product of a number with its conjugate. Thus, if $N(u) = 1$, we are done because the conjugate is just the inverse. Thus, both directions are verified and the proof is complete.

(b) and (c):

These are fairly straightforward computations. Because neither 3 nor 7 is a square, and each is not a multiple of 5, it follows that no norm of any element in R can be 3 or 7.

(d):

These are again just computations. Note that

$$N(3) = 9 = 3 \cdot 3$$
$$N(7) = 49 = 7 \cdot 7$$
$$N(1 + 2\sqrt{-5}) = N(1 - 2\sqrt{-5}) = 21 = 7 \cdot 3$$

and no element of R has norm 3 or norm 7 so thus all of these cannot be reduced further (hence irreducible).

(e):

When we check, we find that

$$3 \cdot 7 = (1 + 2\sqrt{-5})(1 - 2\sqrt{-5}) = (1 + 4 \cdot 5) = 21$$

(f):

The case in part (e) shows us that non unique factorizations exist in this ring R! This is really cool because it is very difficult to actually construct and work with a ring where factorizations are not unique.