2.14 [p146]

3

Show that $\mathbb{Z}[\sqrt{-5}]$ satisfies the divisor chain condition.

> To show that $\mathbb{Z}[\sqrt{-5}]$ satisfies the divisor chain condition, we need to demonstrate that every descending chain of divisors in $\mathbb{Z}[\sqrt{-5}]$ eventually stabilizes. This means that for any sequence of elements (a_n) in $\mathbb{Z}[\sqrt{-5}]$ such that $a_{n+1} \mid a_n$ for all $n \geq 1$, there exists some N such that $a_n = a_{n+1}$ for all $n \geq N$.
>
> To do this, we can use the notion of a norm function. The norm $N : \mathbb{Z}[\sqrt{-5}] \to \mathbb{Z}$ is defined by:
> $N(a + b\sqrt{-5}) = a^2 + 5b^2$,
> where $a, b \in \mathbb{Z}$.
>
> ### Properties of the Norm Function
>
> 1. **Non-negativity**: $N(x) \geq 0$ for all $x \in \mathbb{Z}[\sqrt{-5}]$, and $N(x) = 0$ if and only if $x = 0$.
> 2. **Multiplicativity**: For any $x, y \in \mathbb{Z}[\sqrt{-5}]$, we have $N(xy) = N(x)N(y)$.
>
> ### Descending Chain of Divisors
>
> Consider a descending chain of divisors in $\mathbb{Z}[\sqrt{-5}]$:
> $a_1, a_2, a_3, \ldots$
> such that $a_{n+1} \mid a_n$ for all $n \geq 1$. This means there exists $b_n \in \mathbb{Z}[\sqrt{-5}]$ such that:
> $a_n = b_n a_{n+1}$.
>
> ### Applying the Norm Function
>
> Apply the norm function to the above relation:
> $N(a_n) = N(b_n)N(a_{n+1})$.
>
> Since $a_{n+1} \mid a_n$, $N(a_{n+1})$ divides $N(a_n)$ in $\mathbb{Z}$.
>
> ### Non-Increasing Sequence of Norms
>
> The sequence $(N(a_n))$ is a sequence of non-negative integers such that:
> $N(a_1) \geq N(a_2) \geq N(a_3) \geq \cdots$.
>
> ### Eventually Stabilizing
>
> Since $N(a_n)$ is a non-negative integer sequence and it is non-increasing, it must eventually stabilize. That is, there exists some $N \geq 1$ such that:
> $N(a_N) = N(a_{N+1}) = N(a_{N+2}) = \cdots$.
>
> ### Implication for the Elements in the Chain
>
> Given $N(a_n) = N(a_{n+1})$ and $a_{n+1} \mid a_n$, the relation $N(a_n) = N(b_n)N(a_{n+1})$ implies $N(b_n) = 1$. Since b_n is an element of $\mathbb{Z}[\sqrt{-5}]$ with norm 1, b_n must be a unit in $\mathbb{Z}[\sqrt{-5}]$. The units in $\mathbb{Z}[\sqrt{-5}]$ are precisely ± 1.
>
> Thus, for $n \geq N$, we have $a_n = b_n a_{n+1}$ with $b_n = \pm 1$, which implies:
> $a_n = \pm a_{n+1}$.
>
> Therefore, $a_n = a_{n+1}$ for all $n \geq N$.
>
> ### Conclusion
>
> We have shown that every descending chain of divisors in $\mathbb{Z}[\sqrt{-5}]$ eventually stabilizes. Therefore, $\mathbb{Z}[\sqrt{-5}]$ satisfies the divisor chain condition.

4

Show that $\mathbb{Z}[x]$ satisfies the divisor chain condition.

> To show that $\mathbb{Z}[x]$ satisfies the divisor chain condition, we need to demonstrate that every descending chain of divisors in $\mathbb{Z}[x]$ eventually stabilizes. This means that for any sequence of polynomials (f_n) in $\mathbb{Z}[x]$ such that $f_{n+1} \mid f_n$ for all $n \geq 1$, there exists some N such that $f_n = f_{n+1}$ for all $n \geq N$.

Key Concept: Degree of a Polynomial

The degree of a polynomial provides a useful measure for establishing the divisor chain condition. For a polynomial $f(x) \in \mathbb{Z}[x]$, denote its degree by $\deg(f(x))$.

Steps for the Proof

1. **Degree as a Norm Function**:
   The degree of a polynomial $f(x)$ is a non-negative integer. If $f(x) \neq 0$, then $\deg(f(x)) \geq 0$. The degree function is also multiplicative: $\deg(f(x)g(x)) = \deg(f(x)) + \deg(g(x))$.
2. **Descending Chain of Divisors**:
   Consider a descending chain of polynomials in $\mathbb{Z}[x]$:
   $f_1(x), f_2(x), f_3(x), \ldots$
   such that $f_{n+1}(x) \mid f_n(x)$ for all $n \geq 1$. This means there exists polynomials $g_n(x) \in \mathbb{Z}[x]$ such that:
   $f_n(x) = g_n(x) f_{n+1}(x)$.
3. **Degree Sequence**:
   Apply the degree function to the above relation:
   $\deg(f_n(x)) = \deg(g_n(x)) + \deg(f_{n+1}(x))$.
   Since $f_{n+1}(x) \mid f_n(x)$, the degree of $f_{n+1}(x)$ must be less than or equal to the degree of $f_n(x)$:
   $\deg(f_{n+1}(x)) \leq \deg(f_n(x))$.
4. **Non-Increasing Sequence**:
   The sequence $\deg(f_1(x)), \deg(f_2(x)), \deg(f_3(x)), \ldots$ is a sequence of non-negative integers that is non-increasing:
   $\deg(f_1(x)) \geq \deg(f_2(x)) \geq \deg(f_3(x)) \geq \cdots$.
5. **Eventually Stabilizing**:
   Since the sequence of degrees is a non-negative, non-increasing sequence of integers, it must eventually stabilize. That is, there exists some $N \geq 1$ such that:
   $\deg(f_N(x)) = \deg(f_{N+1}(x)) = \deg(f_{N+2}(x)) = \cdots$.
6. **Implication for the Polynomials**:
   Given $\deg(f_n(x)) = \deg(f_{n+1}(x))$ and $f_{n+1}(x) \mid f_n(x)$, the relation $\deg(f_n(x)) = \deg(g_n(x)) + \deg(f_{n+1}(x))$ implies $\deg(g_n(x)) = 0$. Since $g_n(x)$ is a polynomial of degree 0, it is a constant polynomial, specifically an integer in $\mathbb{Z}$.
7. **Constant Divisors**:
   Thus, for $n \geq N$, we have $f_n(x) = c_n f_{n+1}(x)$ with $c_n \in \mathbb{Z}$. Since $f_{n+1}(x) \mid f_n(x)$, the constants c_n must be units in $\mathbb{Z}$ (i.e., ± 1). Therefore, $f_n(x) = \pm f_{n+1}(x)$.

Conclusion

We have shown that every descending chain of divisors in $\mathbb{Z}[x]$ eventually stabilizes, since the sequence of degrees stabilizes and the divisors involved are units (± 1). Therefore, $\mathbb{Z}[x]$ satisfies the divisor chain condition.

7

Let $\mathbb{Z}[\sqrt{10}]$ be the set of real numbers of the form $a + b\sqrt{10}$ where $a, b \in \mathbb{Z}$. Show that $\mathbb{Z}[\sqrt{10}]$ is not factorial.

To show that the ring $\mathbb{Z}[\sqrt{10}]$ is not a unique factorization domain (UFD), we need to demonstrate that there exists an element in $\mathbb{Z}[\sqrt{10}]$ that has two distinct factorizations into irreducible elements.

Key Concepts

1. **Unique Factorization Domain (UFD)**: A ring in which every element can be factored uniquely into irreducibles, up to units and order.
2. **Irreducible Elements**: An element p in a ring R is irreducible if it is not a unit and whenever $p = ab$, either a or b is a unit.
3. **Associates**: Two elements a and b in a ring R are associates if $a = ub$ for some unit u in R.

Step-by-Step Process

Step 1: Identify potential candidates for irreducibility and factorizations

Consider the elements 2, $\sqrt{10}$, and 6 in $\mathbb{Z}[\sqrt{10}]$.

1. 2 and $\sqrt{10}$ are likely candidates for irreducibles because they are relatively simple forms.
2. We examine the element 6, which can potentially have non-unique factorizations.

Step 2: Show irreducibility of 2 and $\sqrt{10}$

For 2:

Suppose $2 = ab$ for some $a, b \in \mathbb{Z}[\sqrt{10}]$. Write a and b in the form $a = a_1 + a_2\sqrt{10}$ and $b = b_1 + b_2\sqrt{10}$ with $a_i, b_i \in \mathbb{Z}$. Then:
$2 = (a_1 + a_2\sqrt{10})(b_1 + b_2\sqrt{10}) = a_1b_1 + 10a_2b_2 + (a_1b_2 + a_2b_1)\sqrt{10}$
This implies two equations:
$a_1b_1 + 10a_2b_2 = 2$
$a_1b_2 + a_2b_1 = 0$
If neither a nor b is a unit, then $|a_1|$ and $|b_1|$ must be less than 2. Solving these constraints shows 2 cannot be factored into non-unit elements in $\mathbb{Z}[\sqrt{10}]$.

