Math 110BH homework 1

Nathan Solomon

January 16, 2024

Due Tuesday, January 16th

1

Show that if $1 = 0$ in a ring R, then R is the zero ring.

Let a be any element of R. Then

$$a = 1a = 0a = (1-1)a = a - a = 0.$$

Since every element of R is zero, R is the zero ring.

2

Find an example of a subring of $\mathbb{Q}$ different from $\mathbb{Z}$ and $\mathbb{Q}$.

Let $\mathbb{Z}[\frac{1}{2}]$ denote the set of rational numbers which are equal to an integer divided by a power of two, called the "dyadic rationals":

$$\mathbb{Z}[\frac{1}{2}] := \left\{ \frac{x}{2^m} : x, m \in \mathbb{Z} \right\}$$

The multiplicative identity in this group is clearly the same as the multiplicative identity in $\mathbb{Q}$, so to prove that $\mathbb{Z}[\frac{1}{2}]$ is a subring of $\mathbb{Q}$, we just need to show that for any dyadic rationals a and b, $a + b$, ab, and $-a$ are also dyadic rationals.

Let x, y, m, n be integers such that $a = x/2^m$ and $b = y/2^n$. Then the following are all dyadic rationals, so $\mathbb{Z}[\frac{1}{2}]$ is a subring of $\mathbb{Q}$.

$$\begin{aligned} a + b &= \frac{2^n x + 2^m y}{2^{m+n}} \\ ab &= \frac{xy}{2^{m+n}} \\ -a &= -\frac{x}{2^m} \end{aligned}$$

$\mathbb{Z}[\frac{1}{2}]$ is not equal to $\mathbb{Z}$ because $\mathbb{Z}[\frac{1}{2}]$ contains $\frac{1}{2}$, and $\mathbb{Z}[\frac{1}{2}]$ is not equal to $\mathbb{Q}$ because $\mathbb{Z}[\frac{1}{2}]$ does not contain $\frac{1}{3}$ (there is no integer x such that $2^x/3$ is an integer).

3

Find all zero divisors in $\mathbb{Z}/m\mathbb{Z}$.

Let a be an integer which is not divisible by m. If a is coprime to m, b is an integer, and ab is an integer multiple of m, then b must also be an integer multiple of m. If a is not coprime to m, then $b = m/\gcd(a,m)$ is an integer which is not divisible by m and which makes ab an integer multiple of m. Therefore $[a]$ is a zero divisor in $\mathbb{Z}/m\mathbb{Z}$ if and only if a and m are coprime, so the set of (nonzero) zero divisors in $\mathbb{Z}/m\mathbb{Z}$ is

$$\{[a]_m : \gcd(a,m) = 1\}.$$

4

Prove that the ring $\mathrm{End}(\mathbb{Z})$ is isomorphic to $\mathbb{Z}$.

Let f be any endomorphism of $\mathbb{Z}$. Using the properties of homomorphisms and of rings, we see that $f(2) = f(1) + f(1) = 2f(1)$, and that $f(3) = 3f(1)$, and $f(-1) = -f(1)$, and so on. By induction, f is uniquely determined by $f(1)$, and f is the function which multiplies any integer by $f(1)$.

Let $h : \mathrm{End}(\mathbb{Z}) \to \mathbb{Z}$ be the map which takes f to $f(1)$. This is a homomorphism, because $h(f+g) = h(\text{multiplication by } (f+g)(1)) = h(\text{multiplication by } f(1) + g(1)) = f(1)+g(1)$, and it's invertible because for any integer x, multiplication by x is an endomorphism of $\mathbb{Z}$.

Therefore h is an isomorphism between $\mathrm{End}(\mathbb{Z})$ and $\mathbb{Z}$.

5

Show that a subring of an integral domain is an integral domain. Is it true that a subring of a field is a field?

Let R be an integral domain, and let S be a subring of R. Since R contains no nonzero zero divisors, and every element in S is in R, S also has no nonzero zero divisors. Therefore S is an integral domain.

It is not true that a subring of a field is a field – for example, the set $\mathbb{Z}[\frac{1}{2}]$ (the dyadic rationals, defined in problem 2) is a subring of the field $\mathbb{Q}$. However, $\mathbb{Z}[\frac{1}{2}]$ is not a field, since it contains 3/2 but not 2/3.

