Team Number: 201

PUMaC 2022* Power Round Cover Sheet

Notes: Remember that this sheet comes first in your solutions. You should submit solutions for the problems in increasing order. Write on one side of the page only. The start of a solution to a problem should start on a new page. Please mark which questions for which you submitted a solution to help us keep track of your solutions.

Problem Number	Points	Attempted?
1.1.1	15	Yes
1.1.2	5	Yes
1.1.3	5	Yes
1.1.4	5	Yes
1.1.5	10	Yes
1.1.6	5	Yes
1.2.1	10	Yes
1.2.2	5	
1.2.3	10	Yes
1.2.4	10	
1.2.5	10	
1.3.1	10	Yes
1.3.2	10	Yes
1.3.3	25	Yes
1.3.4	10	Yes
2.1.1	10	Yes
2.1.2	10	Yes
2.2.1	10	Yes
2.2.2	20	Yes
2.2.3	10	Yes
2.2.4	10	Yes
2.2.5	20	Yes
2.2.6	5	
2.2.7	10	Yes
2.3.1	15	Yes
2.3.2	5	Yes
2.3.3	15	
2.3.4	10	
2.3.5	15	Yes
2.3.6	10	
2.4.1	15	Yes
2.4.2	10	
2.4.3	15	

Problem Number	Points	Attempted?
2.4.4	30	
2.4.5	10	Yes
2.4.6	10	Yes
2.4.7	25	Yes
2.4.8	20	
3.0.1	5	Yes
3.0.2	15	Yes
3.0.3	10	Yes
3.0.4	20	Yes
4.1.1	30	Yes
4.1.2	25	Yes
4.1.3	15	Yes
4.1.4	25	Yes
4.1.5	40	Yes
4.2.1	10	Yes
4.2.2	15	Yes
4.2.3	20	Yes
4.2.4	25	Yes
4.2.5	30	
4.3.1	10	
4.3.2	5	
4.3.3	40	
4.3.4	30	
5.1.1	25	
5.2.1	25	
5.2.2	10	
5.2.3	15	
5.2.4	20	
5.2.5	15	
5.3.1	15	
5.3.2	10	
5.3.3	30	
5.3.4	10	

Contents

1 Problem 1.1.1

Proof. 1. In $2\mathbb{Z}$, there does not exist multiplicative identity 1.

2. We can show that $\mathbb{C}[x]$ has all the ring's properties:

   - $\mathbb{C}[x]$ is closed under addition and multiplication
   - Addition in $\mathbb{C}[x]$ is adding the coefficients together, which does not change the degree. Suppose $i_1, i_2 \in \mathbb{C}[x]$ such that $i_1 = a_1 + b_1x$ and $i_2 = a_2 + b_2x$. We have $i_1 + i_2 = (a_1+a_2)+(b_1+b_2)x \in \mathbb{C}[x]$, and $i_1i_2 = (a_1+b_1x)(a_2+b_2x) = (a_1a_2+x^2b_1b_2)+(a_1b_2+a_2b_1)x$. Both the sum and multiplication of i_1, i_2 lie in $\mathbb{C}[x]$, so $\mathbb{C}[x]$ is closed under addition and multiplication.
   - For each element i in $\mathbb{C}[x]$, we can always find an element i' such that $i + (i') = 0$.
   -

□

2 Problem 1.1.2

Proof. We can show that $\mathbb{Z}/n\mathbb{Z}$ is a ring because it has all the properties.

- $\mathbb{Z}/n\mathbb{Z}$ is closed under addition and multiplication
  - Based on the definition of $\mathbb{Z}/n\mathbb{Z}$, $\mathbb{Z}/n\mathbb{Z}$ only has {0,1,. . . ,n-1} because they are the remainders after divided by n. $\forall a, b \in \mathbb{Z}$, $a + b$ and ab must $\in${0,1,. . . ,n-1}after divided by n, which they are both inZ/nZ.Therefore, $\mathbb{Z}/n\mathbb{Z}$ is closed under addition and multiplication.
- Addition and multiplication are associative in $\mathbb{Z}/n\mathbb{Z}$
  - *Addition*: $\forall a, b \in \mathbb{R}, a + b = b + a$.Therefore, a+b=b+a in $\mathbb{Z}/n\mathbb{Z}$ because they have the same remainder divided by n.
    $Multiplication$: $\forall a, b \in \mathbb{R}, ab = ba$.Therefore, ab=ba in $\mathbb{Z}/n\mathbb{Z}$ because they have the same remainder divided by n.

– The same reason applies to the commutative property.

–

□

3 Problem 1.1.3

Proof. Because R is the ring, it has the multiplicative identity 1. Because 1 is in the ring, the additive inverse -1 must be in the ring. The element $x \in \mathbb{R}$ such that $r+xr = 1 \cdot r + x \cdot r = (1+x)r = 0$ is the additive inverse of the multiplicative identity = -1. □

4 Problem 1.1.4

Proof. Suppose that the set of odd integers I, as a subset of $\mathbb{Z}$, is an ideal. We know $1 \in I$ and $2 \in \mathbb{Z}$. However, $1 \cdot 2 \notin I$. Therefore, it does not hold the second property of Definition 1.1.3 and is not an ideal. □

5 Problem 1.1.5

Proof. All the prime ideals are $\langle x-a\rangle, a \in \mathbb{C}$
Since, according to the theorem that any nonconstant polynomials in $\mathbb{C}$ can be written as a product of linear factors, $ab \in \langle x-a\rangle$ if and only if a or b is divisible by $\langle x-a\rangle$ □

6 Problem 1.1.6

Proof. 1.) $S = \{x \in \mathbb{R} | x < 0\}$ and $S' = \{x \in \mathbb{R} | x > 0\}$
Suppose $f(s) = f(t)$, we have $\mid s \mid = \mid t \mid$, $s < 0$, and $t < 0$. So, $s = t$
Therefore, the function is **injective**.
For all $a \in \mathbb{R}^+$, There is $-a \in \mathbb{R}^-$ such that $f(-a) = a$
Therefore, the function is **surjective**.

2.) $f(x) = e^x$ never reach the negative value, therefore, the function is **not surjective**.
Suppose $f(s) = f(t)$, we have $e^s = e^t$, $e^{s-t} = 1$, $s - t = 0$, $s = t$.
Therefore, the function is **injective**.

3.) For $f(x) = sin(x) = 0$, there are more than solutions in $[0, 2\pi]$, which is $0, \pi, 2\pi$.
Therefore, the function is **not injective**.
Because the range of $sin(x)$ for $x \in [0, 2\pi]$ is $[-1, 1]$, the function is **surjective**. □

7 Problem 1.2.1

Proof. As the example in page 7 already shown that $r = a+b\sqrt{2}$ is a ring. We will further show that it is also a field. For $r = a + b\sqrt{2} \in R$, where $a, b \in \mathbb{Q}$, $\frac{1}{r} = \frac{a - b\sqrt{2}}{a^2 - 2b^2} = \frac{a}{a^2 - 2b^2} + \frac{b}{2b^2 - a^2}\sqrt{2} \in R$ Therefore, $r = a + b\sqrt{2}$ is a field. □

8 Problem 1.2.2

Proof. (write your solution here) □

9 Problem 1.2.3

Proof. consider the smallest positive element in I, say i. Assume that there is an element j that is not divisible by i. We can write $j = ai + b$ when $0 < b < i$. Because $-1 \in \mathbb{Z}$, we also have that $-i$ is in I.
If $a > 0$, We have $j + (-i) \in I, ..., j + a(-i) = b \in I$
If $a < 0$, We have $j + i \in I, ..., j + (-a)i = b \in I$
If $a = 0$, We have $b \in I$
which contradicts the assumption that i is the smallest positive element in I
Therefore, there does not exist j that is not divisible by i.
Because of this, every element in I can be generated by i (the smallest positive element in I).
$\mathbb{Z}$ is a PID. □

10 Problem 1.2.4

Proof. (write your solution here) □

11 Problem 1.2.5

Proof. (write your solution here) □

12 Problem 1.3.1

Proof. If $r_1 + I = r_1' + I$, $r_2 + I = r_2' + I$, then $r_1' = r_1 + i_1'$, $r_2' = r_2 + i_2'$ for some $i_1', i_2' \in I$. Suppose $r_1 + r_2 + i \in (r_1 + I) + (r_2 + I) = (r_1 + r_2) + I$, where $i \in I$. Then $r_1 + r_2 + i = (r_1' + r_2') + (i - i_1' - i_2')) \in (r_1' + r_2') + I = (r_1' + I) + (r_2' + I)$. Hence, $(r_1 + I) + (r_2 + I) \subseteq (r_1' + I) + (r_2' + I)$. Similarly, $(r_1' + I) + (r_2' + I) \subseteq (r_1 + I) + (r_2 + I)$. Hence, $(r_1 + I) + (r_2 + I) = (r_1' + I) + (r_2' + I)$.