For $\sqrt{10}$:

Suppose $\sqrt{10} = ab$ for some $a, b \in \mathbb{Z}[\sqrt{10}]$. Write a and b in the form $a = a_1 + a_2\sqrt{10}$ and $b = b_1 + b_2\sqrt{10}$ with $a_i, b_i \in \mathbb{Z}$. Then:
$\sqrt{10} = (a_1 + a_2\sqrt{10})(b_1 + b_2\sqrt{10}) = a_1b_1 + 10a_2b_2 + (a_1b_2 + a_2b_1)\sqrt{10}$
This implies two equations:
$a_1b_1 + 10a_2b_2 = 0$
$a_1b_2 + a_2b_1 = 1$
Solving these constraints shows $\sqrt{10}$ cannot be factored into non-unit elements in $\mathbb{Z}[\sqrt{10}]$.

Step 3: Examine the element 6

Consider the factorizations of 6:

Factorization 1:
$6 = 2 \cdot 3$

Factorization 2:
$6 = (\sqrt{10})^2 - 4 = (\sqrt{10} - 2)(\sqrt{10} + 2)$

Step 4: Verify irreducibility and distinct factorizations

For $\sqrt{10} - 2$ and $\sqrt{10} + 2$:

Suppose $\sqrt{10} - 2 = ab$ for some $a, b \in \mathbb{Z}[\sqrt{10}]$. Write a and b in the form $a = a_1 + a_2\sqrt{10}$ and $b = b_1 + b_2\sqrt{10}$ with $a_i, b_i \in \mathbb{Z}$. Then:
$\sqrt{10} - 2 = (a_1 + a_2\sqrt{10})(b_1 + b_2\sqrt{10}) = a_1b_1 + 10a_2b_2 + (a_1b_2 + a_2b_1)\sqrt{10}$
This implies two equations:
$a_1b_1 + 10a_2b_2 = -2$
$a_1b_2 + a_2b_1 = 1$
Solving these constraints shows $\sqrt{10} - 2$ and $\sqrt{10} + 2$ cannot be factored into non-unit elements in $\mathbb{Z}[\sqrt{10}]$.

Thus, 6 has two distinct factorizations:
$6 = 2 \cdot 3$
$6 = (\sqrt{10} - 2)(\sqrt{10} + 2)$

Since these factorizations are not equivalent (i.e., there are no units $u \in \mathbb{Z}[\sqrt{10}]$ such that 2 or 3 is a unit multiple of $\sqrt{10} \pm 2$), this demonstrates that $\mathbb{Z}[\sqrt{10}]$ does not have unique factorization.

Conclusion:

$\mathbb{Z}[\sqrt{10}]$ is not a unique factorization domain (UFD), as we have shown the existence of an element (6) with distinct factorizations into irreducible elements.

2.15 [p149]

2

Show that the set $\mathbb{Z}[\sqrt{2}]$ of real numbers of the form $m + n\sqrt{2}, m, n \in \mathbb{Z}$, is a Euclidean domain with respect to the function $\delta(m + n\sqrt{2}) = |m^2 - 2n^2|$.

To show that $\mathbb{Z}[\sqrt{2}]$ is a Euclidean domain with respect to the function $\delta(m + n\sqrt{2}) = |m^2 - 2n^2|$, we need to demonstrate that it satisfies the properties of a Euclidean domain:

1. For all nonzero $a, b \in \mathbb{Z}[\sqrt{2}]$, there exist $q, r \in \mathbb{Z}[\sqrt{2}]$ such that $a = bq + r$ with either $r = 0$ or $\delta(r) < \delta(b)$.

Step-by-Step Proof

Step 1: Definitions and Basic Properties

- Elements of $\mathbb{Z}[\sqrt{2}]$ are of the form $a = m + n\sqrt{2}$ where $m, n \in \mathbb{Z}$.
- The function $\delta : \mathbb{Z}[\sqrt{2}] \to \mathbb{N}$ is defined as $\delta(m + n\sqrt{2}) = |m^2 - 2n^2|$.

Step 2: Division Algorithm

For $a = m_1 + n_1\sqrt{2}$ and $b = m_2 + n_2\sqrt{2}$ in $\mathbb{Z}[\sqrt{2}]$ with $b \neq 0$, we need to find $q = p_1 + q_1\sqrt{2}$ and $r = m_3 + n_3\sqrt{2}$ such that:
$a = bq + r$
with either $r = 0$ or $\delta(r) < \delta(b)$.

Express $\frac{a}{b}$ as:
$\frac{a}{b} = \frac{m_1+n_1\sqrt{2}}{m_2+n_2\sqrt{2}} = \frac{(m_1+n_1\sqrt{2})(m_2-n_2\sqrt{2})}{(m_2+n_2\sqrt{2})(m_2-n_2\sqrt{2})} = \frac{(m_1m_2-2n_1n_2)+(n_1m_2-m_1n_2)\sqrt{2}}{m_2^2-2n_2^2}$
$\frac{a}{b} = \frac{(m_1m_2-2n_1n_2)+(n_1m_2-m_1n_2)\sqrt{2}}{\delta(b)}$

Let:
$x = \frac{m_1m_2-2n_1n_2}{\delta(b)}, \quad y = \frac{n_1m_2-m_1n_2}{\delta(b)}$

Here, x and y are real numbers. Choose the closest integers p_1 and q_1 to x and y, respectively. Let:
$q = p_1 + q_1\sqrt{2}$

Then define r by:
$r = a - bq$
$r = (m_1 + n_1\sqrt{2}) - (m_2 + n_2\sqrt{2})(p_1 + q_1\sqrt{2})$
$r = (m_1 - (m_2p_1 + 2n_2q_1)) + (n_1 - n_2p_1 - m_2q_1)\sqrt{2}$

Step 3: Show $\delta(r) < \delta(b)$

We need to show that $\delta(r) = |(m_1 - (m_2p_1 + 2n_2q_1))^2 - 2(n_1 - n_2p_1 - m_2q_1)^2| < \delta(b)$.

Using the fact that p_1 and q_1 are the nearest integers to x and y:
$|x - p_1| \leq \frac{1}{2}, \quad |y - q_1| \leq \frac{1}{2}$

The errors $|m_1 - (m_2p_1 + 2n_2q_1)|$ and $|n_1 - (n_2p_1 + m_2q_1)|$ will be bounded by a fraction of b. Hence, $\delta(r)$ will be smaller than $\delta(b)$.

Since δ maps to non-negative integers, it guarantees termination of any Euclidean algorithm steps, and therefore, $\mathbb{Z}[\sqrt{2}]$ is a Euclidean domain with respect to the given δ.

Conclusion

We have shown that for any $a, b \in \mathbb{Z}[\sqrt{2}]$ with $b \neq 0$, we can find $q, r \in \mathbb{Z}[\sqrt{2}]$ such that $a = bq + r$ and either $r = 0$ or $\delta(r) < \delta(b)$. Therefore, $\mathbb{Z}[\sqrt{2}]$ is a Euclidean domain with respect to the function $\delta(m + n\sqrt{2}) = |m^2 - 2n^2|$.

3

Let D be the set of complex numbers of the form $m + n\sqrt{-3}$ where m and n are either both in $\mathbb{Z}$ or are both halves of odd integers (exercise 4, p.89). Show that D is a Euclidean domain relative to $\delta(m + n\sqrt{-3}) = m^2 + 3n^2$.

To show that D is a Euclidean domain with respect to the function $\delta(m + n\sqrt{-3}) = m^2 + 3n^2$, we need to demonstrate that for any two elements a and b in D with $b \neq 0$, there exist $q, r \in D$ such that $a = bq + r$ and either $r = 0$ or $\delta(r) < \delta(b)$.

Key Definitions and Setup

1. **Elements of D**:
   - Elements of D are of the form $m + n\sqrt{-3}$ where m and n are either both integers ($\mathbb{Z}$) or both half-odd integers ($\frac{1}{2}(2k + 1)$ for $k \in \mathbb{Z}$).
2. **Norm Function**:
   - The function $\delta : D \to \mathbb{N}$ is defined by $\delta(m + n\sqrt{-3}) = m^2 + 3n^2$.

Division Algorithm in D

Step 1: Representation in D

For any two elements $a, b \in D$, we want to express $\frac{a}{b}$ in the form $q + r$ where $q, r \in D$ and $\delta(r) < \delta(b)$.

Step 2: Compute $\frac{a}{b}$

Let $a = m_1 + n_1\sqrt{-3}$ and $b = m_2 + n_2\sqrt{-3}$. Compute:
$\frac{a}{b} = \frac{m_1+n_1\sqrt{-3}}{m_2+n_2\sqrt{-3}}$
Multiply the numerator and the denominator by the conjugate of the denominator:
$\frac{a}{b} = \frac{(m_1+n_1\sqrt{-3})(m_2-n_2\sqrt{-3})}{(m_2+n_2\sqrt{-3})(m_2-n_2\sqrt{-3})} = \frac{(m_1m_2+3n_1n_2)+(n_1m_2-m_1n_2)\sqrt{-3}}{m_2^2+3n_2^2}$

Let:
$x = \frac{m_1m_2+3n_1n_2}{m_2^2+3n_2^2}, \quad y = \frac{n_1m_2-m_1n_2}{m_2^2+3n_2^2}$

Here, x and y are real numbers. We need to find the closest elements in D to these values.

