Math 110BH homework 2

Nathan Solomon

January 23, 2024

Due January 23rd

1

Prove that every (left) ideal of the product $R \times S$ of two rings is a product $I \times J$, where $I \subset R$ and $J \subset S$ are (left) ideals.

Let K be any left ideal of $R \times S$. Then for any $(a, b) \in K$ and any $(x, y) \in R \times S$, $(x, y) \cdot (a, b) = (xa, yb)$ is also in K. Let $\pi_1 : R \times S \to R$ and $\pi_2 : R \times S \to S$ be the projection homomorphisms which take any (x, y) to x and to y, respectively. Define I to be $\pi_1(K)$ and J to be $\pi_2(K)$. I is a left ideal of R because:

- It contains zero – since $(0, 0) \in R \times S$ and $\pi_1((0, 0)) = 0$, I also contains 0.
- It is closed under addition – if $a_1, a_2 \in I$, then because π_1 is surjective, there exist elements $b_1, b_2 \in J$ such that (a_1, b_1) and $(a_2, b_2) \in K$, which implies $(a_1 + a_2, b_1 + b_2) \in K$, so $a_1 + b_2$ is in $\pi_1(K)$.
- It is closed under left multiplication by any element of I – if $a \in I$, then by the same logic, there exists some $(a, b) \in K$, so for any $(x, y) \in R \times S$, (xa, yb) is also in K, which implies xa is in I.

So I is a left ideal of R, and by the same reasoning, J is a left ideal of S, and we already stated that $K = I \times J$.

2

- (a) Find all idempotents in $\mathbb{Z}/105\mathbb{Z}$.
- (b) Prove that $\mathbb{Z}/p^n\mathbb{Z}$, p a prime, has no nontrivial idempotents.

- (a) The python code “print([x for x in range(105) if x**2%105==x])” shows that the answer is

$$\{0, 1, 15, 21, 36, 70, 85, 91\}.$$

  Alternatively, we can use the Chinese Remainder Theorem to say that $\mathbb{Z}/105\mathbb{Z}$ is ring-isomorphic to $\mathbb{Z}/3\mathbb{Z}\times\mathbb{Z}/5\mathbb{Z}\times\mathbb{Z}/7\mathbb{Z}$. An element of $([a],[b],[c]) \in \mathbb{Z}/3\mathbb{Z}\times\mathbb{Z}/5\mathbb{Z}\times\mathbb{Z}/7\mathbb{Z}$ is idempotent if and only $[a]_3$, $[b]_5$, and $[c]_7$ are all idempotent.

  If a is an idempotent element in a field $\mathbb{F}$, then $a^2 = a$, so a can be zero. If a is nonzero, then a is invertible, so $a^{-1}a^2 = a^{-1}a$, meaning is the identity. We know that $\mathbb{Z}/p\mathbb{Z}$ is a field when p is prime, so the only idempotent elements of $\mathbb{Z}/p\mathbb{Z}$ are $[0]$ and $[1]$.

  Therefore in $\mathbb{Z}/3\mathbb{Z}\times\mathbb{Z}/5\mathbb{Z}\times\mathbb{Z}/7\mathbb{Z}$, the idempotent elements are precisely the 8 elements for which each component is either $[0]$ or $[1]$. That set is generated by $(1, 0, 0)$, $(0, 1, 0)$, and $(0, 0, 1)$. To find the element of $\mathbb{Z}/105\mathbb{Z}$ which corresponds to $(1, 0, 0)$, we need to find a number which is congruent to 1 (modulo 3) and is a multiple of both 5 and 7, so we test all multiples of 35 between 0 and 104 until we find that it's 70. By the same method, we find $(0, 1, 0)$ corresponds to 21 and $(0, 0, 1)$ corresponds to 15, and we can then take the sum (modulo 105) of all subsets of $\{70, 21, 15\}$ to get the full list of idempotents:

$$\{0, 1, 15, 21, 36, 70, 85, 91\}.$$

- (b) Suppose there exists an idempotent element $a \in \mathbb{Z}/p^n\mathbb{Z}$. Then $a(a-1)$ is a multiple of p^n. If a is a multiple of p, then $a - 1$ is not, and if $a - 1$ is a multiple of p, then a is not. Therefore either a or $a - 1$ divides p^n, which is true if and only if a is equal to $[0]$ or $[1]$ in $\mathbb{Z}/p^n\mathbb{Z}$.

3

Suppose a commutative ring has finitely many idempotents. Prove that the number of idempotents is a power of 2.

Lemma: if x is idempotent and $x \neq 1$, then x is not invertible. Proof: if x is invertible and idempotent, then $x = x^{-1}x^2 = x^{-1}x = 1$.

Let R be a ring with finitely many idempotents. If R does not contain any nontrivial idempotents, than it has either 1 or 2 idempotents, so we're done.

If R contains a nontrivial idempotent a, then $R = aR + (1 - a)R$, so by the Chinese Remainder Theorem, R is isomorphic to $R/aR \times R/(1 - a)R$, which implies the number of idempotents in R is the number of idempotents in R/aR times the number of idempotents in $R/(1 - a)R$. By the lemma above, a and $1 - a$ are not invertible, so neither aR nor $(1 - a)R$ are unit ideals. Therefore R/aR and $R/(1 - a)R$ are both nonzero rings, meaning they contain at least two distinct idempotents (zero and one).