Moreover, if $r_1 r_2 + i \in (r_1 + I) + (r_2 + I) = (r_1 r_2) + I$, then $r_1 r_2 + i = (r_1' - i_1')(r_2' - i_2') + i = r_1' r_2' + (i - i_1' r_2' - i_2'(r_1' + i_1')) \in (r_1' r_2') + I = (r_1' + I) \cdot (r_2' + I)$. Hence $(r_1 + I) \cdot (r_2 + I) \subseteq (r_1' + I) \cdot (r_2' + I)$. Similarly, $(r_1' + I) \cdot (r_2' + I) \subseteq (r_1 + I) \cdot (r_2 + I)$. Hence, $(r_1 + I) \cdot (r_2 + I) = (r_1' + I) \cdot (r_2' + I)$. □

13 Problem 1.3.2

Proof. If $r_1 + I, r_2 + I \in R/I$, then $(r_1 + I) + (r_2 + I) = (r_1 + r_2) + I$, $(r_1 + I)(r_2 + I) = (r_1 r_2) + I$. Hence, all the properties of addition and multiplication of R carries down over to R/I. Define 0 in R/I to be $0 + I = I$ and 1 to be $1 + I$. Then R/I is a ring. □

14 Problem 1.3.3

Proof. 1. If $i, i' \in I_1 \cap I_2$, then $i + i' \in I_1$, $i + i' \in I_2$, so $i + i' \in I_1 \cap I_2$. If $i \in I_1 \cap I_2$, $r \in R$, then $ri \in I_1$, $ri \in I_2$, so $ri \in I_1 \cap I_2$. Hence, $I_1 \cap I_2$ is an ideal.

2. Let $\phi : R/(I_1 \cap I_2) \longrightarrow (R/I_1) \times (R/I_2)$, $r + I_1 \cap I_2 \rightsquigarrow (r + I_1, r + I_2)$. Let $(r + I_1, r + I_2) = (r' + I_1, r' + I_2)$ if and only if $r + I_1 = r' + I_1$ and $r + I_2 = r' + I_2$ if $r + I_1 \cap I_2 = r' + I_1 \cap I_2$. Hence, ϕ is well-defined. It is a homomorphism since $\phi((r_1 + I_1 \cap I_2) + (r_2 + I_1 \cap I_2)) = \phi(r_1 + I_1 \cap I_2) + \phi(r_2 + I_1 \cap I_2)$ and $\phi(r(r_1 + I_1 \cap I_2)) = r\phi(r_1 + I_1 \cap I_2)$.

3. $(r + I_1, r + I_2) = 0$ if and only if $r \in I_1 \cap I_2$, which implies that $r + I_1 \cap I_2 = I_1 \cap I_2$. Therefore, the kernal of ϕ contains only the zero element, so ϕ is injective.

4. Since $I_1 + I_2 = R$, $1 = i_1 + i_2$ for some $i_1 \in I_1, i_2 \in I_2$. $(i_1 + i_2)r_1 = r_1 = i_1 r_1 + i_2 r_1$, but since $i_1 r_1 \in I_1$, we also have $i_2 r_1 \in r_1 + I_1$. Similarly, $i_1 r_2 \in r_2 + I_2$. Consider $r = i_2 r_1 + i_1 r_2$. Since $i_1 r_2 \in I_1$, $i_2 r_1 \in r_1 + I_1$, we have $r \in r_1 + I_1$. Similarly, $r \in r_2 + I_2$. Therefore, $\phi(r + (I_1 \cap I_2)) = (r + I_1, r + I_2) = (r_1 + I_1, r_2 + I_2)$. This shows that ϕ is surjective.

□

15 Problem 1.3.4

Proof. Let $I_1 = \langle m \rangle$, $I_2 = \langle n \rangle$. If m, n are relatively prime, then $I_1 + I_2 = \mathbb{Z}$ and $I_1 \cap I_2 = \langle mn \rangle$. By the previous problem, there is a bijection ϕ from $\mathbb{Z}/(I_1 \cap I_2)$ to $(R/I_1) \times (R/I_2)$ that takes $r + I_1 \cap I_2$ to $(r + I_1, r + I_2)$. Hence, there is a unique r such that $\phi(r + I_1 \cap I_2) = (r_1 + I_1, r_2 + I_2)$. This r is the unique residue (mod mn), as desired. □

16 Problem 2.1.1

Proof. 1.)
Let v_1, v_2, and v_3 be polynomials with complex coefficients and V is the set of polynomials with complex coefficients.
Let $v_1 = a_n \cdot x^n + ... + a_2 \cdot x^2 + a_1 \cdot x + a_0$, $v_2 = b_n \cdot x^n + ... + b_2 \cdot x^2 + b_1 \cdot x + b_0$, and $v_3 = c_n \cdot x^n + ... + c_2 \cdot x^2 + c_1 \cdot x + c_0$.

property 1:
$v_1 + v_2 = (a_n + b_n) \cdot x^n + ... + (a_2 + b_2) \cdot x^2 + (a_1 + b_1) \cdot x + (a_0 + b_0)$
For $s \in \mathbb{C}$, $s \cdot v_1 = (s \cdot a_n) \cdot x^n + ... + (s \cdot a_2) \cdot x^2 + (s \cdot a_1) \cdot x + (s \cdot a_0)$
Because $\mathbb{C}$ is closed under addition and scalar multiplication, $v_1 + v_2 \in V$ and $s \cdot v_1 \in V$.

property 2: $(v_1 + v_2) + v_3 = v_1 + (v_2 + v_3) = (a_n + b_n + c_n) \cdot x^n + ... + (a_2 + b_2 + c_3) \cdot x^2 + (a_1 + b_1 + c_1) \cdot x + (a_0 + b_0 + c_0)$
$s_1 \cdot (s_2 \cdot v_1) = (s_1 \cdot s_2) \cdot v_1 = s_1 \cdot s_2 \cdot a_n \cdot x^n + ... + s_1 \cdot s_2 \cdot a_2 \cdot x^2 + s_1 \cdot s_2 \cdot a_1 \cdot x + s_1 \cdot s_2 \cdot a_3$

property 3: $v_1 + v_2 = v_2 + v_1$ because the coefficients are in the set of complex numbers which have commutative property.

property 4: 0 is the identity element for $+$

property 5: The additive inverse is the polynomial with all the coefficients being additive inverses of those of initial polynomial.

property 6: 1 is the identity element for $\cdot$

property 7: Because the coefficients are in $\mathbb{C}$, the polynomials also follow the distributive law.