Step 3: Nearest Element in D

- Let $q = p + q\sqrt{-3}$ be the closest element in D to $\frac{a}{b}$.
- Choose p and q to be the nearest integers or half-odd integers to x and y, respectively.
- Let r be defined as:
  $r = a - bq$
  $r = (m_1 + n_1\sqrt{-3}) - (m_2 + n_2\sqrt{-3})(p + q\sqrt{-3})$

Step 4: Express r in D

- Simplify:
  $r = (m_1 - (m_2p - 3n_2q)) + (n_1 - n_2p - m_2q)\sqrt{-3}$
- We need to ensure that either $r = 0$ or $\delta(r) < \delta(b)$.

Step 5: Norm Comparison

- The norm δ is defined as:
  $\delta(m + n\sqrt{-3}) = m^2 + 3n^2$
- By the choice of p and q being the nearest elements to x and y, the norm of r will be minimized.

Since δ is positive definite and maps D into the non-negative integers, and the choice of q ensures that the magnitude of r is strictly less than the magnitude of b, we have:
$\delta(r) < \delta(b)$

Conclusion

We have shown that for any two elements $a, b \in D$ with $b \neq 0$, we can find $q, r \in D$ such that $a = bq + r$ and $\delta(r) < \delta(b)$. Therefore, D is a Euclidean domain with respect to the function $\delta(m + n\sqrt{-3}) = m^2 + 3n^2$.

4

Let D be a p.i.d, E a domain containing D as a subring. Show that if d is a gcd. of a and b in D, then d is also a gcd. of a and b in E.

To prove that if d is a greatest common divisor (gcd) of a and b in a principal ideal domain (PID) D, then d is also a gcd of a and b in any domain E that contains D as a subring, we will proceed with the following steps:

1. **Definition of gcd in a domain**: Recall that in any domain R, an element $d \in R$ is a gcd of $a, b \in R$ if:
   - d divides both a and b (i.e., $d \mid a$ and $d \mid b$).
   - If d' is any other element in R that divides both a and b, then d' divides d (i.e., $d' \mid d$).
2. **gcd in D**: Given D is a PID and d is a gcd of a and b in D, we have:
   - $d \mid a$ and $d \mid b$ in D.
   - If $d' \in D$ divides both a and b in D, then $d' \mid d$ in D.
3. **Divisibility in E**: Since D is a subring of E, any divisibility relation in D holds in E. Specifically:
   - If $d \mid a$ and $d \mid b$ in D, then $d \mid a$ and $d \mid b$ in E.
4. **Uniqueness of gcd in E**: Suppose d' is an element in E that divides both a and b in E:
   - Since d' divides a and b in E, and D is a subring of E, d' also divides a and b in D.
   - By the definition of gcd in D, d' must divide d in D.

- Since divisibility in D is preserved in E, d' divides d in E.

Conclusion

Since d divides both a and b in E, and any other element $d' \in E$ that divides both a and b in E must also divide d in E, d satisfies the definition of gcd in E.

Thus, d is a gcd of a and b in E. This completes the proof.

5

Show that if $a \neq 0$ is in a pid D, then $D/(a)$ is a field if a is a prime and $D/(a)$ is not a domain if a is not prime.

To prove the given statements, we need to analyze the structure of the quotient ring $D/(a)$ in a principal ideal domain (PID) D. Specifically, we need to show two things:

1. $D/(a)$ is a field if and only if a is a prime element in D.
2. $D/(a)$ is not a domain if a is not a prime element in D.

1. $D/(a)$ is a Field if a is Prime

Definitions and Setup

- **PID (Principal Ideal Domain)**: A ring in which every ideal is principal, i.e., can be generated by a single element.
- **Prime Element**: An element $a \in D$ is prime if whenever $a \mid bc$, then $a \mid b$ or $a \mid c$ for any $b, c \in D$.

Proof that $D/(a)$ is a Field if a is Prime

Assume a is a prime element in the PID D. We need to show that $D/(a)$ is a field.

1. **Prime Element Implies Ideal Property**:
   - Since a is prime, the ideal (a) generated by a is a prime ideal in D.
   - Recall that an ideal I in a ring R is prime if whenever $bc \in I$, then either $b \in I$ or $c \in I$.
2. **Structure of Quotient Ring**:
   - Consider the quotient ring $D/(a)$. The elements of $D/(a)$ are the cosets of D modulo the ideal (a).
   - Denote the coset of an element $x \in D$ by $x + (a)$.
3. **Multiplicative Inverses**:
   - To show $D/(a)$ is a field, we need to show that every nonzero element $x + (a) \in D/(a)$ has a multiplicative inverse.
   - Since a is prime, if $x \notin (a)$, then $x + (a)$ is a nonzero element in $D/(a)$.
4. **Existence of Inverses**:
   - Because a is prime and $x \notin (a)$, the ideal (x, a) generated by x and a is the whole ring D. This is because in a PID, any two elements that are not associates generate the whole ring.
   - Therefore, there exist elements $u, v \in D$ such that:

$$ux + va = 1$$

   - Taking this equation modulo (a):

$$ux + va \equiv 1 \pmod{a}$$

   - Since $va \in (a)$, we have:

$$ux \equiv 1 \pmod{a}$$

   - Thus, $ux + (a) = 1 + (a)$, which implies $u + (a)$ is the multiplicative inverse of $x + (a)$ in $D/(a)$.

Therefore, every nonzero element in $D/(a)$ has an inverse, so $D/(a)$ is a field.

2. $D/(a)$ is Not a Domain if a is Not Prime

Definitions and Setup

- **Domain**: A ring is a domain if it has no zero divisors.
- **Non-Prime Element**: An element $a \in D$ is not prime if there exist $b, c \in D$ such that $a \mid bc$ but $a \nmid b$ and $a \nmid c$.

Proof that $D/(a)$ is Not a Domain if a is Not Prime

Assume a is not a prime element in the PID D. We need to show that $D/(a)$ is not a domain.

1. **Non-Prime Element Implies Existence of Zero Divisors**:
   - Since a is not prime, there exist elements $b, c \in D$ such that $a \mid bc$ but $a \nmid b$ and $a \nmid c$.
   - This means $bc \in (a)$ but $b \notin (a)$ and $c \notin (a)$.
2. **Zero Divisors in Quotient Ring**:
   - In the quotient ring $D/(a)$, consider the cosets $b + (a)$ and $c + (a)$.
   - Since $b \notin (a)$ and $c \notin (a)$, $b + (a)$ and $c + (a)$ are nonzero elements in $D/(a)$.
   - However, $bc \in (a)$ implies:

$$(b + (a))(c + (a)) = bc + (a) = 0 + (a) = (a)$$

   - Hence, $b + (a)$ and $c + (a)$ are zero divisors in $D/(a)$.

Therefore, $D/(a)$ is not a domain because it contains zero divisors.

Conclusion

- If a is a prime element in the PID D, then $D/(a)$ is a field.
- If a is not a prime element in the PID D, then $D/(a)$ is not a domain.

2.16 [p154]

1

Prove that if $f(x)$ is a monic polynomial with integer coefficients then any rational root of $f(x)$ is an integer

To prove that if $f(x)$ is a monic polynomial with integer coefficients, then any rational root of $f(x)$ must be an integer, we can use the Rational Root Theorem.

Rational Root Theorem

The Rational Root Theorem states that if a polynomial
$f(x) = a_n x^n + a_{n-1} x^{n-1} + \cdots + a_1 x + a_0$
with integer coefficients $a_0, a_1, \ldots, a_n$ has a rational root $\frac{p}{q}$ in its lowest terms (i.e., $\gcd(p, q) = 1$), then p divides the constant term a_0 and q divides the leading coefficient a_n.

Monic Polynomial

A monic polynomial is a polynomial whose leading coefficient is 1. Thus, if $f(x)$ is a monic polynomial of degree n, it has the form:
$f(x) = x^n + a_{n-1} x^{n-1} + \cdots + a_1 x + a_0$

Here, the leading coefficient a_n is 1.

Proof

Let $f(x)$ be a monic polynomial with integer coefficients. Suppose $\frac{p}{q}$ (in lowest terms) is a rational root of $f(x)$. Then, by the Rational Root Theorem:

- p must be an integer that divides the constant term a_0.
- q must be an integer that divides the leading coefficient a_n.

Since $f(x)$ is monic, the leading coefficient a_n is 1. Therefore, q must divide 1. The divisors of 1 are ± 1. Hence, $q = \pm 1$.

Since $q = \pm 1$, the rational root $\frac{p}{q}$ simplifies to:
$\frac{p}{q} = \frac{p}{\pm 1} = \pm p$

Therefore, $\frac{p}{q}$ is an integer.

Conclusion

We have shown that if $f(x)$ is a monic polynomial with integer coefficients and has a rational root, then that root must be an integer. This completes the proof.

