Math250aHw1

Trustin Nguyen

December 3, 2023

Exercise 1: Let k be a field. The ring of formal power series in 1 variable $k[[x]]$ has a unique maximal ideal.

Proof. Consider the homomorphism $\varphi : k[[x]] \to k$. The kernel of this homomorphism will be the maximal ideal. We can take φ to be the evaluation map at 0. Then $\ker \varphi = (x)$ since any polynomial with x as a factor will be sent to 0. Now suppose that we had another ideal $(f) \neq (x)$. Then we will show that it will be equal to the whole ring. We make clear that f is not divisible by x otherwise, $(f) \subseteq (x)$. This equates to showing that every polynomial that is not divisible by x is invertible. We have that:

$$\frac{1}{1-x} = 1 + x + x^2 + \dots$$

and to get the inverse of a polynomial f, we can make the substitution $x = 1 - f$ to get:

$$\frac{1}{1-(1-f)} = \frac{1}{f}$$

But this does not work with all $f \in R$ because for $f = x$, we have:

$$\frac{1}{x} = 1 + 1 - x + (1-x)^2 + \dots$$

which has an infinite degree 0 term which is not in our field. Suppose that $x \nmid f$. Then there is a non-zero constant:

$$f = a_0 + a_1 x + a_2 x^2 + \dots$$

This means that we can make the constant term equal to 1:

$$a_0^{-1} f = 1 + a_0^{-1} a_1 x + a_0^{-1} a_2 x^2 + \dots$$

We note that if $a_0^{-1} f$ is invertible, then f is invertible:

$$a_0^{-1} f \cdot g = 1 \implies f \cdot a_0^{-1} g = 1$$

So we have:

$$\frac{1}{1-(1-a_0^{-1}f)} = \frac{1}{1-(-a_0^{-1}a_1 x - a_0^{-1}a_2 x^2 - \dots)} = 1 + (1 - a_0^{-1}f) + (1 - a_0^{-1}f)^2 + \dots$$

But this is well defined because if we take the term of the lowest degree of each of the powers in our sum: $a_0^{-1}a_1 x$, the lowest exponent in the polynomial $(a_0^{-1}f)^k$ would be k since $(a_0^{-1}a_1 x)^k$ has degree k. So each term of $(a_0^{-1}f)^{-1}$ is in our field. Therefore, we have proven that (x) is the unique maximal ideal. □

Exercise 2: Let R be a commutative ring, and let $S \subseteq R$ be a multiplicatively closed subset (that is, if $a, b \in S$, then $ab \in S$.) If I is an ideal maximal with respect to the property $I \cap S = \emptyset$ then I is prime.

Proof. Suppose that $xy \in I$ and $x \notin I$. Consider the cosets of I, and let the representatives of all but the additive identity $(0 + I)$ be elements of S. This implies that $I \cup S = R$. We have that:

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

But $x \in S$, and $y \notin S$ (otherwise, we say that $xy \in S$ leading to a contradiction), so $y \in I$. So I is prime. □

Exercise 3: If R is a principal ideal ring (that is, every ideal of R is principal), $p \in R$ an element that generates a prime ideal, and $a \notin (p)$, then $(a, p) = R$.

Proof. Suppose $(p) \neq R$. Since R is a PID, we have that for some $u \in R$, $(u) = (a, p)$. This means that:

$$ux = a$$
$$uy = p$$

But we note that since p is prime, $a \notin (p)$, then neither u nor x are in (p). This means that $y \in p$ So we can say that $y = wp$:

$$uwp = p$$

So $(uw - 1)p = 0$ and $uw = 1$ therefore, u is a unit. But since u is a unit, then $1 \in (u)$ so $(u) = R$. □

Exercise 4: If A, B are ideals in the commutative ring R, and $A + B = R$ then $AB = A \cap B$.

Proof. We will show a two sided containment:

($AB \subseteq A \cap B$) We have that AB is the set of all sums:

$$a_1b_1 + \ldots + a_nb_n$$

for $a_i \in A$ and $b_i \in B$. Since $b_i \in R$, we have by definition that that sum above is in A. Since it is a commutative ring, all ideals are two-sided. This means that also,

$$a_1b_1 + \ldots + a_nb_n \in B$$

So this sum is actually in the intersection $A \cap B$.