2.)
property 1:
$v_1 + v_2 = (a_n + b_n) \cdot x^n + ... + (a_2 + b_2) \cdot x^2 + (a_1 + b_1) \cdot x + (a_0 + b_0)$
For $s \in \mathbb{Q}$, $s \cdot v_1 = (s \cdot a_n) \cdot x^n + ... + (s \cdot a_2) \cdot x^2 + (s \cdot a_1) \cdot x + (s \cdot a_0)$
Because $\mathbb{R} \cdot \mathbb{Q} \in \mathbb{R}$ and $\mathbb{R}$ is closed under addition, $v_1 + v_2 \in V$ and $s \cdot v_1 \in V$.

property 2: $(v_1 + v_2) + v_3 = v_1 + (v_2 + v_3) = (a_n + b_n + c_n) \cdot x^n + ... + (a_2 + b_2 + c_3) \cdot x^2 + (a_1 + b_1 + c_1) \cdot x + (a_0 + b_0 + c_0)$
$s_1 \cdot (s_2 \cdot v_1) = (s_1 \cdot s_2) \cdot v_1 = s_1 \cdot s_2 \cdot a_n \cdot x^n + ... + s_1 \cdot s_2 \cdot a_2 \cdot x^2 + s_1 \cdot s_2 \cdot a_1 \cdot x + s_1 \cdot s_2 \cdot a_3$

property 3: $v_1 + v_2 = v_2 + v_1$ because the coefficients are in the set of real numbers which have commutative property.

property 4: 0 is the identity element for $+$

property 5: The additive inverse is the polynomial with all the coefficients being additive inverses of those of initial polynomial.

property 6: 1 is the identity element for $\cdot$

property 7: Because the coefficients are in $\mathbb{R}$, the polynomials also follow the distributive law. $\square$

17 Problem 2.1.2

Proof. 1. If $v = 0$, then $1 \cdot v = 0$ but $1 \neq 0$, implying that $S \cup \{v\}$ is linearly dependent. Suppose $v \neq 0$. Since S is a spanning set, $v = c_1 s_1 + c_2 s_2 + \cdots + c_n s_n$, where $c_1, c_2, \ldots, c_n \in k$ and $s_1, s_2, \ldots, s_n \in S$. Since $v \neq 0$, not all of $c_1, c_2, \ldots, c_n$ is 0. But $c_1 s_1 + c_2 s_2 + \cdots + c_n s_n - 1 \cdot v = 0$ is a linear combination that equals 0. Hence, $S \cup \{v\}$ is linearly dependent.

2. Let $v = c_1 s_1 + c_2 s_2 + \cdots + c_n s_m$, where $c_1, \ldots, c_m$ and $s_1, \ldots, s_m \in S$. Let $w = s_m$. Then, $w = v - c_1 (c_m)^{-1} s_1 - c_2 (c_m)^{-1} s_2 - \cdots - c_{m-1} (c_m)^{-1} s_{m-1}$. Suppose $v_0 = k_1 s_1' + k_2 s_2' + \cdots + k_n s_n'$, where $k_1, \ldots, k_n \in k$ and $s_1', \ldots, s_n' \in S$. If $w \notin \{s_1', \ldots, s'nm\}$, then v_0 is a linear combination of elements in $(S - \{w\}) \cup \{v\}$. If $w \in \{s_1', \ldots, s_n'\}$, without loss of generality, assume $s_n' = w$. Then, $v_0 = k_1 s_1' + \cdots + k_{n-1} s_{n-1}' + k_n (v - c_1 (c_m)^{-1} s_1 - \cdots - c_{m-1} (c_m)^{-1} s_{m-1})$. This is a linear combination of elements in $(S - \{w\}) \cup \{v\}$. Hence, $(S - \{w\}) \cup \{v\}$ is a spanning set.

□

18 Problem 2.2.1

Proof. **Example 1:** $2, x, x^2$
If $a \cdot 2 + b \cdot x + c \cdot x^2 = 0$ as polynomials, where $a, b, c \in \mathbb{C}$, then $a = b = c = 0$. Furthermore, every polynomial of degree at most 2, by definition, can be written in the form $\frac{a}{2} \cdot 2 + b \cdot x + c \cdot x^2$, and so these elements $2, x, x^2$ are a basis.
Example 2: $3, x, x^2$
If $a \cdot 3 + b \cdot x + c \cdot x^2 = 0$ as polynomials, where $a, b, c \in \mathbb{C}$, then $a = b = c = 0$. Furthermore, every polynomial of degree at most 2, by definition, can be written in the form $\frac{a}{3} \cdot 3 + b \cdot x + c \cdot x^2$, and so these elements $3, x, x^2$ are a basis. □

19 Problem 2.2.2

Proof. 1.)
Let S be a spanning set in field k. Because S is a spanning set, v can be written as $v = w_1 \cdot c_1 + w_2 \cdot c_2 + ... + w_x \cdot c_x$ where $w_i \in S$ and $c_i \in k$
We have a linear combination, $w_1 \cdot c_1 + w_2 \cdot c_2 + ... + w_x \cdot c_x + v \cdot (-1) = 0$. Therefore, $S \cup \{v\}$ is linearly dependent.
2.) Because $v = w_1 \cdot c_1 + w_2 \cdot c_2 + ... + w_x \cdot c_x$ and $v \neq 0$, there must be $w_i \in \{w_1, w_2, ..., w_x\}$ such that $w_i \neq 0$
$w_i = \dfrac{v - w_1 \cdot c_1 - ... - w_{i-1} \cdot c_{i-1} - w_{i+1} \cdot c_{i+1} - ... - w_x \cdot c_x}{c_i}$
We will prove that w_i is the vector such that $(S - \{w\}) \cup \{v\}$ is a spanning set.
Let V be the vector space. Suppose that $(S - \{w_i\}) \cup \{v\}$ is NOT a spanning set.
There must exist a vector $a \in V$, such that there is no expression of a as a linear combination of vectors in $(S - \{w\}) \cup \{v\}$.
However, because S is a spanning set, a can be written as a linear combination of vectors in S.
If there exists a linear combination that does not include w_i, then $(S - \{w_i\}) \cup \{v\}$ is a spanning set which leads to CONTRADICTION.
If all the linear combinations include w_i, then substitute w_i with
$\dfrac{v - w_1 \cdot c_1 - ... - w_{i-1} \cdot c_{i-1} - w_{i+1} \cdot c_{i+1} - ... - w_x \cdot c_x}{c_i}$
Because this linear combination exists, $(S - \{w_i\}) \cup \{v\}$ is a spanning set which leads to CONTRADICTION.

We can conclude that there exists a vector w_i in S such that $(S - \{w_i\}) \cup \{v\}$ is a spanning set □

20 Problem 2.2.3

Proof. According to the condition $L \not\subset S$, $|L| > 0$ and $|L - S| > 0$.
Because L is a linearly independent set, all elements in L are non-zero.
Now, we have that S is a spanning set, and Let v be a vector that doesn't lie in S, but in $L - S$.
According to Problem 2.2.2(2), there must exists a vector w_i in S such that $(S - \{w_i\}) \cup \{v\}$ is a spanning set.
We want to show that this vector w_i exists in $S - L$, not just S.

□

21 Problem 2.2.4

Proof. Continuing the process in Problem 2.2.3, we can see that $|L-S|$ is decreasing until it reaches 0 when $L \subset S$. Because S is finite, L must be finite. Moreover, $|L| \leq |S|$
We can conclude that the size of every linearly independent set is at most the size of every spanning set. □

22 Problem 2.2.5

Proof. 1.) If the spanning set is not a basis yet, there exists a linear combination between some vectors in the set. From those vectors, remove one. This will not affect its spanning property. Repeat the process continuously will result in a spanning set that has no linear combination, which is a basis.
2.) If the linearly independent set is not a basis yet, the span of all the vectors in the set does not cover the vector space. Suppose there is a vector a outside of the span of the current set, we may add vector a to our linearly independent set. This will not affect its linearly independent property because a is outside of the span of all the vectors in the set. Repeat the process continuously will result in a linearly independent set that span the vector space, which is a basis. □

23 Problem 2.2.6

Proof. □

24 Problem 2.2.7

Proof. Suppose W is a subspace of V, but $dimW > dimV$.