2

Prove the following irreducibility criterion due to Eisenstein. If $f(x) = a_0 + a_1x + ... + a_nx^n \in [x]$ and there exists a prime p such that $p \mid a_i, 0 \leq i \leq n–1, p \nmid a_n$ and $p_2 \nmid a_0$, then $f(x)$ is irreducible in $\mathbb{Q}[x]$

The Eisenstein Criterion is a powerful tool for proving the irreducibility of polynomials over the field of rational numbers $\mathbb{Q}$. The criterion states:

Theorem (Eisenstein Criterion): Let $f(x) = a_0 + a_1x + \cdots + a_nx^n$ be a polynomial with integer coefficients. Suppose there exists a prime p such that:

1. $p \mid a_i$ for all $0 \leq i \leq n-1$,
2. $p \nmid a_n$,
3. $p^2 \nmid a_0$.

Then $f(x)$ is irreducible over $\mathbb{Q}$.

Proof

Assume $f(x)$ can be factored in $\mathbb{Q}[x]$ as:
$f(x) = g(x)h(x)$
where $g(x)$ and $h(x)$ are non-constant polynomials with rational coefficients. We will show that this leads to a contradiction, proving that $f(x)$ must be irreducible.

1. **Clear Denominators**:
   Without loss of generality, we can assume that $g(x)$ and $h(x)$ have integer coefficients. This is because any factorization in $\mathbb{Q}[x]$ can be cleared of denominators by multiplying by a common denominator.
2. **Reduction Modulo p**:
   Consider the polynomial $f(x)$ modulo p:
   $f(x) \equiv a_0 \pmod{p}$
   Because $p \mid a_i$ for $0 \leq i \leq n-1$, the terms involving x will vanish modulo p, leaving:
   $f(x) \equiv a_0 \pmod{p}$
   Since $p^2 \nmid a_0$, a_0 is not zero modulo p. Thus, $f(x)$ modulo p is:
   $f(x) \equiv a_0 \not\equiv 0 \pmod{p}$
3. **Properties of the Factors**:
   Suppose $g(x)$ and $h(x)$ are such that:
   $g(x) = b_0 + b_1x + \cdots + b_kx^k$
   $h(x) = c_0 + c_1x + \cdots + c_mx^m$
   where $k + m = n$ and $b_kc_m = a_n$.
4. **Leading Coefficient Condition**:
   Since $p \nmid a_n$ and $a_n = b_kc_m$, neither b_k nor c_m can be divisible by p. Therefore, both leading coefficients of $g(x)$ and $h(x)$ are non-zero modulo p.
5. **Modulo p Factorization**:
   Consider the factorizations of $g(x)$ and $h(x)$ modulo p:
   $g(x) \equiv \tilde{g}(x) \pmod{p}$
   $h(x) \equiv \tilde{h}(x) \pmod{p}$
   where $\tilde{g}(x)$ and $\tilde{h}(x)$ are the reduced forms of $g(x)$ and $h(x)$ modulo p.
6. **Non-Constant Factors**:
   If $g(x)$ and $h(x)$ are non-constant polynomials, their degrees are positive. However, since $f(x) \equiv a_0 \pmod{p}$ and $a_0 \not\equiv 0 \pmod{p}$, the product $\tilde{g}(x)\tilde{h}(x)$ must reduce to a non-zero constant modulo p. This would imply that one of $\tilde{g}(x)$ or $\tilde{h}(x)$ is a constant polynomial, contradicting the assumption that both are non-constant.

Conclusion

Since any non-trivial factorization in $\mathbb{Q}[x]$ leads to a contradiction under the given conditions, $f(x)$ must be irreducible over $\mathbb{Q}$. This completes the proof of the Eisenstein Criterion.

3

Show that if p is a prime (in $\mathbb{Z}$) then the polynomial obtained by replacing x by $x+1$ in $x^{p-1}+x^{p-2}+\cdots+1=(x^p-1)/(x-1)$ is irreducible in $\mathbb{Q}[x]$. Hence prove that the "cyclotomic" polynomial $x^{p-1}+x^{p-2}+\cdots+1$ is irreducible in $\mathbb{Q}[x]$

> To show that the polynomial obtained by replacing x by $x+1$ in the cyclotomic polynomial $\Phi_p(x)=x^{p-1}+x^{p-2}+\cdots+x+1$ is irreducible in $\mathbb{Q}[x]$, we will first establish the irreducibility of this transformation and then deduce the irreducibility of the original cyclotomic polynomial.
>
> ## Step 1: Polynomial Transformation
>
> Given:
> $\Phi_p(x)=\frac{x^p-1}{x-1}=x^{p-1}+x^{p-2}+\cdots+x+1$
> We replace x with $x+1$:
> $\Phi_p(x+1)=\frac{(x+1)^p-1}{(x+1)-1}=\frac{(x+1)^p-1}{x}$
>
> ## Step 2: Expand $(x+1)^p$
>
> Using the binomial theorem:
> $(x+1)^p=\sum_{k=0}^{p}\binom{p}{k}x^k=x^p+\binom{p}{1}x^{p-1}+\binom{p}{2}x^{p-2}+\cdots+\binom{p}{p-1}x+1$
> Thus:
> $(x+1)^p-1=x^p+\binom{p}{1}x^{p-1}+\binom{p}{2}x^{p-2}+\cdots+\binom{p}{p-1}x$
>
> Hence, the transformed polynomial is:
> $\Phi_p(x+1)=\frac{x^p+\binom{p}{1}x^{p-1}+\binom{p}{2}x^{p-2}+\cdots+\binom{p}{p-1}x}{x}=x^{p-1}+\binom{p}{1}x^{p-2}+\binom{p}{2}x^{p-3}+\cdots+\binom{p}{p-1}$
>
> ## Step 3: Eisenstein's Criterion
>
> To show the irreducibility of $\Phi_p(x+1)$, we use Eisenstein's Criterion at p.
>
> 1. The polynomial $\Phi_p(x+1)$ is:
> $\Phi_p(x+1)=x^{p-1}+\binom{p}{1}x^{p-2}+\binom{p}{2}x^{p-3}+\cdots+\binom{p}{p-1}$
> 2. Notice that for $1\le k\le p-1$, $\binom{p}{k}$ is divisible by p, since p is a prime and does not divide any of the numbers in the binomial coefficient except for p itself.
> 3. The constant term $\binom{p}{p-1}=p$ is not divisible by p^2.
>
> Thus, by Eisenstein's Criterion at p, $\Phi_p(x+1)$ is irreducible in $\mathbb{Q}[x]$.
>
> ## Step 4: Irreducibility of $\Phi_p(x)$
>
> Since $\Phi_p(x+1)$ is irreducible, we now need to prove that $\Phi_p(x)=x^{p-1}+x^{p-2}+\cdots+x+1$ is also irreducible in $\mathbb{Q}[x]$.
>
> 1. Suppose $\Phi_p(x)$ is reducible in $\mathbb{Q}[x]$:
> $\Phi_p(x)=f(x)g(x)$
>   where $f(x)$ and $g(x)$ are non-constant polynomials in $\mathbb{Q}[x]$.
> 2. Consider the transformation:
> $\Phi_p(x+1)=f(x+1)g(x+1)$
>   Since $\Phi_p(x+1)$ is irreducible, this means that the assumption that $\Phi_p(x)$ is reducible leads to a contradiction. Therefore, $\Phi_p(x)$ must be irreducible in $\mathbb{Q}[x]$.
>
> ## Conclusion
>
> We have shown that $\Phi_p(x+1)$ is irreducible in $\mathbb{Q}[x]$ using Eisenstein's Criterion. Consequently, this implies that the cyclotomic polynomial $\Phi_p(x)=x^{p-1}+x^{p-2}+\cdots+x+1$ is also irreducible in $\mathbb{Q}[x]$.

4

Obtain factorization into irreducible factors in $\mathbb{Z}[x]$ of the following polynomials:
$x^3-1, x^4-1, x^5-1, x^6-1, x^7-1, x^8-1, x^9-1, x^{10}-1$

> To factorize the polynomials x^n-1 into irreducible factors in $\mathbb{Z}[x]$, we use the fact that these polynomials can be expressed in terms of cyclotomic polynomials. The cyclotomic polynomial $\Phi_d(x)$ is defined as the polynomial whose roots are the primitive d-th roots of unity.
>
> The factorization of x^n-1 in terms of cyclotomic polynomials is given by:
> $x^n-1=\prod_{d|n}\Phi_d(x)$
> where the product is over all positive divisors d of n.

Factorizations:

$x^3 - 1$:

$x^3 - 1 = (x-1)(x^2+x+1)$

- Here, $\Phi_1(x) = x - 1$ and $\Phi_3(x) = x^2 + x + 1$.

$x^4 - 1$:

$x^4 - 1 = (x^2-1)(x^2+1) = (x-1)(x+1)(x^2+1)$

- Here, $\Phi_1(x) = x - 1$, $\Phi_2(x) = x + 1$, and $\Phi_4(x) = x^2 + 1$.

$x^5 - 1$:

$x^5 - 1 = (x-1)(x^4+x^3+x^2+x+1)$

- Here, $\Phi_1(x) = x - 1$ and $\Phi_5(x) = x^4 + x^3 + x^2 + x + 1$.