If we let n be the number of idempotents in a ring R, the paragraph above proves that if n is greater than two, n is the product of two natural numbers which are each at least two, and which each represent the number of idempotents in some other ring. Since n is finite, this means we can repeatedly decompose R as a product of rings until R is expressed as a product of rings which each have exactly one or two elements, which means the number of idempotents in R is a power of 2.

4

Show that the ring $M_2(\mathbb{R})$ has infinitely many idempotents.

For any real number a, the matrix

$$A := \begin{bmatrix} 0 & 0 \\ a & 1 \end{bmatrix}$$

satisfies the equation $A^2 = A$, so there are infinitely many idempotents in $M_2(\mathbb{R})$. More generally, a real matrix is idempotent if and only if it represents a projection.

5

Describe all homomorphisms from $\mathbb{Z} \times \mathbb{Z}$ to $\mathbb{Z}$. In each case, determine the kernel and the image.

Let f be a ring homomorphism from $\mathbb{Z} \times \mathbb{Z}$ to $\mathbb{Z}$. Since the multiplicative identity in $\mathbb{Z} \times \mathbb{Z}$ is $(1, 1)$, we know that $f((1, 1)) = 1$.

Now let $x = f((1, 0))$. Since $1 = f((1, 1)) = f((1, 0) + (0, 1)) = x + f((0, 1))$, we can say that $f((0, 1)) = 1 - x$, and so for any $a, b \in \mathbb{Z}$, $f((a, b)) = xa + (1 - x)b$. Therefore f is fully defined by what x is, and x can be any integer, so every ring homomorphism $f : \mathbb{Z} \times \mathbb{Z} \to \mathbb{Z}$ can be defined by

$$f((a, b)) = ax + (1 - x)b \text{ for some integer } x.$$

For any $a \in \mathbb{Z}$, $f((a, a)) = a$, so f is surjective, so $\mathrm{Im}(f) = 0$ no matter what x is. The kernel of f is the set of pairs (a, b) for which $ax = (x - 1)b$. Below are some examples.

x	$\mathrm{Ker}(f)$
0	$\{\dots, (-1, 0), (0, 0), (1, 0), \dots\}$
1	$\{\dots, (0, -1), (0, 0), (0, 1), \dots\}$
2	$\{\dots, (-1, -2), (0, 0), (1, 2), \dots\}$
3	$\{\dots, (-2, -3), (0, 0), (2, 3), \dots\}$

6

Prove that an element a of a commutative ring R is invertible if and only if a does not belong to any maximal ideal of R.

Let a be an invertible element of R, and let I be an ideal of R which contains a. Then for any element $x \in R$, I also contains $(xa^{-1})a = x$, so $I = R$, therefore any ideal I which contains an invertible element a is not maximal.

By that same logic, if a is an element of R which is not invertible and I is an ideal of R which contains a, then $I \neq R$. Then in the poset of ideals of R, there exists a chain of ideals which includes I, and if Zorn's lemma is true, then that chain terminates in a maximal ideal, which would have to contain a.

So assuming Zorn's lemma, an element of a commutative ring is invertible if and only if it does not belong to any maximal ideal.

7

Determine all maximal and prime ideals of $\mathbb{Z}/n\mathbb{Z}$.

8

Let R be a commutative ring. The *radical* $\mathrm{Rad}(R)$ of R is the intersection of all maximal ideals in R.

- (a) Determine $\mathrm{Rad}(\mathbb{Z})$ and $\mathrm{Rad}(\mathbb{Z}/12\mathbb{Z})$.
- (b) Prove that $\mathrm{Rad}(R)$ consists of all elments $a \in R$ such that $1 + ab$ is invertible for all $b \in R$.

- (a) We proved in class that the set of maximal ideals of $\mathbb{Z}$ is the set of ideals generated by prime numbers, so a number x is only in the intersection of all ideals if it is a multiple of every prime number. Therefore $\mathrm{Rad}(\mathbb{Z}) = 0$.

  In the previous question, we showed that every maximal ideal of $\mathbb{Z}/12\mathbb{Z}$ has the form
- (b)

9

- (a) Prove that every nilradical $\mathrm{Nil}(R)$ of a commutative ring R is contained in every prime ideal of R.
- (b) Prove that $\mathrm{Nil}(R) \subset \mathrm{Rad}(R)$.

- (a) Let x be some element of the nilradical of R. Then there exists a positive integer m such that $x^m = 0$. Let P be a prime ideal of R.

  Base case: x^n is in P when $n = m$, because $x^m = 0 \in P$.

Inductive step: if x^n is in P, then since $x^n = x^{n-1}x$, either x or x^{n-1} is in P.

Since m is finite, induction is valid here, so x^n is in P for any positive integer n less than or equal to m. Therefore $x \in P$.

- (b) Every maximal ideal is prime, and we showed that if x is nilpotent, every prime ideal contains x. Therefore every maximal ideal contains every nilpotent element, so

$$\mathrm{Nil}(R) \subset \mathrm{Rad}(R).$$

10

> Let A be an abelian group (written additively). Define a product on the (additive) group $R = \mathbb{Z} \oplus A$ by $(n, a) \cdot (m, b) = (nm, nb + ma)$.
>
> - (a) Prove that R is a ring.
> - (b) Determine all prime and maximal ideals of R.

- (a) R is an abelian group under addition. R contains a multiplicative identity, which is $(1, 0)$. From the definition of the product $(\cdot)$, we see that R is also associative, left-distributive, and right-distributive.
- (b)