□

25 Problem 2.3.1

Proof. Because $f(v_1 + v_2) = f(v_1) + f(v_2)$ for all $v_1, v_2 \in V$
Substitute $v1$ with 0 and $v2$ with 0:
$f(0) = 2 \cdot f(0)$
$f(0) = 0$
Substitute $v1$ with v and $v2$ with $-v$:
$0 = f(0) = f(v) + f(-v)$
We will prove that $f(sv) = sf(v)$ for all $s \in \mathbb{N}$
Base case: $s = 1 : f(1 \cdot v) = 1 \cdot f(v)$ which is trivial
Inductive case: Assume $f(nv) = nf(v)$, will prove that $f((n+1)v) = (n+1)f(v)$
Substitute $v1$ with nv and $v2$ with v:
$f(nv + v) = f(nv) + f(v)$
$f((n+1)v) = nf(v) + f(v) = (n+1)f(v)$
Therefore, $f(sv) = sf(v)$ for all $s \in \mathbb{N}$

Substitute v with $\frac{v}{s}$ in the latest equation
$f(\frac{v}{s}) = \frac{f(v)}{s}$ for all $s \in \mathbb{N}$
Combining these two equations and $-f(v) = f(-v)$,
we have that $T : V \to W$ satisfies $T(sv) = sT(v)$ for all $s \in \mathbb{Q}$
f is a linear transformation. □

26 Problem 2.3.2

Proof. Because $kerT$ is the set of elements $v \in V$such that $T(v) = 0_W$, $kerT$ is obviously a subset of V.
Let $T(v_1) = 0$ and $T(v_2) = 0$, we have $T(v_1 + v_2) = 0$ and $T(s \cdot v_1) = 0$
Let $T(v_1) = 0$, we know $T(0) = 0$, so $T(-v_1) = 0$
Therefore, $kerT$ is a subspace of V □

27 Problem 2.3.3

Proof. (write your solution here) □

28 Problem 2.3.4

Proof. (write your solution here) □

29 Problem 2.3.5

Proof. 1.) The basis of $kerT$ consists of $w_1, w_2, ..., w_n$
According to Problem 2.3.2 , $kerT$ is a subspace of V. According to Problem 2.2.5(2), the basis of $kerT$, which is linearly independent, can be extended to a basis of V.
2.)
$imT = T(c_1w_1 + c_2w_2 + ... + c_nw_n + c_{n+1}w_{n+1} + ... + c_mw_m)$
$= 0 + c_{n+1}T(w_{n+1}) + ... + c_mT(w_m)$
Now, we know that $T(w_{n+1}), ..., T(w_m)$ span imT
Suppose there exists a linear combination between them,
$a_{n+1}T(w_{n+1}) + ... + a_mT(w_m) = 0$
We will have $T(a_{n+1}w_{n+1} + ... + a_mw_m) = 0$
Therefore, $a_{n+1}w_{n+1} + ... + a_mw_m$ is in $kerT$ which spans $w_1, w_2, ..., w_n$
We will have that $w_1, w_2, ..., w_m$ is not a basis of V, which is a CONTRADICTION.
So, $T(w_{n+1}), ..., T(w_m)$ form a basis for imT

□

30 Problem 2.3.6

Proof. (write your solution here) □

31 Problem 2.4.1

Proof. For each v, because w_i are bases (linearly independent), there exists a unique $\begin{pmatrix} a_1 \\ a_2 \\ \vdots \\ a_m \end{pmatrix}$

So, the map is well-defined.

$f : V \to k^n$ is injective because the same $\begin{pmatrix} a_1 \\ a_2 \\ \vdots \\ a_m \end{pmatrix}$ would give the same v.

Suppose $f : V \to k^n$ is not surjective

There is no v that yields $\begin{pmatrix} b_1 \\ b_2 \\ \vdots \\ b_m \end{pmatrix}$, then there will exist $v = b_1w_1 + ... + b_nw_n \notin V$, which is a CONTRADICTION.

Therefore, there is an isomorphism between V and k^n

□

32 Problem 2.4.2

Proof. (write your solution here) □

33 Problem 2.4.3

Proof. (write your solution here) □

34 Problem 2.4.4

Proof. (write your solution here) □

35 Problem 2.4.5

Proof. 1.) $\begin{pmatrix} 1 & 0 & -1 \\ 0 & 1 & 2 \end{pmatrix}$

2.) $\begin{pmatrix} 1 & 0 & 0 & -\frac{37}{19} \\ 0 & 1 & 0 & 2 \\ 0 & 0 & 1 & -\frac{15}{19} \end{pmatrix}$ □

36 Problem 2.4.6

Proof. For any column, if there exists more than one nonzero value, do the row operation such that there is only one nonzero value left, then divide that row by that last value to create 1. □

37 Problem 2.4.7

Proof. Start at the first column, if there exists more than one nonzero value, do the row operation such that there is only one nonzero value left,
then divide that row by itself to create 1,
then switch the pivot to the first row.
If there exists only one nonzero, only divide and switch its row to the first row.

At the second column, if there exists at least one nonzero value on the different row than the existed pivot, do the row operation such that the value on the same row with the existed pivot become 0 (this will not affect the column to the left because those row without existed pivot only have 0 to the left of the current column), then continue until there is only one nonzero value left, divide to make it 1, then switch it to the second row.
If all the nonzero values are on the same row with the existed pivot, we leave it as it was.

For all the other column, we do the same process did in the second column.
This satisfies the properties of the reduced row echelon form.
1) Every row with at least one nonzero entry has their leftmost nonzero entry as a 1 because the process always divide the whole row to make 1.
2) Each pivot is the only nonzero entry in its column was guaranteed through the process.
3) The pivot of the ith row is left of the pivot of the jth row if i ¡ j is guaranteed by switching the row with new pivot to the row below the earlier pivot.
4) The rows with all zeros are on the bottom of the matrix. This is also guaranteed by switching the row. □

38 Problem 2.4.8

Proof. (write your solution here) □

39 Problem 3.0.1

Proof. If $m_1, m_2 \in I$, then by the definition of an ideal, $m_1 + m_2 \in I$, and for all $r \in R, m \in M$, we have $r \cdot m \in M$. Hence, M is closed under addition and scalar multiplication. Since the operations of $+$ and $\cdot$ are those of the ring R, these operations follow the commutative, associative, and distributive laws. Since $0 \in I$, and for all $m \in I \subseteq R$, $0 + m = m$, the operation $+$ has an identity element. Since $1_R \cdot m = m$ for all $m \in I \subseteq R$, property 6 also suffices. Lastly, for all $m \in I$, we have $-m \in I$ with $m + (-m) = 0$. Hence, I is an R-module under the addition and multiplication operations of the ring R. □

40 Problem 3.0.2

Proof. Let M be a finitely generated free module. Let $\{m_1, m_2, \ldots, m_n\}$ be a free basis of M. Then every element $m \in M$ can be uniquely expressed as $m = r_1m_1 + r_2m_2 + \cdots + r_nm_n$ for some $r_1, r_2, \ldots, r_n \in R$. Consider the map $\phi : M \longrightarrow R^n$ defined by

$$\phi(m) = \phi(r_1m_1 + r_2m_2 + \cdots + r_nm_n) = (r_1, r_2, \ldots, r_n)$$

This mapping is well-defined, since for each m the corresponding $\{r_1, r_2, \ldots, r_n\}$ is unique. Furthermore, if $m = r_1m_1 + r_2m_2 + \cdots + r_nm_n$, $m' = r_1'm_1 + r_2'm_2 + \cdots + r_n'm_n$, and $r \in R$, then

$$\phi(m + m') = \phi((r_1 + r_1')m_1 + (r_2 + r_2')m_2 + \cdots + (r_n + r_n')m_n)$$

$$= (r_1 + r_1', r_2 + r_2', \ldots, r_n + r_n') = (r_1, r_2, \ldots, r_n) + (r_1', r_2', \ldots, r_n') = \phi(m) + \phi(m')$$

$$\phi(rm) = \phi(rr_1m_1 + rr_2m_2 + \cdots rr_nm_n) = (rr_1, rr_2, \ldots, rr_n) = r(r_1, r_2, \ldots, r_n) = r\phi(m)$$

This shows that ϕ is a homomorphism. For all $(r_1, r_2, \ldots, r_n) \in R^n$, we have $\phi(r_1m_1 + r_2m_2 + \cdots + r_nm_n) = (r_1, r_2, \ldots, r_n)$, so ϕ is surjective. If $\phi(m) = \phi(r_1m_1 + r_2m_2 + \cdots + r_nm_n) = 0$, then $(r_1, r_2, \ldots, r_n) = 0$, which implies that $m = r_1m_1 + r_2m_2 + \cdots r_nm_n = 0$. Hence, ϕ is injective. We conclude that ϕ is an isomorphism from M to R_n. Therefore, M is isomorphic to R^n. □

41 Problem 3.0.3

Proof. Notice that for all $m, m' \in M$ and $r \in R$,

$$\kappa_{M,N}(m + m') = (m + m') + N = (m + N) + (m' + N) = \kappa_{M,N}(m) + \kappa_{M,N}(m')$$

$$\kappa_{M,N}(r \cdot m) = (r \cdot m) + N = r \cdot (m + N) = r\kappa_{M,N}(m)$$