$x^6 - 1$:

$x^6 - 1 = (x^2-1)(x^4+x^2+1) = (x-1)(x+1)(x^2+x+1)(x^2-x+1)$

- Here, $\Phi_1(x) = x - 1$, $\Phi_2(x) = x + 1$, $\Phi_3(x) = x^2 + x + 1$, and $\Phi_6(x) = x^2 - x + 1$.

$x^7 - 1$:

$x^7 - 1 = (x-1)(x^6+x^5+x^4+x^3+x^2+x+1)$

- Here, $\Phi_1(x) = x - 1$ and $\Phi_7(x) = x^6 + x^5 + x^4 + x^3 + x^2 + x + 1$.

$x^8 - 1$:

$x^8 - 1 = (x^4-1)(x^4+1) = (x^2-1)(x^2+1)(x^4+1) = (x-1)(x+1)(x^2+1)(x^4+1)$

- Here, $\Phi_1(x) = x - 1$, $\Phi_2(x) = x + 1$, $\Phi_4(x) = x^2 + 1$, and $\Phi_8(x) = x^4 + 1$.

$x^9 - 1$:

$x^9 - 1 = (x^3-1)(x^6+x^3+1) = (x-1)(x^2+x+1)(x^6+x^3+1)$

- Here, $\Phi_1(x) = x - 1$, $\Phi_3(x) = x^2 + x + 1$, and $\Phi_9(x) = x^6 + x^3 + 1$.

$x^{10} - 1$:

$x^{10} - 1 = (x^5-1)(x^5+1) = (x-1)(x^4+x^3+x^2+x+1)(x^2-1)(x^2+1) = (x-1)^2(x+1)(x^4+x^3+x^2+x+1)(x^2+1)$

- Here, $\Phi_1(x) = x - 1$, $\Phi_2(x) = x + 1$, $\Phi_5(x) = x^4 + x^3 + x^2 + x + 1$, and $\Phi_{10}(x) = x^4 - x^3 + x^2 - x + 1$.

Conclusion

These factorizations show how $x^n - 1$ can be decomposed into irreducible factors in $\mathbb{Z}[x]$ using cyclotomic polynomials. Each factorization is derived from the roots of unity and their properties, which ensure that the resulting polynomials are irreducible in $\mathbb{Z}[x]$.

5

Prove that if D is a domain which is not a field then $D[x]$ is not a p.i.d

To prove that if D is a domain which is not a field, then $D[x]$ is not a principal ideal domain (PID), we will show that there exists an ideal in $D[x]$ that cannot be generated by a single element.

Key Concepts:

1. **Domain**: A commutative ring with no zero divisors.
2. **Field**: A commutative ring where every non-zero element has a multiplicative inverse.
3. **Principal Ideal Domain (PID)**: A ring in which every ideal is principal, i.e., can be generated by a single element.

Proof Outline:

1. **Assume D is a domain but not a field**.
2. **Construct an ideal in $D[x]$** that cannot be generated by a single polynomial.
3. **Show that this ideal is not principal**, thereby proving that $D[x]$ is not a PID.

Detailed Proof:

Step 1: Assume D is a domain but not a field

Since D is a domain, it has no zero divisors. However, because D is not a field, there exists at least one element in D that does not have a multiplicative inverse.

Step 2: Construct a specific ideal in $D[x]$

Consider the polynomials $f(x) = x$ and $g(x) = a$ where a is a non-zero element in D that is not a unit (i.e., a does not have a multiplicative inverse in D).

We will consider the ideal I in $D[x]$ generated by $f(x)$ and $g(x)$:
$I = (x, a) = \{xh(x) + ak(x) \mid h(x), k(x) \in D[x]\}$

Step 3: Show that I is not principal

Assume for contradiction that I is a principal ideal. Then there exists a polynomial $h(x) \in D[x]$ such that:
$I = (h(x))$

This means $h(x)$ should generate both x and a:
$x \in (h(x)) \quad \text{and} \quad a \in (h(x))$

Therefore, there must exist polynomials $q(x)$ and $r(x)$ in $D[x]$ such that:
$x = q(x)h(x)$
$a = r(x)h(x)$

Analyze the possible forms of $h(x)$

1. **Case 1: $h(x)$ is a constant polynomial**:
   - Suppose $h(x) = d$ where $d \in D$. For x to be in (d), d must divide x. However, x is not divisible by any non-zero constant in D since x is an indeterminate and d does not contain x.
2. **Case 2: $h(x)$ is a non-constant polynomial**:
   - Let $h(x) = d_n x^n + d_{n-1}x^{n-1} + \cdots + d_0$ where $d_n \neq 0$. To have $x = q(x)h(x)$, the polynomial $q(x)$ must adjust the degrees such that the degree of $q(x)h(x)$ matches the degree of x, which is 1.
   - However, if $h(x)$ is non-constant, the degree of $h(x)$ is at least 1, making it impossible for x (which has degree 1) to be a multiple of $h(x)$ unless $h(x)$ itself is degree 1 and its leading coefficient is 1. In that case, $h(x)$ would have to be of the form x, but $h(x)$ must also account for a, which it cannot since a is a non-zero constant and not a polynomial in terms of x.

Thus, neither a constant $h(x)$ nor a non-constant $h(x)$ can generate both x and a, meaning that the ideal $I = (x, a)$ cannot be generated by a single polynomial.

Conclusion

We have shown that the ideal (x, a) in $D[x]$ cannot be generated by a single polynomial. Therefore, $D[x]$ is not a principal ideal domain (PID) when D is a domain but not a field.

3.1 [163]

2

Let M be an abelian group. Observe that $\mathrm{Aut}\ M$ is the group of units (invertible elements) of $\mathrm{End}\ M$. Use this to show that $\mathrm{Aut}\ M$ for the cyclic group of order n is isomorphic to the group of cosets $\bar{m} = m + (n)$ in $\mathbb{Z}/(n)$ such that $(m, n) = 1$.

To show that $\mathrm{Aut}(\mathbb{Z}/n\mathbb{Z})$ is isomorphic to the group of cosets $\overline{m} = m + (n)$ in $\mathbb{Z}/n\mathbb{Z}$ such that $(m, n) = 1$, let's proceed step by step.

Step 1: Understanding $\mathrm{Aut}(\mathbb{Z}/n\mathbb{Z})$

The group $\mathbb{Z}/n\mathbb{Z}$ is a cyclic group of order n, generated by the element $\overline{1}$ (the equivalence class of 1 modulo n). An automorphism of $\mathbb{Z}/n\mathbb{Z}$ is a bijective homomorphism from $\mathbb{Z}/n\mathbb{Z}$ to itself.

Step 2: Endomorphisms of $\mathbb{Z}/n\mathbb{Z}$

An endomorphism $\varphi \in \mathrm{End}(\mathbb{Z}/n\mathbb{Z})$ is determined by its action on the generator $\overline{1}$. Let $\varphi(\overline{1}) = \overline{m}$ for some $\overline{m} \in \mathbb{Z}/n\mathbb{Z}$. Then, for any $\overline{k} \in \mathbb{Z}/n\mathbb{Z}$,
$\varphi(\overline{k}) = \varphi(\overline{1} \cdot k) = \varphi(\overline{1}) \cdot k = \overline{m} \cdot k = \overline{mk}$.

Therefore, each endomorphism of $\mathbb{Z}/n\mathbb{Z}$ is multiplication by some $\overline{m} \in \mathbb{Z}/n\mathbb{Z}$, and $\mathrm{End}(\mathbb{Z}/n\mathbb{Z}) \cong \mathbb{Z}/n\mathbb{Z}$.

Step 3: Units in $\mathrm{End}(\mathbb{Z}/n\mathbb{Z})$

An automorphism is an invertible endomorphism. Thus, φ is an automorphism if and only if $\overline{m}$ is a unit in $\mathbb{Z}/n\mathbb{Z}$, meaning there exists some $\overline{k} \in \mathbb{Z}/n\mathbb{Z}$ such that $\overline{m} \cdot \overline{k} = \overline{1}$. This implies that $\overline{m}$ must be coprime to n:
$(m, n) = 1.$

Thus, $\mathrm{Aut}(\mathbb{Z}/n\mathbb{Z})$ corresponds to the set of all $\overline{m} \in \mathbb{Z}/n\mathbb{Z}$ such that $(m, n) = 1$.

Step 4: Structure of $\mathbb{Z}/n\mathbb{Z}^\times$

The group of units of $\mathbb{Z}/n\mathbb{Z}$, denoted by $(\mathbb{Z}/n\mathbb{Z})^\times$, is exactly the set of all $\overline{m} \in \mathbb{Z}/n\mathbb{Z}$ such that $(m, n) = 1$. This set forms a group under multiplication modulo n.

Step 5: Isomorphism

Therefore, we have:
$\mathrm{Aut}(\mathbb{Z}/n\mathbb{Z}) \cong (\mathbb{Z}/n\mathbb{Z})^\times$
where $(\mathbb{Z}/n\mathbb{Z})^\times$ is the group of all cosets $\overline{m} = m + (n)$ such that $(m, n) = 1$.

