110A HW3

Warren Kim

Winter 2024

Question 1

Let R be a ring. Show that $1 = 0$ if and only if $R = \{0\}$.

Response

Proof: ($\implies$) Let R be a ring and suppose $1 = 0$. Then, for any $a \in R$, we can write $a = 1 \cdot a = a \cdot 1$. But since $1 = 0$, we have $a = 0 \cdot a = a \cdot 0 = 0$, so $a = 0$. Because a was arbitrary, $a = 0$ is the only element in R.
($\impliedby$) Let R be a ring and let it be defined by $R = \{0\}$. Then, because it's a ring, there exists an element $1_R \in R$ such that $1_R \cdot a = a \cdot 1_R = a$ for any $a \in R$. Because 0 is the only element in R, set $1_R = 0$. Then, since 0 is the only element in R, we have that $a = 0$, so $a \cdot 1_R = 1_R \cdot a = 0 = a = 0 \cdot a = a \cdot 0$. $\square$

Question 2

Let R be a ring, and consider the associated polynomial ring $R[x]$.

1. Show that R is commutative if and only if $R[x]$ is commutative.
2. Suppose R is commutative. Show that R is an integral domain if and only if $R[x]$ is an integral domain.

Response

1. Show that R is commutative if and only if $R[x]$ is commutative.

   Proof: ($\implies$) Suppose R is a commutative ring. Then, consider the associated polynomial ring $R[x]$. Note that x is commutative with all $a \in R$; i.e. $ax = xa$. Then, suppose we have two elements $\sum_{i=0}^{n} a_i x^i, \sum_{j=0}^{m} b_j x^j \in R[x]$ for some $n, m \in \mathbb{Z}_{>0}$. Then

   $$\begin{aligned}
   \left(\sum_{i=0}^{n} a_i x^i\right)\left(\sum_{j=0}^{m} b_j x^j\right) &= \sum_{i=0}^{n}\sum_{j=0}^{m} a_i x^i b_j x^j \\
   &= \sum_{i=0}^{n}\sum_{j=0}^{m} x^i a_i b_j x^j && a_i x^i = x^i a_i \\
   &= \sum_{i=0}^{n}\sum_{j=0}^{m} (a_i b_j) x^i x^j && a_i x^i = x^i a_i \\
   &= \sum_{i=0}^{n}\sum_{j=0}^{m} (a_i b_j) x^{i+j} && x^i x^j = x^{i+j} \\
   &= \sum_{i=0}^{n}\sum_{j=0}^{m} (b_j a_i) x^{j+i} && R \text{ is commutative} \\
   &= \left(\sum_{j=0}^{m} b_j x^j\right)\left(\sum_{i=0}^{n} a_i x^i\right)
   \end{aligned}$$

   so $R[x]$ is commutative.
   ($\impliedby$) Suppose $R[x]$ is a commutative ring. Then given two elements $\sum_{i=0}^{n} a_i x^i, \sum_{j=0}^{m} b_j x^j \in R[x]$ for some $n, m \in \mathbb{Z}_{>0}$, we have that for any $i < n$ and $j < m$, $(a_i x^i)(b_j x^j) = (b_j x^j)(a_i x^i)$. Then

   $$\begin{aligned}
   (a_i b_j) x^{i+j} &= (x^i a_i) b_j x^j && a_i x^i = x^i a_i \\
   &= a_i x^i b_j x^j && a_i x^i = x^i a_i \\
   &= b_j x^j a_i x^i && (a_i x^i)(b_j x^j) = (b_j x^j)(a_i x^i) \\
   &= x^j b_j a_i x^i && a_i x^i = x^i a_i \\
   (a_i b_j) x^{i+j} &= (b_j a_i) x^{j+i} && a_i x^i = x^i a_i
   \end{aligned}$$

   So, $a_i b_j = b_j a_i$, and since $a_i, b_j \in R$ were arbitrary, R is commutative. $\square$