Hence, $\kappa_{M,N}$ is a homomorphism. For all $m + N \in M/N$, we have $m + N = \kappa_{M,N}(m)$, so $\kappa_{M,N}$ is a surjective homomorphism. Note that $\kappa_{M,N}(m) = m + N = 0 + N$ if and only if $m \in N$. Therefore, the kernal of $\kappa_{M,N}$ is N. □

42 Problem 3.0.4

Proof. 1. Given $m + \ker\phi \in M/\ker\phi$, let $\bar{\phi}(m + \ker\phi) = \bar{\phi}(\kappa_{M,N}(m)) = \phi(m)$. We first prove that this mapping is well-defined.
If $m, m' \in M$, $m + \ker\phi = m' + \ker\phi$, then $m' = m + k$, where $k \in \ker\phi$. Since ϕ is a homomorphism,

$$\phi(m') = \phi(m + k) = \phi(m) + \phi(k) = \phi(m)$$

Therefore, $\bar{\phi}\kappa_{M,N}(m) = \bar{\phi}\kappa_{M,N}(m')$., so the mapping is well defined. Also notice that if $m, m' \in M$, $r \in R$ then

$$\bar{\phi}((m + m') + \ker\phi) = \phi(m + m') = \phi(m) + \phi(m') = \bar{\phi}(m + \ker\phi) + \bar{\phi}(m' + \ker\phi)$$

$$\bar{\phi}(rm + \ker\phi) = \phi(rm) = r\phi(m) = r\bar{\phi}(m + \ker\phi)$$

Therefore, $\bar{\phi}$ is the homomorphism we want.

2. We will prove that $\bar{\phi}$ is an isomorphism from $M/\ker\phi$ to $\operatorname{im}\phi$.
If $\bar{\phi}(m + \ker\phi) = 0$, then $\phi(m) = 0$, which implies that $m \in \ker\phi$. Therefore, $m + \ker\phi = 0 + \ker\phi$. Hence, $\ker\bar{\phi} = \{0 + \ker\phi\}$.
If $\bar{\phi}(m + \ker\phi) = \bar{\phi}(m' + \ker\phi)$, then

$$\bar{\phi}((m + \ker\phi) - (m' + \ker\phi)) = \bar{\phi}((m - m') + \ker\phi) = \bar{\phi}(m + \ker\phi) - \bar{\phi}(m' + \ker\phi) = 0$$

Which implies that $(m + \ker\phi) - (m' + \ker\phi) \in \ker\bar{\phi}$. But $\ker\bar{\phi}$ contains only one element, namely, $0 + \ker\phi$. Hence, $(m + \ker\phi) - (m' + \ker\phi) = 0 + \ker\phi$. So $m + \ker\phi = m' + \ker\phi$. This shows that $\bar{\phi}$ is injective.
For each $m \in M$, $\bar{\phi}(m + \ker\phi) = \phi(m)$. Therefore, $\operatorname{im}\bar{\phi} = \operatorname{im}\phi$. This implies that $\bar{\phi}$ is a bijective map from $M/\ker\phi$ to $\operatorname{im}\phi$, which means that $M/\ker\phi$ is isomorphic to $\operatorname{im}\phi$.

□

43 Problem 4.1.1

Proof. 1. Let R be a Noetherian ring. Suppose for the sake of contradiction that there is an ideal I of R that was not generated by finitely many elements. Let $i_1 \in I$, and $I_1 =< i_1 >$. Suppose $I_n =< i_1, i_2, \ldots, i_n >$. Since I is not finitely generated, $I_n \subset I$ but $I_n \neq I$. Hence, there is an element i_{n+1} such that $i_{n+1} \notin I_n$. Let $I_{n+1} =< i_1, i_2, \ldots, i_n, i_{n+1} >$. In this way, we have created an ascending chain $I_1 \subset I_2 \subset I_3 \subset \cdots$ such that for each $n \in \mathbb{N}$, $I_{n+1} \neq I_n$. Hence, R is not a Noetherian ring, contradiction. Therefore, every ideal can be generated by a finite set of elements in R.

2. Let $I = \bigcup_{i=1}^{\infty} I_i$. If $i_1, i_2 \in I$, then $i_1 \in I_{n_1}$, $i_2 \in I_{n_2}$ for some $n_1, n_2 \in \mathbb{N}$. Without loss of generality, assume $n_1 \leq n_2$. Then $I_{n_1} \subseteq I_{n_2}$, so $i_1 \in I_{n_2}$. By the definition of ideal, $i_1 + i_2 \in I_{n_2} \subset I$. Hence, I is closed under addition. If $i \in I$, then there exists $n \in \mathbb{N}$ such that $i \in I_n$. If $r \in R$, then by definition, $r \cdot i \in I_n \subset I$. Hence, I is an ideal of R.

3. Suppose $I_1 \subseteq I_2 \subseteq I_3 \subseteq \ldots$ be a chain of ideals. Let $I = \bigcup_{i=1}^{\infty} I_i$. By part 2, I is an ideal. From the condition we know that I can be generated by a finite set of elements $\{i_1, i_2, \ldots, i_m\}$. Since $i_1, i_2, \ldots, i_m \in I$, there is $n_1, n_2, \ldots, n_m \in \mathbb{N}$ such that $i_1 \in I_{n_1}, i_2 \in I_{n_2}, \ldots, i_{n_m} \in I_m$. Choose $n = \max\{n_1, n_2, \ldots, n_m\}$. Then, $i_1, i_2, \ldots, i_m \in I_n$, so $< i_1, i_2, \ldots, i_m >\subseteq I_n$. But $I_n \subseteq I =< i_1, i_2, \ldots, i_m >$. Hence, $I_n =< i_1, i_2, \ldots, i_m >$. For all $n' > n$, $I_n =< i_1, i_2, \ldots, i_m >\subseteq I_{n'}$, but $I_{n'} \subseteq I = I_n =< i_1, i_2, \ldots, i_m >$. Therefore, $I_n = I_{n'}$, so R is Noetherian.

4. If R is a PID, then every ideal of R can be generated by one element. By part 3, R is Noetherian.

□

Notation: throughout section 4 and 5, $< r_1, r_2, \ldots, r_n >$ or $\langle r_1, r_2, \ldots, r_n \rangle$ is used to denote the ideal or the submodule generated by $r_1, r_2, \ldots, r_n$. If it is clear whether the algebraic structure denoted is an ideal or submodule, we will not specify the algebraic structure.

44 Problem 4.1.2

Proof. 1. Let M be a Noetherian module. Suppose for the sake of contradiction that there is a submodule M' of M that was not generated by finitely many elements. Let $m_1 \in M'$, and $I_1 =< m_1 >$. Suppose $M_n =< m_1, m_2, \ldots, m_n >$. Since M' is not finitely generated, $M_n \subset M'$ but $M_n \neq M'$. Hence, there is an element m_{n+1} such that $m_{n+1} \notin M_n$. Let $M_{n+1} =< m_1, m_2, \ldots, m_n, m_{n+1} >$. In this way, we have created an ascending chain $M_1 \subset M_2 \subset M_3 \subset \cdots$ such that for each $n \in \mathbb{N}$, $M_{n+1} \neq M_n$. Hence, M is not a Noetherian module, contradiction. Therefore, every submodule can be generated by a finite set of elements in M.

2. We first prove that for any chain $M_1 \subseteq M_2 \subseteq M_3 \subseteq \cdots$, $\bigcup_{i=1}^{\infty} M_i$ is a submodule.

   Let $M' = \bigcup_{i=1}^{\infty} M_i$. Since addition and multiplication in M' are the same as those in M, they follow commutative, associative, and distributive law. Since $M' \subseteq M$, for all $m \in M'$, $0 + m = m$ and $1 \cdot m = m$. If $m \in M'$, then there exists $n \in \mathbb{N}$ such that $m \in M_n$. Then, m has an additive inverse in M_n, which implies that m has an additive inverse in M'.

   If $m_1, m_2 \in M'$, then $m_1 \in M_{n_1}$, $m_2 \in M_{n_2}$ for some $n_1, n_2 \in \mathbb{N}$. Without loss of generality, assume $n_1 \leq n_2$. Then $I_{n_1} \subseteq I_{n_2}$, so $m_1 \in M_{n_2}$. By the definition of submodule, $m_1 + m_2 \in M_{n_2} \subset M'$. Hence, M' is closed under addition. If $m \in M$, then there exists $n \in \mathbb{N}$ such that $m \in M_n$. If $r \in R$, then by definition, $r \cdot m \in M_n \subset M'$. Hence, M' is a submodule of M.