Conclusion

We have shown that $\mathrm{Aut}(\mathbb{Z}/n\mathbb{Z})$ is isomorphic to the group of cosets $\overline{m} = m + (n)$ in $\mathbb{Z}/n\mathbb{Z}$ such that $(m, n) = 1$. Thus:
$\mathrm{Aut}(\mathbb{Z}/n\mathbb{Z}) \cong (\mathbb{Z}/n\mathbb{Z})^\times$.

3

Determine $\mathrm{Aut}\, M$ for $M = (\mathbb{Z}^{(2)}, +, 0)$.

To determine $\mathrm{Aut}(M)$ for $M = (\mathbb{Z}^{(2)}, +, 0)$, where $\mathbb{Z}^{(2)}$ is the abelian group of ordered pairs of integers under addition, we need to find the group of automorphisms of M. An automorphism is a bijective homomorphism from M to itself.

Structure of $\mathbb{Z}^{(2)}$

$\mathbb{Z}^{(2)}$ is the set of all ordered pairs of integers (a, b) with component-wise addition:
$(a, b) + (c, d) = (a + c, b + d).$

Automorphisms of $\mathbb{Z}^{(2)}$

An automorphism of $\mathbb{Z}^{(2)}$ is a linear map $T : \mathbb{Z}^{(2)} \to \mathbb{Z}^{(2)}$ that is bijective and preserves the group structure. Since T is a linear map, it can be represented by a 2×2 matrix with integer entries:
$T\left(\begin{pmatrix} a \\ b \end{pmatrix}\right) = A \begin{pmatrix} a \\ b \end{pmatrix}$
where A is a 2×2 integer matrix.

To be an automorphism, T must be bijective. This means that A must be an invertible matrix with an integer inverse. The invertibility condition for a 2×2 matrix $A = \begin{pmatrix} a & b \\ c & d \end{pmatrix}$ is that the determinant $\det(A)$ is ± 1.

Determining the Automorphism Group

1. **Matrix Representation**: An automorphism T is given by a matrix A such that:
   $A = \begin{pmatrix} a & b \\ c & d \end{pmatrix}$
   with $a, b, c, d \in \mathbb{Z}$ and $\det(A) = ad - bc = \pm 1$.
2. **Group of Automorphisms**: The set of all such matrices forms the group $\mathrm{GL}_2(\mathbb{Z})$, the general linear group of 2×2 invertible matrices over the integers. Specifically, we have:
   $\mathrm{GL}_2(\mathbb{Z}) = \{A \in \mathbb{Z}^{2\times 2} \mid \det(A) = \pm 1\}.$

Conclusion

The automorphism group of $M = \mathbb{Z}^{(2)}$ is $\mathrm{GL}_2(\mathbb{Z})$:
$\mathrm{Aut}(M) = \mathrm{GL}_2(\mathbb{Z}).$

This group consists of all 2×2 integer matrices with determinant ± 1. These matrices represent the bijective linear transformations of $\mathbb{Z}^{(2)}$ that preserve the group structure.

4

Determine $\mathrm{End}(\mathbb{Q}, +, 0)$.

> To determine $\mathrm{End}(\mathbb{Q}, +, 0)$, where $\mathbb{Q}$ is considered as an abelian group under addition, we need to find all endomorphisms of this group. An endomorphism of $(\mathbb{Q}, +, 0)$ is a homomorphism from $\mathbb{Q}$ to itself that preserves the group operation.
>
> ## Key Concepts:
>
> 1. **Endomorphism**: A map $\varphi : \mathbb{Q} \to \mathbb{Q}$ is an endomorphism if it satisfies:
> $$\varphi(a + b) = \varphi(a) + \varphi(b) \quad \text{for all } a, b \in \mathbb{Q}.$$
> 2. **Linear Map**: Since $(\mathbb{Q}, +, 0)$ is a vector space over $\mathbb{Q}$ (as well as an abelian group), every endomorphism of $(\mathbb{Q}, +, 0)$ must be a linear map. Therefore, an endomorphism φ can be written as:
> $$\varphi(q) = q \cdot \varphi(1) \quad \text{for all } q \in \mathbb{Q}.$$
>
> ## Step-by-Step Solution:
>
> ### Step 1: Determine the Value of $\varphi(1)$
>
> Let $\varphi : \mathbb{Q} \to \mathbb{Q}$ be an endomorphism. Since φ is a linear map, we can determine $\varphi(q)$ for any $q \in \mathbb{Q}$ if we know $\varphi(1)$.
>
> Let $k = \varphi(1) \in \mathbb{Q}$. Then for any rational number q,
> $$\varphi(q) = \varphi\left(\frac{m}{n}\right) = \frac{m}{n} \cdot \varphi(1) = \frac{m}{n} \cdot k = kq,$$
> where $q = \frac{m}{n}$ is in its lowest terms with $m, n \in \mathbb{Z}$ and $n \neq 0$.
>
> ### Step 2: Check Properties of φ
>
> Since $\varphi(q) = kq$ defines φ completely, we need to check that it satisfies the homomorphism property:
> $$\varphi(a + b) = k(a + b) = ka + kb = \varphi(a) + \varphi(b).$$
> This holds for all $a, b \in \mathbb{Q}$.
>
> ### Step 3: All Possible Endomorphisms
>
> From the above, we see that for each $k \in \mathbb{Q}$, the map $\varphi_k : \mathbb{Q} \to \mathbb{Q}$ defined by $\varphi_k(q) = kq$ is a valid endomorphism of $(\mathbb{Q}, +, 0)$. Therefore, every endomorphism of $(\mathbb{Q}, +, 0)$ is of the form φ_k for some $k \in \mathbb{Q}$.
>
> ## Conclusion
>
> The set of all endomorphisms of the abelian group $(\mathbb{Q}, +, 0)$ is given by:
> $$\mathrm{End}(\mathbb{Q}, +, 0) = \{\varphi_k \mid k \in \mathbb{Q}\},$$
> where $\varphi_k(q) = kq$ for all $q \in \mathbb{Q}$. This set is isomorphic to the field $\mathbb{Q}$ itself, since each endomorphism corresponds uniquely to a rational number k. Thus:
> $$\mathrm{End}(\mathbb{Q}, +, 0) \cong \mathbb{Q}.$$

3.2 [165]

1

Let M be a left R-module and let η be a homomorphism of a ring S into R. Show that M becomes a left S-module if we define $ax = \eta(a)(x)$ for $a \in S, x \in M$.

> To show that M becomes a left S-module with the action defined by $ax = \eta(a)(x)$ for $a \in S$ and $x \in M$, we need to verify that this action satisfies the axioms of a left module over the ring S.
>
> ## Step-by-Step Verification:
>
> ### Given:
>
> - M is a left R-module.
> - η is a ring homomorphism from S to R.
> - Define the action of S on M by:
> $$ax = \eta(a)(x) \quad \text{for all } a \in S, x \in M.$$

Goal:

Verify that M, with the action defined above, satisfies the axioms of a left S-module:

1. $a(x+y) = ax + ay$ for all $a \in S$ and $x, y \in M$.
2. $(a+b)x = ax + bx$ for all $a, b \in S$ and $x \in M$.
3. $a(bx) = (ab)x$ for all $a, b \in S$ and $x \in M$.
4. $1_S x = x$ for all $x \in M$, where 1_S is the multiplicative identity in S.

Verification:

1. **Distributivity of the module action over addition in M:**

$$a(x+y) = \eta(a)(x+y)$$

Since $\eta(a)$ is an element of R and M is a left R-module, we have:

$$\eta(a)(x+y) = \eta(a)(x) + \eta(a)(y)$$

Thus,

$$a(x+y) = \eta(a)(x) + \eta(a)(y) = ax + ay.$$

This verifies the first axiom.

2. **Distributivity of the module action over addition in S:**

$$(a+b)x = \eta(a+b)(x).$$

Since η is a ring homomorphism, we have:

$$\eta(a+b) = \eta(a) + \eta(b).$$

Therefore,

$$(a+b)x = (\eta(a) + \eta(b))(x).$$

Using the fact that M is a left R-module, we have:

$$(\eta(a) + \eta(b))(x) = \eta(a)(x) + \eta(b)(x).$$

Thus,

$$(a+b)x = ax + bx.$$

This verifies the second axiom.

3. **Compatibility of the module action with multiplication in S:**

$$a(bx) = a(\eta(b)(x)).$$

By definition of the action,

$$a(bx) = \eta(a)(\eta(b)(x)).$$

Since η is a ring homomorphism, we have:

$$\eta(a)(\eta(b)) = \eta(ab).$$

Therefore,

$$\eta(a)(\eta(b)(x)) = \eta(ab)(x).$$

Thus,

$$a(bx) = \eta(ab)(x) = (ab)x.$$

This verifies the third axiom.

4. **Action of the multiplicative identity:**

$$1_S x = \eta(1_S)(x).$$

Since η is a ring homomorphism, it maps the multiplicative identity in S to the multiplicative identity in R:

$$\eta(1_S) = 1_R.$$

Therefore,

$$1_S x = 1_R x = x.$$

This verifies the fourth axiom.