6

Prove that a finite integral domain is a field.

For any nonzero element b of a finite integral domain R, let $m_b : R \to R$ be the function defined by $m_b(a) = ab$. If a and a' are nonzero elements of R for which $m_b(a) = m_b(a')$, then

$0 = m_b(a) - m_b(a') = ab - a'b = (a - a')b$. Since b is nonzero, $a - a'$ is also nonzero. We have shown that $m_b(a) = m_b(a')$ implies $a = a'$, meaning that m_b is injective.

Since m_b is an injective function from a finite set to itself, it must also be a bijection, so $m_b^{-1}(1)$ is well-defined. In fact, $m_b^{-1}(1)$ is b^{-1}, because $bm_b^{-1}(1) = m_b(m_b^{-1}(1)) = 1$.

We have shown that every nonzero element b of a finite integral domain R is invertible. Since we already know integral domains are commutative and nonzero, this proves that every finite integral domain is a field.

7

- (a) Find a ring A such that for any ring R there is exactly one ring homomorphism $A \to R$.
- (b) Find a ring B such that for any ring R there is exactly one ring homomorphism $R \to B$.

- (a) For any ring R, suppose f is a ring homomorphism from $\mathbb{Z}$ to R. Using the properties of ring homomorphisms, we know that $f(1) = 1_R$, and also that

  $$f(0) = f(0) + f(0) - f(0) = f(0 + 0) - f(0) = f(0) - f(0) = 0.$$

  Now that we know $f(1)$ and $f(0)$, we can use the fact that f is an additive group homomorphism to see that for any nonnegative integer n, $f(n)$ is equal to 1_R added to 0_R n times, and $f(-n)$ is equal to 1_R subtracted from 0_R n times. The morphism f which is defined this way is unique, so it is the only ring homomorphism from $\mathbb{Z}$ to R.
- (b) For any ring R, the only homomorphism from R to the zero ring is the one which maps every element to zero.

8

By "an ideal", in this problem, we mean left (respectively, right or two-sided) ideal. Let $f : R \to S$ be a ring homomorphism.

- (a) Let J be an ideal of S. Show that $f^{-1}(J)$ is an ideal of R that contains $\mathrm{Ker}(f)$.
- (b) Prove that if f is surjective and I is an ideal of R, then $f(I)$ is an ideal of S. Show that the correspondence $I \mapsto f(I)$ yields a bijection between the set of all ideals of R that contain $\mathrm{Ker}(f)$ and the set of all ideals of S. Determine the inverse bijection.

- (a) (Left) ideal are, by definition, subsets of rings which contain zero, are closed under addition, and are closed under (left) multiplication by elements of the original ring. Therefore J contains zero, and so

$$\mathrm{Ker}(f) = f^{-1}(0) \subset f^{-1}(J).$$

For any homomorphism f, $f(0) = 0$, so $0 \in \mathrm{Ker}(f)$. For any two elements $a, b \in f^{-1}(J)$,

$$f(a+b) = f(a) + f(b) \in J + J \subset J$$

and, assuming we are considering left ideals for now, for any $x \in R, a \in f^{-1}(J)$,

$$f(xa) = f(x)f(a) \in f(x)J \subset J$$

which implies $xa \in f^{-1}(J)$. That last step can easily be changed to work for right or two-sided ideals instead.

This proves that $f^{-1}(J)$ is a (left) ideal of R which contains $\mathrm{Ker}(f)$.

- (b) $f(I)$ clearly contains zero, so we only need to show that $a+b$ and xa are in $f(I)$ for any $a, b \in f(I), x \in S$.

For any $a, b \in f(I)$, there exist elements $a', b' \in f^{-1}(f(I)) = I + \mathrm{Ker}(f)$ such that $f(a') = a$ and $f(b') = b$. Then $a' + b' \in I + \mathrm{Ker}(f)$, which implies $f(a' + b') = a + b$. Also, for any $x \in S$, since f is surjective, there exists an element $x' \in R$ such that $f(x') = x$, so $xa = f(x')f(a') = f(x'a') \in f(I)$. Therefore $f(I)$ is an ideal.