   Suppose $M_1 \subseteq M_2 \subseteq M_3 \subseteq \ldots$ be a chain of ideals. Let $M' = \bigcup_{i=1}^{\infty} M_i$. M' is a submodule of M. From the condition we know that M' can be generated by a finite set of elements $\{m_1, m_2, \ldots, m_k\}$. Since $m_1, m_2, \ldots, m_k \in M'$, there is $n_1, n_2, \ldots, n_k \in \mathbb{N}$ such that $m_1 \in M_{n_1}, m_2 \in M_{n_2}, \ldots, m_{n_k} \in M_{n_k}$. Choose $n = \max\{n_1, n_2, \ldots, n_k\}$. Then, $m_1, m_2, \ldots, m_k \in M_n$, so $< m_1, m_2, \ldots, m_k > \subseteq M_n$. But $M_n \subseteq M' =< m_1, m_2, \ldots, m_k >$. Hence, $M_n =< m_1, m_2, \ldots, m_k >$. For all $n' > n$, $M_n =< m_1, m_2, \ldots, m_k > \subseteq M_{n'}$, but $M_{n'} \subseteq M' = M_n =< m_1, m_2, \ldots, m_k >$. Therefore, $M_n = M_{n'}$, so M is Noetherian.

□

Notation: throughout section 4 and 5, $< r_1, r_2, \ldots, r_n >$ or $\langle r_1, r_2, \ldots, r_n \rangle$ is used to denote the ideal or the submodule generated by $r_1, r_2, \ldots, r_n$. If it is clear whether the algebraic structure denoted is an ideal or submodule, we will not specify the algebraic structure.

45 Problem 4.1.3

Proof. Let $M' \subseteq N$ be a submodule of N. Since $N \subseteq M$ is a submodule of M, M' is also a submodule of M. Since M is Noetherian, M' finitely generated. Therefore, every submodule of N is finitely generated, implying that N is Noetherian.

I claim that if $M' \in M/N$ is a submodule of M/N, then $M_0 \in M$, the preimage of M' under $\kappa_{M,N}$, is a submodule of M. Notice that if $m, m_1, m_2 \in M_0$, then $m = m' + n, m_1 = m_1' + n_1, m_2 = m_2' + n_2$, where $m', m_1', m_2' \in M', n, n_1, n_2 \in N$. Then $m_1 + m_2 = (m_1' + m_2') + (n_1 + n_2)$, and if $r \in R$, then $rm = rm' + rn$. So $\kappa_{M,N}(m_1 + m_2) = (m_1' + m_2') + N = (m_1' + N) + (m_2' + N) \in M'$ and $\kappa_{M,N}(rm) = (rm) + N = r(m + N) \in M'$, since M' is a submodule. Hence, $m_1 + m_2, rm \in M_0$. Moreover, the commutative, associative, and distributive law, the existence of 0, 1, and the additive inverse carry over from the corresponding properties of M. Therefore, M_0 is a submodule of M.

Let $M_1' \subseteq M_2' \subseteq M_3' \subseteq \cdots$ be a chain of submodule of M/N. Let $M_1, M_2, M_3, \ldots$ be the preimage of $M_1', M_2', M_3', \ldots$ under $\kappa_{M,N}$, respectively. Then, $M_1 \subseteq M_2 \subseteq M3 \subseteq \cdots$. By definition, there exists $n \in \mathbb{N}$ such that for all $m \geq n$, $M_m = M_n$. Therefore, for all $m \geq n$, $M_m' = M_n'$. This shows that M/N is Noetherian.

□

Notation: throughout section 4 and 5, $< r_1, r_2, \ldots, r_n >$ or $\langle r_1, r_2, \ldots, r_n \rangle$ is used to denote the ideal or the submodule generated by $r_1, r_2, \ldots, r_n$. If it is clear whether the algebraic structure denoted is an ideal or submodule, we will not specify the algebraic structure.

46 Problem 4.1.4

Proof. 1. If $m \in M_2$, then $\kappa_{M,N}(m) = m + N$. Since $\kappa_{M,N}(M_1) = \kappa_{M,N}(M_2)$, we have $m + N \in \kappa_{M,N}(M_2) = \kappa_{M,N}(M_1)$. Therefore, $m + N = \kappa_{M,N}(m') = m' + N$, where $m' \in M_1 \subseteq M_2$. Then, $m' - m \in N$, and since $m', m \in M_2$, we have $m' - m \in M_2 \cap N$. But $M_2 \cap N = M_1 \cap N$, so $m' - m \in M_1 \cap N \subseteq M_1$. Hence, $m \in M_1$. Therefore, $M_1 = M_2$.

2. Let $M_1' \subseteq M_2' \subseteq M_3' \subseteq \cdots$ be a chain of submodule of M/N. Let $M_1, M_2, M_3, \ldots$ be the preimage of $M_1', M_2', M_3', \ldots$ under $\kappa_{M,N}$, respectively. By definition, there exists $n_1 \in \mathbb{N}$ such that for all $m \geq n_1$, $M_m' = M_n'$, so $\kappa_{M,N}(M_m) = \kappa_{M,N}(M_{n_1})$. Consider the chain of submodule $M_1 \cap N \subseteq M_2 \cap N \subseteq M_3 \cap N \subseteq \cdots$. Since each element in the chain of submodule is a submodule of N, there exists $n_2 \in \mathbb{N}$ such that for all $m \geq n_2$, $M_m \cap N = M_{n_2} \cap N$. Choose n to be the greater of n_1 and n_2. Then, for all $m \geq n$, we have $M_m \cap N = M_n \cap N$ and $\kappa_{M,N}(M_m) = \kappa_{M,N}(M_n)$. By the previous part, $M_m = M_n$. This implies that M is Noetherian. □

Notation: throughout section 4 and 5, $< r_1, r_2, \ldots, r_n >$ or $\langle r_1, r_2, \ldots, r_n \rangle$ is used to denote the ideal or the submodule generated by $r_1, r_2, \ldots, r_n$. If it is clear whether the algebraic structure denoted is an ideal or submodule, we will not specify the algebraic structure.

47 Problem 4.1.5

Proof. 1. By Problem 4.1.2 part 1, if M is a Noetherian module, then every submodule of M is finitely generated. Since M is a submodule of itself, M is finitely generated.

2. If M is a submodule of R, then M is an ideal of R. This is because if $m, m_1, m_2 \in M$, $r \in R$, then $m_1 + m_2 \in M$, $rm \in M$, and by definition, M is an ideal of R. If $M_1 \subseteq M_2 \subseteq M_3 \subseteq \cdots$ is a chain of submodule of R, then it is also a chain of ideals of R. Since R is a Noetherian ring, there exists $n \in \mathbb{N}$ such that for all $m \geq n$, we have $M_m = M_n$. Therefore, R is also a Northerian R-module.

3. I claim that R^{n-m} is a free module generated by a free basis of $n - m$ elements. Let $r_1 = (1, 0, 0, \ldots, 0), r_2 = (0, 1, 0, \ldots 0), r_3 = (0, 0, 1, \ldots, 0), \ldots, r_n = (0, 0, 0, \ldots, 1)$. It is clear that $\{r_1, r_2, \ldots, r_n\}$ is a free basis for R^n, and $\{r_1, r_2, \ldots, r_m\}$ is a free basis for R^m, treated as a submodule of R^n. Consider $\{r_{m+1} + R^m, r_{m+2} + R^m, \ldots, r_n + R^m\}$. Suppose $r' + R^m \in R^n/R^m$. Since $r' \in R^n$, $r' = c_1r_1 + c_2r_2 + \cdots + c_nr_n$ for some $c_1, c_2, \ldots, c_n \in R$. Since $c_1r_1 + c_2r_2 + \cdots + c_mr_m \in R^m$, $r' + R^m = (c_{m+1}r_{m+1} + c_{m+1}r_{m+1} + \cdots + r_nr_n) + R^m = c_{m+1}(r_{m+1} + R^m) + c_{m+2}(r_{m+2} + R^m) + \ldots + c_n(r_n + R^m)$. Hence, $\{r_{m+1} + R^m, r_{m+2} + R^m, \ldots, r_n + R^m\}$ is a generating set. If $c_{m+1}(r_{m+1} + R^m) + c_{m+2}(r_{m+2} + R^m) + \ldots + c_n(r_n + R^m) = 0$, then $c_{m+1}r_{m+1} + c_{m+2}r_{m+2} + \cdots + c_nr_n \in R^m$. But this could only happen when $c_{m+1} = c_{m+2} = \cdots = c_n = 0$. Hence, $\{r_{m+1} + R^m, r_{m+2} + R^m, \ldots, r_n + R^m\}$ is linearly independent, and so a free basis of $n - m$ elements.