Conclusion:

We have verified that the action defined by $ax = \eta(a)(x)$ for $a \in S$ and $x \in M$ satisfies all the axioms of a left S-module. Thus, M becomes a left S-module with this action.

2

Let M be a left R-module and let $B = \{b \in R | \forall x \in M, bx = 0\}$. Verify that B is an ideal in R. Show also that if C is any ideal contained in B then M becomes a left R/C-module by defining $(a + C)x = ax$.

To prove that $B = \{b \in R \mid \forall x \in M, bx = 0\}$ is an ideal in R, and to show that if C is any ideal contained in B, then M becomes a left R/C-module with the action $(a + C)x = ax$, we proceed as follows:

Step 1: Verify that B is an Ideal in R

Proof that B is an Ideal:

1. **Additive Closure**:
   - Let $b_1, b_2 \in B$. Then for any $x \in M$:

     $$b_1 x = 0 \quad \text{and} \quad b_2 x = 0.$$

     We need to show that $(b_1 + b_2) \in B$. Consider:

     $$(b_1 + b_2)x = b_1 x + b_2 x = 0 + 0 = 0.$$

     Therefore, $b_1 + b_2 \in B$.
2. **Absorbing Multiplication by Elements of R**:
   - Let $b \in B$ and $r \in R$. We need to show that $rb \in B$. For any $x \in M$:

     $$(rb)x = r(bx).$$

     Since $b \in B$, $bx = 0$ for all $x \in M$. Thus:

     $$r(bx) = r \cdot 0 = 0.$$

     Therefore, $(rb)x = 0$ for all $x \in M$, which means $rb \in B$.
3. **Containment of Zero**:
   - Clearly, $0 \in B$ because for any $x \in M$:

     $$0 \cdot x = 0.$$

Since B is closed under addition and multiplication by elements of R, and contains the zero element, B is an ideal in R.

Step 2: Show that M Becomes a Left R/C-Module

Let C be an ideal contained in B. We define the action of R/C on M by:

$$(a + C)x = ax \quad \text{for } a \in R \text{ and } x \in M.$$

We need to verify that this defines a valid module structure.

Well-Definedness:

To ensure that this definition is well-defined, we must check that if $a + C = a' + C$ in R/C, then $ax = a'x$ for all $x \in M$.

If $a + C = a' + C$, then $a - a' \in C$. Since $C \subseteq B$, for any $c \in C$ and $x \in M$, we have $cx = 0$. Therefore:

$$(a - a')x = 0 \implies ax - a'x = 0 \implies ax = a'x.$$

This shows that the action $(a + C)x = ax$ is well-defined.

Module Axioms:

1. **Additivity**:
   - For $(a + C), (b + C) \in R/C$ and $x \in M$:

     $$((a + C) + (b + C))x = ((a + b) + C)x = (a + b)x.$$

On the other hand:

$$(a+C)x + (b+C)x = ax + bx.$$

Since $(a+b)x = ax + bx$, the additivity axiom is satisfied.

2. **Compatibility with Scalar Multiplication**:
   - For $(a+C) \in R/C$, $r \in R$, and $x \in M$:

     $$(r(a+C))x = ((ra)+C)x = (ra)x.$$

     On the other hand:

     $$r((a+C)x) = r(ax).$$

     Since $(ra)x = r(ax)$, this axiom is satisfied.
3. **Action of Identity**:
   - For the multiplicative identity $1_R + C$ in R/C and $x \in M$:

     $$(1_R + C)x = 1_R x = x.$$

     This satisfies the identity axiom.

Conclusion:

The set $B = \{b \in R \mid \forall x \in M, bx = 0\}$ is an ideal in R. Moreover, if C is an ideal contained in B, then M becomes a left R/C-module with the action $(a+C)x = ax$. This action is well-defined and satisfies the axioms of a left module.

3

Let M be a left R-module, S a subring of R. Show that M is a left S-module if we define $bx, b \in S, x \in M$, as given in M as left R-module. (Note that this is a special case of exercise 1). In particular, the ring R can be regarded as a left S-module in this way.

To show that M is a left S-module if we define the action of S on M as the same action given in M as a left R-module, we need to verify that the module axioms for M as a left S-module are satisfied. Here, S is a subring of R, and the action of S on M is defined using the action of R on M.

Module Axioms for a Left S-Module

We need to check the following axioms for all $a, b \in S$ and $x, y \in M$:

1. $a(x+y) = ax + ay$
2. $(a+b)x = ax + bx$
3. $(ab)x = a(bx)$
4. $1_S x = x$ (where 1_S is the multiplicative identity in S)

Verification

Axiom 1: Distributivity of S-module action over addition in M

For $a \in S$ and $x, y \in M$:
$a(x+y)$
By the definition of the action (which is the same as the R-module action):
$a(x+y) = a \cdot_R (x+y)$
Since M is a left R-module, this is:
$a \cdot_R (x+y) = a \cdot_R x + a \cdot_R y$
Thus:
$a(x+y) = ax + ay$

Axiom 2: Distributivity of S-module action over addition in S

For $a, b \in S$ and $x \in M$:
$(a+b)x$
By the definition of the action (which is the same as the R-module action):
$(a+b)x = (a+b) \cdot_R x$
Since S is a subring of R, this is:
$(a+b) \cdot_R x = a \cdot_R x + b \cdot_R x$
Thus:
$(a+b)x = ax + bx$

Axiom 3: Compatibility of S-module action with multiplication in S

For $a, b \in S$ and $x \in M$:
$(ab)x$
By the definition of the action (which is the same as the R-module action):
$(ab)x = (ab) \cdot_R x$
Since S is a subring of R and M is a left R-module, we have:
$(ab) \cdot_R x = a \cdot_R (b \cdot_R x)$
Thus:
$(ab)x = a(bx)$

Axiom 4: Action of the multiplicative identity

For the multiplicative identity $1_S \in S$ and $x \in M$:
$1_S x$
By the definition of the action (which is the same as the R-module action):
$1_S x = 1_S \cdot_R x$
Since S is a subring of R and the multiplicative identity of S is also the multiplicative identity of R, we have:
$1_S \cdot_R x = 1_R \cdot_R x = x$
Thus:
$1_S x = x$

Conclusion

We have verified that the action of S on M, defined using the same action given by the R-module structure, satisfies all the axioms of a left S-module. Therefore, M is indeed a left S-module with this action.

Special Case: R as a Left S-Module

Consider R as a left R-module with the module action given by multiplication in R. We need to show that R can be regarded as a left S-module in the same way.

For $a \in S$ and $r \in R$, the action is defined by:
ar
By the definition of the action (which is multiplication in R):
$ar \in R$
Since S is a subring of R, this action satisfies the module axioms. Therefore, R itself can be regarded as a left S-module with this action.

4

Let $V = \mathbb{R}^{(n)}$ the vector space of n-tuples of real numbers with the usual addition and multiplication by elements of R. Let T be the linear transformation of V defined by

$$\boldsymbol{x = (x_1, x_2, \ldots, x_n) \to Tx = (x_n, x_1, x_2, \ldots, x_{n-1})}$$

Consider V as left $\mathbb{R}[\lambda]$-module as in the text, and determine: (a) λx, (b)$(\lambda^2 + 2)x$, (c)$(\lambda^{n-1} + \lambda^{n-2} + \ldots + 1)x$. What elements satisfy $(\lambda^2 - 1)x = 0$?

Given $V = \mathbb{R}^{(n)}$, the vector space of n-tuples of real numbers with the usual addition and multiplication by elements of $\mathbb{R}$, and a linear transformation $T : V \to V$ defined by:

$$x = (x_1, x_2, \ldots, x_n) \to Tx = (x_n, x_1, x_2, \ldots, x_{n-1}),$$

we consider V as a left $\mathbb{R}[\lambda]$-module where λ acts as the linear transformation T.

Part (a): λx

To determine λx for $x = (x_1, x_2, \ldots, x_n)$:

$$\lambda x = T(x) = (x_n, x_1, x_2, \ldots, x_{n-1}).$$

Part (b): $(\lambda^2 + 2)x$

To determine $(\lambda^2 + 2)x$, we first need to compute $\lambda^2 x$.

$$\lambda^2 x = T(T(x)) = T((x_n, x_1, x_2, \ldots, x_{n-1})) = (x_{n-1}, x_n, x_1, x_2, \ldots, x_{n-2}).$$

Now, $(\lambda^2 + 2)x$ is given by:

$$(\lambda^2 + 2)x = \lambda^2 x + 2x = (x_{n-1}, x_n, x_1, x_2, \ldots, x_{n-2}) + 2(x_1, x_2, \ldots, x_n) = (x_{n-1} + 2x_1, x_n + 2x_2, x_1 + 2x_3, \ldots, x_{n-2} + 2x_n).$$

Part (c): $(\lambda^{n-1} + \lambda^{n-2} + \cdots + 1)x$

To determine $(\lambda^{n-1} + \lambda^{n-2} + \cdots + 1)x$, we first compute $\lambda^k x$ for $k = 0, 1, 2, \dots, n-1$.

$$\begin{aligned}
\lambda^0 x &= x = (x_1, x_2, \dots, x_n), \\
\lambda^1 x &= \lambda x = (x_n, x_1, x_2, \dots, x_{n-1}), \\
\lambda^2 x &= (x_{n-1}, x_n, x_1, x_2, \dots, x_{n-2}), \\
&\vdots \\
\lambda^{n-1} x &= (x_2, x_3, \dots, x_n, x_1).
\end{aligned}$$

Then,

$$(\lambda^{n-1} + \lambda^{n-2} + \cdots + 1)x = \lambda^{n-1}x + \lambda^{n-2}x + \cdots + \lambda^0 x = (x_2, x_3, \dots, x_n, x_1) + (x_3, x_4, \dots, x_1, x_2) + \cdots + (x_1, x_2, \dots, x_n).$$

The result is the sum of all cyclic permutations of the components of x.