2. Suppose R is commutative. Show that R is an integral domain if and only if $R[x]$ is an integral domain.

Proof: Suppose R is commutative.
($\Longrightarrow$) Let R be an integral domain. Then, for any nonzero $a, b \in R$, we have $ab \neq 0$. Now, consider nonzero $\sum_{i=0}^{n} a_i x^i, \sum_{j=0}^{m} b_j x^j \in R[x]$ for some $n, m \in \mathbb{Z}_{>0}$. Then

$$\left(\sum_{i=0}^{n} a_i x^i\right) \cdot \left(\sum_{j=0}^{m} b_j x^j\right) = \sum_{i=0}^{n} \sum_{j=0}^{m} (a_i b_j) x^{i+j} \neq 0$$

because $a_i b_j \neq 0$ if a_i, b_j are nonzero, so $R[x]$ is an integral domain.
($\Longleftarrow$) Let $R[x]$ be an integral domain. Then, consider nonzero $a, b \in R$. Then define $a_0 := a, b_0 := b \in R[x]$ where a_0, b_0 are the zero polynomials. Since $R[x]$ is an integral domain, $a_0 b_0 \neq 0$. but $a_0 = a, b_0 = b$, so $ab \neq 0$ for any nonzero $a, b \in R$. $\square$

Question 3

Prove the parts of Proposition 2.1 (in the notes) that were not proved in class.

Response

4. The multiplicative identity is unique.

Proof: Let R be a ring. Suppose we have two identities $1_1, 1_2 \in R$. Then, we have the following: $1_1 = 1_1 \cdot 1_2 = 1_2 \cdot 1_1 = 1_2$, so $1_1 = 1_2$. □

5. If a is a unit, its inverse is unique.

Proof: Let R be a ring and $a \in R$ be a unit. Suppose there exist $a_1^{-1}, a_2^{-2} \in R$ such that a_1^{-1}, a_2^{-2} are inverses of a. Then, we have the following: $aa_1^{-1} = 1 = aa_2^{-1}$, so $aa_1^{-1} = aa_2^{-1}$ and since a is nonzero, $a_1^{-1} = a_2^{-1}$ by the cancellation property. □

8. $-(-a) = a$.

Proof: Let R be a ring and $a \in R$. Then,

$$\begin{aligned} -(-a) &= 0 - (-a) \\ &= (a + (-a)) + (-(-a)) \\ &= a + ((-a) - (-a)) && a - b = a + (-b) \\ &= a + 0 \\ -(-a) &= a \end{aligned}$$

□

9. $-(a + b) = -a - b$.

Proof: Let R be a ring and $a, b \in R$. Then,

$$\begin{aligned} -(a+b) &= 0 - (a+b)) \\ &= 0 + 0 - (a+b)) \\ &= (a-a) + (-b+b) - (a+b) \\ &= a + (-a-b) + b - (a+b) && a - b = a + (-b) \\ &= (-a-b) + (a+b) - (a+b) \\ &= (-a-b) + 0 \\ -(a+b) &= -a - b \end{aligned}$$

□

10. $-(a - b) = -a + b$.

Proof: Let R be a ring and $a, b \in R$. Then,

$$\begin{aligned} -(a-b) &= -(a+(-b)) \\ &= -a-(-b) && -(a+b) = -a-b \\ -(a-b) &= -a+b && -(-a) = a \end{aligned}$$

□

11. $(-a)(-b) = ab$.

Proof: Let R be a ring and $a, b \in R$. Then,

$$\begin{aligned} (-a)(-b) &= a(-(-b)) && -ab = a(-b) \\ (-a)(-b) &= ab && -(-a) = a \end{aligned}$$

□

Question 4

Let R and S be rings, and let $f : R \to S$ be a ring homomorphism. Let $a, b \in R$. Prove the following:

1. $f(a-b) = f(a) - f(b)$.
2. If $a \in R$ is a unit, then $f(a)$ is a unit as well, with $f(a^{-1}) = f(a)^{-1}$.

Response

1. $f(a-b) = f(a) - f(b)$.