   Proceed as it is in Problem 3.0.2, we can show that R^n/R^m is isomorphic to ${}^{n-m}$.

4. We use induction. By part 2, we know that R is an Noetherian R-module. Assume by induction that R^n is a Noetherian R-module. Then, since R^{n+1}/R is isomorphic to R^n, and both R and R^n are Noetherian, by Problem 4.1.4 part 2, R^{n+1} is also Noetherian. This completes the induction and shows that R^n is Noetherian for every positive integer n.

5. We use induction. For the base case, let M is a R-module generated by a single element, m. Then, M is isomorphic to R, a Noetherian R-module. Hence M is a Noetherian R-module. Assume by strong induction that if M is a R-module generated by n or less elements, then M is Noetherian. Let M be a R-module generated by $n + 1$ elements, $m_1, m_2, \ldots, m_{n+1}$. Consider M_1 be the submodule of M generated by m_1. Then, if $m' + M_1 \in M/M_1$, and $m' = r_1m_1 + r_2m_2 + \cdots + r_{n+1}m_{n+1}$, where $r_1, r_2, \ldots, r_{n+1} \in R$, then $m' + M_1 = (r_1m_1 + r_2m_2 + \cdots + r_{n+1}m_{n+1}) + M_1 = r_1(m_1 + M_1) + r_2(m_2 + M_1) + \cdots + r_{n+1}(m_{n+1} + M_1) = r_2(m_2 + M_1) + r_3(m_3 + M_1) + \cdots + r_{n+1}(m_{n+1} + M_1)$. Hence, M/M_1 is a submodule generated by $\{m_2 + M_1, m_3 + M_1, m_{n+1} + M_1\}$, a set of n elements. By our induction hypothesis, M/M_1 is Noetherian. Since M_1 is also Noetherian by our base case, M is Noetherian. This completes the induction and shows that if M is finitely generated, then M is a Noetherian R-module.

□

Notation: throughout section 4 and 5, $< r_1, r_2, \ldots, r_n >$ or $\langle r_1, r_2, \ldots, r_n \rangle$ is used to denote the ideal or the submodule generated by $r_1, r_2, \ldots, r_n$. If it is clear whether the algebraic structure denoted is an ideal or submodule, we will not specify the algebraic structure.

48 Problem 4.2.1

Proof. Denote $\sum_{i=1}^{n} a_{i,j}e_i$ to be A_j. This corresponds to the jth column of A. If $S_i = (s_{1,i}, s_{2,i}, \ldots, s_{m,i}$, the submodule generated by $\{s_{1,i}, s_{2,i}, \ldots, s_{m,i}\}$, then $AS_i = s_{1,i}A_1 + s_{2,i}A_2 + \cdots + s_{m,i}A_m$. Since $A_1, A_2, \ldots, A_m \in N(A)$, $AS_i \in N(A)$. Notice that the column of $A' = AS$ is $AS_1, AS_2, \ldots, AS_m$. If $a' \in N(A')$, then $a' = r_1AS_1 + r_2AS_2 + \cdots + r_mAS_m$ for some $r_1, r_2, \ldots, r_m \in R$. This implies that $a' \in N(A)$. So $N(A') \subseteq N(A)$.

Notice that $A = (AS)S'$, where S' is the inverse of S. Denote S'_i to be the ith column of S'. If $S'_i = (s'_1, s'_2, \ldots, s'_m)$, then $A_i = s'_1(AS_1) + s'_2(AS_2) + \cdots + s'_m(AS_m)$. Since $AS_1, AS_2, \ldots, AS_m \in N(A')$, $A_i \in N(A')$. If $a \in N(A)$, then $a' = r_1A1 + r_2A_2 + \cdots + r_mA_m$ for some $r_1, r_2, \ldots, r_m \in R$. This implies that $a \in N(A')$. So $N(A) \subseteq N(A')$. Hence, $N(A) = N(A')$. □

Notation: throughout section 4 and 5, $< r_1, r_2, \ldots, r_n >$ or $\langle r_1, r_2, \ldots, r_n \rangle$ is used to denote the ideal or the submodule generated by $r_1, r_2, \ldots, r_n$. If it is clear whether the algebraic structure denoted is an ideal or submodule, we will not specify the algebraic structure.

49 Problem 4.2.2

Proof. Let $\phi : R^n/N(A) \longrightarrow R^n/N(A')$, $r + N(A) \rightsquigarrow Sr + N(A')$. If $r_1 + N(A) = r_2 + N(A) \in R^n/N(A)$, then $r_2 = r_1 + Ar_0$, since any element of $N(A)$ can be expressed as Ar_0 for some $r_0 \in R$. Then, $\phi(r_2 + N(A)) = Sr_2 + N(A') = S(r_1 + Ar_0) + N(A') = Sr_1 + A'r_0 + N(A') = Sr_1 + N(A') = \phi(r_1 + N(A))$. Therefore, this map is well-defined. Furthermore, $\phi((r_1 + N(A)) + (r_2 + N(A))) = \phi((r_1 + r_2) + N(A)) = S(r_1 + r_2) + N(A') = (Sr_1 + N(A')) + (Sr_2 + N(A')) = \phi(r_1 + N(A)) + \phi(r_2 + N(A))$. And if $r \in R$, then $\phi(r(r_1 + N(A))) = S(r(r_1)) + N(A') = r(Sr_1 + N(A')) = r\phi(r_1 + N(A))$. Hence, ϕ is a homomorphism. The fact ϕ is an isomorphism is implied from the fact that $\phi' : R^n/N(A') \rightsquigarrow R^n/N(A), r + N(A') \rightsquigarrow S^{-1}r + N(A)$ is the inverse of ϕ. □

Notation: throughout section 4 and 5, $< r_1, r_2, \ldots, r_n >$ or $\langle r_1, r_2, \ldots, r_n \rangle$ is used to denote the ideal or the submodule generated by $r_1, r_2, \ldots, r_n$. If it is clear whether the algebraic structure denoted is an ideal or submodule, we will not specify the algebraic structure.

50 Problem 4.2.3

Proof. 1. Since R is a PID and r_1, r_2 are not all 0, $\langle r_1, r_2\rangle = \langle r\rangle$ for some $r \neq 0 \in R$. Hence, $r = ar_1 + br_2$, and $r_1 = cr, r_2 = dr$ for some $a, b, c, d \in R$. Let S be the matrix $\begin{bmatrix} a & b \\ -d & c \end{bmatrix}$. Then, $S\begin{bmatrix} r_1 \\ r_2 \end{bmatrix} = \begin{bmatrix} ar_1 + br_2 \\ -d(cr) + c(dr) \end{bmatrix} = \begin{bmatrix} r \\ 0 \end{bmatrix}$. Notice that $r = ar_1 + br_2 = acr + bdr = (ac + bd)r$. Since R is an integral domain and $r \neq 0, ac + bd = 1$, so $\begin{bmatrix} c & -b \\ d & a \end{bmatrix}$ is the inverse of S. Hence, S is the desired invertible matrix.