For any 2 ideals $I_1, I_2 \subset R$ which contain $\mathrm{Ker}(f)$, suppose $I_1 \neq I_2$. This implies $I_1/\mathrm{Ker}(f) \neq I_2/\mathrm{Ker}(f)$, so $f(I_1) \neq f(I_2)$, meaning that this map ($I \mapsto f(I)$, $\mathrm{Ker}(f) \subset I$) is injective. Also, it's surjective, because for any ideal $J \in f(I)$, $f^{-1}(J)$ is an ideal of R which contains $\mathrm{Ker}(f)$.

The inverse of the map $I \mapsto f(I)$ (for any I which contains $\mathrm{Ker}(f)$) is the function which takes any ideal of S to its preimage.

9

- (a) An element a of a ring R is called *nilpotent* if $a^n = 0$ for some $n \in \mathbb{N}$. Show that if R is a commutative ring, then the set $\mathrm{Nil}(R)$ of all nilpotent elements in R is an ideal (called the *nilradical* of R).

- (b) Prove that a polynomial $f(X) = a_0 + a_1X + \cdots + a_nX^n \in R[X]$ over a commutative ring R is nilpotent if and only if all a_i are nilpotent in R.

- (a) For any $a, b \in \text{Nil}(R)$, let m and n be natural numbers such that $a^m = 0 = b^n$. Then every term in the expansion of $(a+b)^{m+n}$ can be rewritten as $a^x b^y$ where x is at least m or y is at least n, so those terms are all zero, meaning $a + b \in \text{Nil}(R)$.

  For any $x \in R, a \in \text{Nil}(R)$, let n be a natural number such that $a^n = 0$. Then $(xa)^n = x^n a^n = 0$, so $xa \in \text{Nil}(R)$.

  Lastly, $\text{Nil}(R)$ contains 0, so it is an ideal.

- (b) If all a_is are nilpotent, then let m be a natural number such that $a_i^m = 0$ for every a_i. Then $f(X)^{mn}$ is a polynomial where every coefficient is the product of mn a_is (allowing the a_is to be repeated). By pigeonholing, for each coefficient, there is some a_i that is repeated at least m times in that product, so that coefficient is zero. Therefore $f(X)^{mn} = 0$, so $f(X)$ is nilpotent.

  If $f(X)$ is nilpotent, then there is a natural number m such that $f(X)^m = 0$. That implies the contant term of $f(X)^m$, which is a_0^m, is zero, so a_0 is nilpotent. If the degree of $f(X)$ is not zero, then consider the polynomial $(f(X) - a_0)/X$. This new polynomial has degree $n - 1$, and if it is nilpotent, then the constant term, a_1, is nilpotent. Repeating this process n times, we see that every coefficient in $f(X)$ has to be nilpotent.

10

> - (a) Prove that if a is a nilpotent element of a ring R, then the element $1+a$ is invertible. (Hint: Use the identity $1 - X^n = (1 - X)(1 + X + \cdots X^{n-1})$.)
> - (b) Prove that a polynomial $f(X) = a_0 + a_1X + \cdots + a_nX^n \in R[X]$ over a commutative ring R is invertible in $R[X]$ if and only if a_0 is invertible in R and all a_i are nilpotent in R for $i \geq 1$. (Hint: Let $g(X) = b_0 + b_1X + \cdots + b_mX^m \in R[X]$ be the inverse of $f(X)$. Prove first that $a_n^{m+1} = 0$. Then use induction.)

- (a) Let n be a natural number such that $a^n = 0$. Then $(1 + a)(1 - a + a^2 - a^3 + \cdots + (-1)^{n-1}a^{n-1}) = 1 \pm a^n = 1$, so $1 + a$ has a multiplicative inverse.

- (b) Base case (n=0): if $f(X)$ is a degree-zero polynomial, then it is invertible if and only if there is a polynomial $g(X)$ such that $f(X)g(X) = 1$. Since $f(X) = a_0$, that's equivalent to $g(X) = a_0^{-1}$, so in this case, $f(X)$ is invertible if and only if a_0 is invertible.

  Inductive step: suppose that every degree-n polynomial over R is invertible if and only if a_0 is invertible and all other a_is are nilpotent. Then let $g(X) = b_0 + b_1X + b_2X^2 + \cdots + b_mX^m$ be the inverse of $f(X)$. The highest-order term of $f(X)g(X)$ is then $a_nb_mX^{n+m}$, so if $n \geq 1$, $a_nb_m = 0$. STILL NEED TO FINISH THIS PROBLEM.