($A \cap B \subseteq AB$) Suppose an element m is in $A \cap B$. Since $A + B = R$, we have that the set contains the identity so:

$$a + b = 1$$

But now, we have:

$$m = am + bm$$

and since $m \in A$ and $m \in B$, we can write m as:

$$m = a_1r_1 + \ldots + a_nr_n$$
$$m = b_1s_1 + \ldots + b_ms_m$$

So therefore:

$$m = a(b_1s_1 + \ldots + b_ms_m) + b(a_1r_1 + \ldots + a_nr_n)$$

Once everything is expanded, m will be clearly of the form:

$$a'_1b'_1 + \ldots + a'_nb'_n$$

which means that $m \in AB$. □

Exercise 5: If k is a field of characteristic $2 > 0$ and G is a group with 2 elements, then $k[G] \cong k[x]/(x^2)$, and this has a unique maximal ideal.

Proof. (Part I) Consider the morphism from $k[G] \to k[x]/(x^2)$ given by:

$$\begin{aligned} 0 \cdot e + 0 \cdot g &\mapsto 0 \\ 1 \cdot e + 0 \cdot g &\mapsto 1 \\ 0 \cdot e + 1 \cdot g &\mapsto x + 1 \\ 1 \cdot e + 1 \cdot g &\mapsto x \end{aligned}$$

so we have:

$$e \mapsto 1 \qquad \text{and} \qquad g \mapsto x + 1$$

To prove that this is a homomorphism:

Additive:

$$\begin{aligned} \varphi(ae + bg) + \varphi(ce + dg) &= a + bx + b + c + dx + d \\ &= a + c + (b + d)x + (b + d) \\ &= \varphi((a + c)e + (b + d)g) \\ &= \varphi(ae + bg + ce + dg) \end{aligned}$$

Multiplicative:

$$\begin{aligned} \varphi(ae + bg)\varphi(ce + dg) &= (a + b + bx)(c + d + dx) \\ &= (ac + ad + adx + bc + bd + bdx + bcx + bdx + bdx^2) \\ &= (ac + bd) + adx + ad + bcx + bc \\ &= \varphi((ae + bg)(ce + dg)) \end{aligned}$$

Since the map is surjective, we have a bijective homomorphism and therefore an isomorphism of rings.

(Part II) We can check by cases the maximal ideal. Since $k[G] \cong k[x]/(x^2)$, we can consider the ring on the right instead. Clearly, 0 must be in the ideal. We cannot have 1 in the ideal, and notice that $x + 1$ has an inverse as it gets mapped to g and we know that $g^2 = 1$. So we have proved that our ideal (x) is maximal in $k[x]/x^2$, and that no other elements in the ring can belong to any maximal ideal. This means that (x) is the unique maximal ideal. Since we know that x is sent to $1e + 1g$, we know that the maximal ideal of $k[G]$ is just $(e + g)$. □

Exercise 6: A commutative ring R is isomorphic to the product of two (nontrivial, that is, with $1 \neq 0$) rings $R_1 \times R_2$ if and only if R contains *nontrivial orthogonal idempotents*, that is, elements $e_1, e_2 \in R$ not equal to 0 or 1, such that $e_1^2 = e_1$, $e_2^2 = e_2$ and $e_1 e_2 = 0$. Find nontrivial orthogonal idempotents in the group algebra $\mathbb{C}[G]$, where $\mathbb{C}$ denotes the complex numbers and G is again the group with 2 elements. This ring has 2 maximal ideals.

Proof. (Part I) ($\to$) Suppose that $R \cong R_1 \times R_2$. Then we have the additive identity element of R denoted as e_0 and the multiplicative identity denoted as e_1. Consider the elements in $R_1 \times R_2$ which are:

$$r_1 = (e_1, e_0) \qquad \text{and} \qquad r_2 = (e_0, e_1)$$

we observe that:

$$r_1^2 = r_1 \qquad \text{and} \qquad r_2^2 = r_2 \qquad \text{and} \qquad r_1 r_2 = (r_0, r_0) = 0$$

But these are two distinct orthogonal idempotent elements in $R_1 \times R_2$. Therefore, we just need to prove that they are non-trivial. This is easily the case because any ring homomorphism

$$\varphi : R \to R_1 \times R_2$$

must satisfy:

$$\varphi(0) = (e_0, e_0)$$
$$\varphi(1) = (e_1, e_1)$$

both of which are elements that we did not choose.