   Proof: Let R, S be rings, $f : R \to S$ a ring homomorphism, and $a, b \in R$. Then,

$$\begin{aligned} f(a-b) &= f(a+(-b)) \\ &= f(a) + f(-b) \\ &= f(a) + f((-1_R) \cdot b) && -a = 1(-a) = -1a = (-1)a \\ &= f(a) + f((-1_R)) \cdot f(b) && f(ab) = f(a) \cdot f(b) \\ &= f(a) + (-1_S) \cdot f(b) && f(1_R) = 1_S \\ f(a-b) &= f(a) - f(b) \end{aligned}$$

   □

2. If $a \in R$ is a unit, then $f(a)$ is a unit as well, with $f(a^{-1}) = f(a)^{-1}$.

   Proof: Let R, S be rings, $f : R \to S$ a ring homomorphism, and $a \in R$ be a unit. Then,

$$\begin{aligned} 1_S &= f(1_R) \\ &= f(aa^{-1}) && 1_R = aa^{-1} \\ 1_S &= f(a) \cdot f(a^{-1}) && f(ab) = f(a) \cdot f(b) \end{aligned}$$

   and

$$\begin{aligned} 1_S &= f(1_R) \\ &= f(a^{-1}a) && 1_R = aa^{-1} \\ 1_S &= f(a^{-1}) \cdot f(a) && f(ab) = f(a) \cdot f(b) \end{aligned}$$

   so $f(a)f(a^{-1}) = f(a^{-1})f(a) = 1_S$. Therefore, $f(a)$ is a unit and define $f(a)^{-1} := f(a^{-1})$, so $f(a^{-1}) = f(a)^{-1}$. □

Question 5

Consider the Gaussian integers, given by $\mathbb{Z}[i] = \{a+bi|a, b \in \mathbb{Z}\}$, where $i^2 = -1$. Consider the map $f : \mathbb{Z}[i] \to \mathbb{Z}[i]$ where $a + bi \mapsto a - bi$. Show f is an isomorphism.

Response

Proof: Let $\mathbb{Z}[i] = \{a + bi : a, b \in \mathbb{Z}\}$ where $i^2 = -1$ and define $f : \mathbb{Z}[i] \to \mathbb{Z}[i]$, $a + bi \mapsto a - bi$. Then

1. $1 \in \mathbb{Z}[i]$: Take $1 \in Z[i]$. Then, $f(1) = f(1 + 0i) = 1 - 0i = 1$.

2. Closure under addition: Consider $a + bi, c + di \in \mathbb{Z}[i]$. Then

$$\begin{aligned} f((a + bi) + (c + di)) &= f(a + bi + c + di) \\ &= f(a + c + bi + di) \\ &= f((a + c) + (b + d)i) \\ &= (a + c) - (b + d)i \\ &= a + c - bi - di \\ &= (a - bi) + (c - di) \\ f((a + bi) + (c + di)) &= f(a + bi) + f(c + di) \end{aligned}$$

3. Closure under multiplication Consider $a + bi, c + di \in \mathbb{Z}[i]$. Then

$$\begin{aligned} f((a + bi) \cdot (c + di)) &= f(ac + bci + adi + bdi^2) \\ &= f(ac + bci + adi - bd) \\ &= f((ac - bd) + (bc + ad)i) \\ &= (ac - bd) - (bc + ad)i \\ &= ac - bd - bci - adi \\ &= ac - bci - adi + bdi^2 \\ &= c(a - bi) - di(a - bi) \\ &= (a - bi) \cdot (c - di) \\ f((a + bi) \cdot (c + di)) &= f(a + bi) \cdot f(c + di) \end{aligned}$$

(1) - (3) show that f is a homomorphism. To show that f is an isomorphism, consider $f : \mathbb{Z}[i] \to \mathbb{Z}[i]$, $f^{-1} := f$. Then for $a + bi \in \mathbb{Z}[i]$, $f(f^{-1}(a + bi)) = f(a - bi) = a + bi = f^{-1}(a - bi) = f^{-1}(f(a + bi))$. So, f is an isomorphism. $\square$

Question 6

Let R be a ring. We say that $a \in R$ is nilpotent if there is some integer n such that $a^n = 0$. Show that $1 + a$ is a unit.