2. Let $i \in \{2, 3, \ldots, n\}$. By the previous part, there is a 2 by 2 invertible matrix $\begin{bmatrix} a & b \\ -d & c \end{bmatrix}$ such that $\begin{bmatrix} a & b \\ -d & c \end{bmatrix}\begin{bmatrix} r_1 \\ r_i \end{bmatrix} = \begin{bmatrix} r \\ 0 \end{bmatrix}$, where $\langle r_1, r_i\rangle = \langle r\rangle$. Consider a matrix S^i defined such that for all $j \neq 1, i$, $S^i_{j,j} = 1$, and $S^i_{1,1} = a, S^i_{1,i} = b, S^i_{i,1} = -d, S^i_{i,i} = c$, and all other entries are 0. Let $x = \begin{bmatrix} x_1 \\ x_2 \\ \vdots \\ x_n \end{bmatrix}$ such that $x_1 = r_1$ and $x_i = r_i$. By matrix multiplication,

$$S^i x = \begin{bmatrix} r \\ x_2 \\ \vdots \\ x_{i-1} \\ 0 \\ x_{i+1} \\ \vdots \\ x_n \end{bmatrix}$$

Moreover, Let S'^i with $S^i_{j,j} = 1$ for all $j \neq 1, i$, $S^i_{j,j} = 1$, and $S^i_{1,1} = c, S^i_{1,i} = -b, S^i_{i,1} = d, S^i_{i,i} = a$, and all other entries 0. By matrix multiplication, S'^i is the inverse of S^i. Hence, S^i is invertible.

Let $S = S^n S^{n-1} \cdots S^2$. Since the product of invertible matrices is invertible, S is invertible. Moreover, multiplication of a vector by S^i changes only the first entry and reduces the ith entry to 0. Hence, $S\begin{bmatrix} r_1 \\ r_2 \\ \vdots \\ r_n \end{bmatrix} = \begin{bmatrix} r \\ 0 \\ \vdots \\ 0 \end{bmatrix}$. So S is the desired invertible matrix.

Let $\mathbf{r} = \begin{bmatrix} r_1 \\ r_2 \\ \vdots \\ r_n \end{bmatrix}$. Multiplication of $\mathbf{r}$ by S^2 changes r_1 to r'_2, where $\langle r'_2\rangle = \langle r_1, r_2\rangle$. Assume by induction that multiplication of $\mathbf{r}$ by $S^k S^{k-1} \cdots S^2$, where $2 \leq k \leq n-1$, changes r_1 to r'_k such

that $\langle r'_k \rangle = \langle r_1, r_2, \ldots, r_k \rangle$. Then, multiplication of $\mathbf{r}$ by $S^{k+1}S^kS^{k-1}\cdots S^2$ changes r_1 to r'_{k+1}, where $\langle r'_{k+1} \rangle = \langle r'_k, r_{k+1} \rangle$. But since $\langle r'_k \rangle = \langle r_1, r_2, \ldots, r_k \rangle$, we have $\langle r'_{k+1} \rangle = \langle r_1, r_2, \ldots, r_{k+1} \rangle$. This completes the induction and shows multiplication of $\mathbf{r}$ by S changes r_1 to r such that $\langle r \rangle = \langle r_1, r_2, \ldots, r_n \rangle$.

3. Let A_i be an n by m matrix, $A_1 = A$. Let the sequence $A_1, A_2, \ldots$ be constructed as following. If $A_{i,1} = \begin{bmatrix} r_i \\ a_{i,2} \\ \vdots \\ a_{i,n} \end{bmatrix}$ is the first column of A_i, then let S_i be an n by n invertible matrix such that $SA_{i,1} = \begin{bmatrix} r'_i \\ 0 \\ \vdots \\ 0 \end{bmatrix}$, with $\langle r'_i \rangle = \langle r_i, a_{i,2}, \ldots, a_{i,n} \rangle$. Then consider the matrix $(SA)^t$, the transpose of SA. Let $A'_{i,1} = \begin{bmatrix} r'_i \\ a'_{i,2} \\ \vdots \\ a'_{i,m} \end{bmatrix}$ be the first column of $(SA)^t$. Then there exists an m by m invertible matrix T such that $T^tA'_{i,1} = \begin{bmatrix} r_{i+1} \\ 0 \\ \vdots \\ 0 \end{bmatrix}$, where $\langle r_{i+1} \rangle = \langle r'_i, a'_{i,2}, \ldots, a'_{i,n} \rangle$. Let $A_{i+1} = S_iA_iT_i$. Notice that $\langle r_i \rangle \subseteq \langle r_i, a_{i,2}, \ldots, a_{i,n} \rangle = \langle r'_i \rangle \subseteq \langle r'_i, a'_{i,2}, \ldots, a'_{i,n} \rangle = \langle r_{i+1} \rangle$. Notice also that by this method of construction, the only nonzero entry in first row of the matrix A_i is r_i.

   Consider the chain of ideals $\langle r_1 \rangle \subseteq \langle r_2 \rangle \subseteq \langle r_3 \rangle \subseteq \cdots$. Since R is a Noetherian ring, there is a $k \in \mathbb{N}$ such that $\langle r_k \rangle = \langle r_{k+1} \rangle$. Since we have shown above that $\langle r_k \rangle \subseteq \langle r'_k \rangle \subseteq \langle r_{k+1} \rangle$, we also have $\langle r_k \rangle = \langle r'_k \rangle$. But $\langle r'_k \rangle = \langle r_i, a_{k,2}, \ldots, a_{k,n} \rangle$. Hence, for all $2 \leq j \leq n$, $a_{k,j} = x_jr_i$ for some $x_j \in R$. Consider a matrix M such that its diagonal entries are all 1, its first column is $\begin{bmatrix} 1 \\ -x_2 \\ \vdots \\ -x_n \end{bmatrix}$. This is an invertible matrix that takes the first column of A_k to $\begin{bmatrix} r_k \\ 0 \\ \vdots \\ 0 \end{bmatrix}$ without changing the entries in the first row. Let $S = MS_kS_{k-1}\cdots S_2S_1$, $T = T_1T_2\cdots T_{k-1}T_k$. Then, since $A_k = S_kS_{k-1}\cdots S_2S_1AT_1T_2\cdots T_{k-1}T_k$, $SAT = MA_k$ has no nonzero entries in the first row or first column except for the $(1,1)$ entry.

□

Notation: throughout section 4 and 5, $< r_1, r_2, \ldots, r_n >$ or $\langle r_1, r_2, \ldots, r_n \rangle$ is used to denote the ideal or the submodule generated by $r_1, r_2, \ldots, r_n$. If it is clear whether the algebraic structure denoted is an ideal or submodule, we will not specify the algebraic structure.

51 Problem 4.2.4

Proof. Let B be an n by n matrix, C be an n by m matrix. Suppose $B = \begin{bmatrix} b & \mathbf{0}_{n-1}^t \\ \mathbf{0}_{n-1} & B' \end{bmatrix}$, where $b \in R$, $\mathbf{0}_{n-1}$ be the zero-vector in R^{n-1}, and B' be an $n-1$ by $n-1$ vector, and suppose $C = \begin{bmatrix} c & \mathbf{0}_{m-1}^t \\ \mathbf{0}_{n-1} & C' \end{bmatrix}$, where $c \in R$, $\mathbf{0}_{m-1}$ be the zero-vector in R^{m-1}, and C' be an $n-1$ by $m-1$ vector. By matrix multiplication, $BC = \begin{bmatrix} bc & \mathbf{0}_{m-1}^t \\ \mathbf{0}_{n-1} & B'C' \end{bmatrix}$. Notice that if $B = \begin{bmatrix} 1 & \mathbf{0}_{n-1}^t \\ \mathbf{0}_{n-1} & B' \end{bmatrix}$ and B' is invertible, then B is also invertible, since $\begin{bmatrix} 1 & \mathbf{0}_{n-1}^t \\ \mathbf{0}_{n-1} & (B')^{-1} \end{bmatrix}$ is the inverse of B.

□

52 Problem 4.2.5

Proof. (write your solution here) □

53 Problem 4.3.1

Proof. (write your solution here) □

54 Problem 4.3.2

Proof. (write your solution here) □

55 Problem 4.3.3

Proof. (write your solution here) □

56 Problem 4.3.4

Proof. (write your solution here) □

57 Problem 5.1.1

Proof. (write your solution here) □

58 Problem 5.2.1

Proof. (write your solution here) □

59 Problem 5.2.2

Proof. (write your solution here) □

60 Problem 5.2.3

Proof. (write your solution here) □

61 Problem 5.2.4

Proof. (write your solution here) □

62 Problem 5.2.5

Proof. (write your solution here) □

63 Problem 5.3.1

Proof. (write your solution here) □

64 Problem 5.3.2

Proof. (write your solution here) □

65 Problem 5.3.3

Proof. (write your solution here) □

66 Problem 5.3.4

Proof. (write your solution here) □