($\leftarrow$) Suppose that our ring contains two nontrivial orthogonal idempotent elements. Then we consider (e_1) and (e_2). Observe that elements, n, in the sum of these ideals:

$$a_1 e_1 + a_2 e_2 = n$$

have the following property for $a_1, a_2 \in R$

$$\begin{aligned} e_1 n + e_2 n &= e_1^2 a_1 + e_1 e_2 a_2 + e_1 e_2 a_1 + e_2^2 a_2 \\ &= n \end{aligned}$$

Therefore, we have:

$$n(e_1 + e_2) = n$$

so

$$e_1 + e_2 = 1$$

But by the Chinese Remainder Theorem, we have:

$$R \cong R/(e_1) \times R/(e_2)$$

Since e_1, e_2 are nontrivial, we will show that neither one of the ideals are trivial. Suppose that e_1 is a unit or $e_1 d = 1$. Then we say that:

$$\begin{aligned} e_1 e_2 &= 0 \\ e_1 d e_2 &= 0 \\ e_2 &= 0 \end{aligned}$$

which is a contradiction. So we are done.

(Part II) We want to find a ring isomorphic to $\mathbb{C}[G]$. We start notice that in the ring $\mathbb{C}[x]$, we have that $(x + i)(x - i) = x^2 + 1$ looks suspiciously close to $g^2 = 1$ which is what we desire. So we take $\mathbb{C}[x]/(x^2 + 1)$. So the mappings can be figured out by realizing that:

$$(1 + ix)^2 = 1 + 2ix - x^2 = 1 + 2ix - x^2 - 1 + 1 = 2 + 2ix$$

which obeys the fact that $(1 \cdot e + 1 \cdot g)^2 = 2 \cdot e + 2 \cdot g$ in $\mathbb{C}[G]$. So we can figure out all the mappings by just the generators of $\mathbb{C}[G]$:

$$1 \cdot e + 0 \cdot g = 1$$
$$0 \cdot e + 1 \cdot g = ix$$

Now we check to see if this is a ring homomorphism. First is addition:

$$\begin{aligned} \varphi(a \cdot e) + \varphi(b \cdot e) &= a + b \\ &= (a + b) \\ &= \varphi((a + b) \cdot e) \\ \varphi(a \cdot e) + \varphi(b \cdot g) &= a + bix \\ &= \varphi(a \cdot e + b \cdot g) \\ \varphi(a \cdot g) + \varphi(b \cdot g) &= aix + bix \\ &= (a + b)ix \\ &= \varphi((a + b) \cdot g) \end{aligned}$$

So we have proven the structure on the generators and therefore the whole group ring. Now for multiplication:

$$\begin{aligned}
\varphi(a \cdot e)\varphi(b \cdot e) &= ab \\
&= \varphi(ab \cdot e) \\
\varphi(a \cdot e)\varphi(b \cdot g) &= abix \\
&= \varphi(ab \cdot g) \\
\varphi(a \cdot g)\varphi(b \cdot g) &= aixbix \\
&= -abx^2 \\
&= -abx^2 - ab + ab \\
&= ab \\
&= \varphi(ab \cdot e)
\end{aligned}$$

So we have that this is an isomorphism because all elements of $\mathbb{C}[x]/(x^2+1)$ are of the form $a + bi + (c + di)x$ which we can get from

$$\varphi((a + bi) \cdot e) + \varphi(-ci \cdot g) + \varphi(d \cdot g) = a + bi + (c + di)x$$

One of the idempotent elements is ix and the other we get from taking $a \cdot e + b \cdot g$ squared:

$$\begin{aligned}
(a \cdot e + b \cdot g)^2 &= (a^2 + b^2) \cdot e + 2ab \cdot g \\
&\implies a^2 + b^2 = a \wedge 2ab = g
\end{aligned}$$

which we can solve to get $a = \frac{1}{2}$ and $b = \frac{1}{2}$. So our second idempotent element is $\frac{1}{2} + \frac{1}{2}ix$. Notice that this element and the last were not orthogonal. It can be easily checked that $\frac{1}{2} + \frac{1}{2}ix$ and $\frac{1}{2} - \frac{1}{2}ix$ are orthogonal however. Therefore our orthogonal idempotent elements are:

- $\frac{1}{2} \cdot e + \frac{1}{2} \cdot g$
- $\frac{1}{2} \cdot e - \frac{1}{2} \cdot g$

~~Didnt finish~~ □