Response

Proof: Let R be a ring and suppose $a \in R$ is nilpotnet; i.e. there is some integer n such that $a^n = 0$. Then, since R is a ring, $1 \in R$. Consider the elements $(1 + a), \sum_{i=0}^{n-1}(-1)^i a^i \in R$. Then

$$\begin{aligned}
(1+a)\left(\sum_{i=0}^{n-1}(-1)^i a^i\right) &= 1 \cdot \left(\sum_{i=0}^{n-1}(-1)^i a^i\right) + a \cdot \left(\sum_{i=0}^{n-1}(-1)^i a^i\right) \\
&= \left(\sum_{i=0}^{n-1}(-1)^i a^i\right) + \left(\sum_{i=0}^{n-1}(-1)^i a^{i+1}\right) \\
&= (1 - a + a^2 - \cdots + (-1)^{n-1}a^{n-1}) + (a - a^2 + a^3 - \cdots + (-1)^{n-2}a^{n-1} + (-1)^{n-1}a^n) \\
&= 1 + (-a + a) + (a^2 - a^2) + \cdots + ((-1)^{n-1}a^{n-1} + (-1)^{n-2}a^{n-1}) + (-1)^{n-1}a^n \\
&= 1 + 0 + 0 + \cdots + 0 + (-1)^{n-1}a^n \\
&= 1 + (-1)^{n-1}a^n \\
&= 1 + 0 \\
(1+a)\left(\sum_{i=0}^{n-1}(-1)^i a^i\right) &= 1
\end{aligned}$$

and

$$\begin{aligned}
\left(\sum_{i=0}^{n-1}(-1)^i a^i\right)(1+a) &= \left(\sum_{i=0}^{n-1}(-1)^i a^i\right) \cdot 1 + \left(\sum_{i=0}^{n-1}(-1)^i a^i\right) \cdot a \\
&= \left(\sum_{i=0}^{n-1}(-1)^i a^i\right) + \left(\sum_{i=0}^{n-1}(-1)^i a^{i+1}\right) \\
&= (1 - a + a^2 - \cdots + (-1)^{n-1}a^{n-1}) + (a - a^2 + a^3 - \cdots + (-1)^{n-2}a^{n-1} + (-1)^{n-1}a^n) \\
&= 1 + (-a + a) + (a^2 - a^2) + \cdots + ((-1)^{n-1}a^{n-1} + (-1)^{n-2}a^{n-1}) + (-1)^{n-1}a^n \\
&= 1 + 0 + 0 + \cdots + 0 + (-1)^{n-1}a^n \\
&= 1 + (-1)^{n-1}a^n \\
&= 1 + 0 \\
\left(\sum_{i=0}^{n-1}(-1)^i a^i\right)(1+a) &= 1
\end{aligned}$$

so $1 + a$ is a unit. □

Question 7

We say that a ring R is a Boolean ring if, for every $a \in R$, we have $a^2 = a$.

1. Show that a Boolean ring R is commutative.
2. Suppose R is a Boolean ring and an integral domain. Show that $|R| = 2$. [Hint: show that any nonzero element must be 1.]

Response

1. Show that a Boolean ring R is commutative.

   Proof: To show that a Boolean ring R is commutative, we will first show that for any $a \in R$, $a = -a$. Since R is a Boolean ring, we have that $-a \in R$ and $a^2 = a$. Then, $(-a)^2 = (-a)(-a) = a^2$, so $-a = a$. Because equality is symmetric, $a = -a$. Now consider $a + b \in R$. Then

   $$\begin{aligned} a + b &= (a + b)^2 \\ &= a^2 + ab + ba + b^2 \\ &= a + ab + ba + b \\ (a - a) + (b - b) &= (a - a) + ab + ba + (b - b) \\ 0 &= ab + ba \\ 0 &= ab - ba && a = -a \end{aligned}$$

   so $ab = ba$. □

2. Suppose R is a Boolean ring and an integral domain. Show that $|R| = 2$.

   Proof: Suppose R is a Boolean ring and an integral domain. Let $a \in R$ be nonzero. Since R is a Boolean ring, $a^2 = a$. Then

   $$\begin{aligned} a^2 &= a \\ a^2 - a &= 0 \\ a(a - 1) &= 0 \end{aligned}$$

   Because R is an integral domain, $a = 0$ or $a = 1$, but because a is chosen to be nonzero, $a = 1$. Since a was arbitrary, this holds for all $a \in R$. Because R is a ring, $0 \in R$. Set $1_R = 1 \in R$. Then, $R := \{0, 1\}$, so $|R| = 2$. □

Question 8

Let R and S be rings. Show that if R and S are isomorphic, then $R[x]$ and $S[x]$ are isomorphic.

Response

Proof: Let R, S be rings. Suppose $R \simeq S$. Then, there exists a bijection $f : R \to S$. Consider the function $g : R[x] \to S[x]$ defined by $\sum_{i=0}^{n} a_i x^i \mapsto \sum_{i=0}^{n} f(a_i)x^i$

Consider two polynomials $\sum_{i=0}^{n} a_i x^i, \sum_{j=0}^{m} b_j x^j \in R[x]$ for some $n, m \in \mathbb{Z}_{>0}$.

1. Closure under addition: Without loss of generality, assume $m \leq n$ and set $b_i = 0$ for $m < i \leq n$. Then

$$\begin{aligned} g\left(\sum_{i=0}^{n} a_i x^i + \sum_{i=0}^{n} b_i x^i\right) &= g\left(\sum_{i=0}^{n} (a_i + b_i)x^i\right) \\ &= \sum_{i=0}^{n} f(a_i + b_i)x^i \\ &= \sum_{i=0}^{n} (f(a_i) + f(b_i))x^i \\ &= \sum_{i=0}^{n} \left(f(a_i)x^i + f(b_i)x^i\right) \\ &= \sum_{i=0}^{n} f(a_i)x^i + \sum_{i=0}^{n} f(b_i)x^i \\ g\left(\sum_{i=0}^{n} a_i x^i + \sum_{i=0}^{n} b_i x^i\right) &= g\left(\sum_{i=0}^{n} a_i x^i\right) + g\left(\sum_{i=0}^{n} b_i x^i\right) \end{aligned}$$

   so g is closed under addition.

2. Closure under multiplication:

$$\begin{aligned}
g\left(\left(\sum_{i=0}^{n} a_i x^i\right)\left(\sum_{j=0}^{m} b_j x^j\right)\right) &= g\left(\sum_{i=0}^{n}\sum_{j=0}^{m} a_i x^i b_j x^j\right) \\
&= g\left(\sum_{i=0}^{n}\sum_{j=0}^{m} x^i a_i b_j x^j\right) && a_i x^i = x^i a_i \\
&= \sum_{i=0}^{n}\sum_{j=0}^{m} x^i f(a_i b_j) x^j \\
&= \sum_{i=0}^{n}\sum_{j=0}^{m} x^i f(a_i)\cdot f(b_j) x^j \\
&= \sum_{i=0}^{n}\sum_{j=0}^{m} f(a_i) x^i \cdot f(b_j) x^j && f(a_i)x^i = x^i f(a_i) \\
&= \left(\sum_{i=0}^{n} f(a_i) x^i\right)\cdot\left(\sum_{j=0}^{m} f(b_j) x^j\right) \\
&= g\left(\sum_{i=0}^{n} a_i x^i\right)\cdot g\left(\sum_{j=0}^{m} b_j x^j\right)
\end{aligned}$$

   so g is closed under multiplication.

3. $g(1_{R[x]}) = 1_{S[x]}$:

$$g(1_{R[x]}) = f(1_R) = 1_S = 1_{S[x]}$$

   so the multiplicative identity exists.

so g is a homomorphism. To show that g is an isomorphism, consider $g^{-1} : S[x] \to R[x]$, $\sum_{i=0}^{n} a_i x^i \mapsto \sum_{i=0}^{n} f^{-1}(a_i) x^i$ where $f^{-1} : S \to R$ is the inverse of f. Then for all $\sum_{i=0}^{n} a_i x^i \in R[x]$

$$g^{-1}\left(g\left(\sum_{i=0}^{n} a_i x^i\right)\right) = g^{-1}\left(\sum_{i=0}^{n} f\left(a_i\right) x^i\right) = \sum_{i=0}^{n} f^{-1}\left(f\left(a_i\right)\right) x^i = \sum_{i=0}^{n} a_i x^i$$

and for all $\sum_{i=0}^{n} b_i x^i \in S[x]$ we have

$$g\left(g^{-1}\left(\sum_{i=0}^{n} b_i x^i\right)\right) = g\left(\sum_{i=0}^{n} f^{-1}\left(b_i\right) x^i\right) = \sum_{i=0}^{n} f\left(f^{-1}\left(b_i\right)\right) x^i = \sum_{i=0}^{n} b_i x^i$$

so g is an isomorphism and therefore $R[x]$ and $S[x]$ are isomorphic. □