Elements that Satisfy $(\lambda^2 - 1)x = 0$

To determine which elements satisfy $(\lambda^2 - 1)x = 0$, we solve:

$$(\lambda^2 - 1)x = \lambda^2 x - x = 0.$$

This means:

$$\lambda^2 x = x.$$

Recall that $\lambda^2 x = (x_{n-1}, x_n, x_1, x_2, \dots, x_{n-2})$. Therefore, we require:

$$(x_{n-1}, x_n, x_1, x_2, \dots, x_{n-2}) = (x_1, x_2, \dots, x_n).$$

This implies:

$$\begin{aligned}
x_{n-1} &= x_1, \\
x_n &= x_2, \\
x_1 &= x_3, \\
x_2 &= x_4, \\
&\vdots \\
x_{n-2} &= x_n.
\end{aligned}$$

From these equations, we see that x must satisfy:

$$x_1 = x_3 = x_5 = \cdots, \quad x_2 = x_4 = x_6 = \cdots.$$

If n is even, all the x_i will be equal in alternating positions. If n is odd, the same two sets of alternating positions hold, but the periodicity implies all elements must be equal. Therefore, in general, x is of the form:

$$x = (a, b, a, b, \dots, a, b) \quad \text{if } n \text{ is even},$$

or

$$x = (a, a, \dots, a) \quad \text{if } n \text{ is odd}.$$

Hence, the elements of V that satisfy $(\lambda^2 - 1)x = 0$ are those that are either repeated pairs (a, b) if n is even or the same value a repeated if n is odd.

3.3 [169]

4

Prove that for any R and R-module M, $\mathrm{Hom}(R, M) \cong (M, +, 0)$.

To prove that for any ring R and any R-module M, $\mathrm{Hom}(R, M) \cong (M, +, 0)$, we will construct an explicit isomorphism between the set of R-module homomorphisms from R to M and the underlying abelian group of M.

Definitions and Setup

- R is a ring.
- M is a left R-module.
- $\mathrm{Hom}(R, M)$ denotes the set of R-module homomorphisms from R to M.

Construction of the Isomorphism

1. **Define a Mapping**:
   Define a map $\Phi : \mathrm{Hom}(R, M) \to M$ by $\Phi(f) = f(1)$ for $f \in \mathrm{Hom}(R, M)$.
2. **Check Well-Definedness**:
   For any R-module homomorphism $f : R \to M$, consider $\Phi(f) = f(1)$. Since f is an R-module homomorphism, it satisfies $f(r \cdot 1) = r \cdot f(1)$ for all $r \in R$. Thus, $\Phi(f) \in M$.
3. **Define the Inverse Mapping**:
   Define a map $\Psi : M \to \mathrm{Hom}(R, M)$ by $\Psi(m)(r) = r \cdot m$ for $m \in M$ and $r \in R$.
4. **Check Well-Definedness**:
   For any $m \in M$, $\Psi(m) : R \to M$ is given by $\Psi(m)(r) = r \cdot m$. We need to check that $\Psi(m)$ is an R-module homomorphism:

$$\Psi(m)(r + s) = (r + s) \cdot m = r \cdot m + s \cdot m = \Psi(m)(r) + \Psi(m)(s),$$

$$\Psi(m)(rs) = (rs) \cdot m = r \cdot (s \cdot m) = r \cdot \Psi(m)(s) = r\Psi(m)(s).$$

   Therefore, $\Psi(m) \in \mathrm{Hom}(R, M)$.
5. **Check that Φ and Ψ are Inverses**:
   - For $f \in \mathrm{Hom}(R, M)$:

$$\Psi(\Phi(f))(r) = \Psi(f(1))(r) = r \cdot f(1).$$

     Since f is an R-module homomorphism, we have:

$$f(r) = f(r \cdot 1) = r \cdot f(1).$$

     Thus,

$$\Psi(\Phi(f))(r) = f(r).$$

     This shows that $\Psi \circ \Phi = \mathrm{id}_{\mathrm{Hom}(R,M)}$.
   - For $m \in M$:

$$\Phi(\Psi(m)) = \Phi(\Psi(m))(1) = \Psi(m)(1) = 1 \cdot m = m.$$

     This shows that $\Phi \circ \Psi = \mathrm{id}_M$.

Since Φ and Ψ are inverses of each other, they establish a bijection between $\mathrm{Hom}(R, M)$ and M.

Conclusion

The map $\Phi : \mathrm{Hom}(R, M) \to M$ defined by $\Phi(f) = f(1)$ is an isomorphism of abelian groups with the inverse given by $\Psi : M \to \mathrm{Hom}(R, M)$ defined by $\Psi(m)(r) = r \cdot m$. Thus, we have shown that:

$$\mathrm{Hom}(R, M) \cong (M, +, 0).$$

This completes the proof.

5

Show that $\mathrm{End}_R\, M$ is the centralizer in $\mathrm{End}\, M$ of the set of group endomorphisms $a_L, a \in R$.

To show that $\mathrm{End}_R\, M$ is the centralizer in $\mathrm{End}\, M$ of the set of group endomorphisms a_L for $a \in R$, we need to understand the structure of $\mathrm{End}_R\, M$, the set of R-module endomorphisms of M, and relate it to the centralizer concept in the context of group endomorphisms.

Definitions

1. $\mathrm{End}_R\, M$: The set of R-module endomorphisms of M, i.e., the set of homomorphisms $\varphi : M \to M$ that respect the R-module structure:

$$\varphi(rm) = r\varphi(m) \quad \text{for all } r \in R, m \in M.$$

2. $\mathrm{End}\, M$: The set of all group endomorphisms of the abelian group $(M, +)$, i.e., the set of homomorphisms $\psi : M \to M$ that respect the group structure:

$$\psi(m_1 + m_2) = \psi(m_1) + \psi(m_2) \quad \text{for all } m_1, m_2 \in M.$$

3. a_L: For each $a \in R$, a_L is the group endomorphism of M given by left multiplication by a:

$$a_L(m) = am \quad \text{for all } m \in M.$$

4. **Centralizer in $\text{End } M$**: The centralizer of a subset S in a ring A is the set of elements in A that commute with every element of S. In this case, the centralizer in $\text{End } M$ of the set $\{a_L \mid a \in R\}$ is the set of endomorphisms $\psi \in \text{End } M$ such that:

$$\psi \circ a_L = a_L \circ \psi \quad \text{for all } a \in R.$$

Proof

To show that $\text{End}_R M$ is the centralizer in $\text{End } M$ of the set $\{a_L \mid a \in R\}$, we need to show that $\varphi \in \text{End}_R M$ if and only if $\varphi \in \text{End } M$ and φ commutes with every a_L for $a \in R$.

(⇒) If $\varphi \in \text{End}_R M$:

1. φ **respects the R-module structure**:

$$\varphi(rm) = r\varphi(m) \quad \text{for all } r \in R, m \in M.$$

2. φ **commutes with a_L for all $a \in R$**:

$$\varphi \circ a_L(m) = \varphi(am) = a\varphi(m) = a_L(\varphi(m)) = a_L \circ \varphi(m).$$

   Thus,

$$\varphi \circ a_L = a_L \circ \varphi \quad \text{for all } a \in R.$$

So, if $\varphi \in \text{End}_R M$, then φ commutes with every a_L for $a \in R$.

(⇐) If $\varphi \in \text{End } M$ commutes with every a_L:

1. φ **commutes with a_L**:

$$\varphi \circ a_L = a_L \circ \varphi \quad \text{for all } a \in R.$$

2. **Evaluate on an element $m \in M$**:

$$\varphi(am) = \varphi(a_L(m)) = a_L(\varphi(m)) = a\varphi(m).$$

   This shows that φ respects the R-module structure:

$$\varphi(am) = a\varphi(m) \quad \text{for all } a \in R, m \in M.$$

Thus, $\varphi \in \text{End}_R M$.

Conclusion

We have shown that $\varphi \in \text{End}_R M$ if and only if $\varphi \in \text{End } M$ and φ commutes with every a_L for $a \in R$. Therefore, $\text{End}_R M$ is the centralizer in $\text{End } M$ of the set of group endomorphisms $\{a_L \mid a \in R\}$:

$$\text{End}_R M = \{\varphi \in \text{End } M \mid \varphi \circ a_L = a_L \circ \varphi \text{ for all } a \in R\}.$$

6

Does $a_L \in \text{End}_R M$?

To determine whether $a_L \in \text{End}_R M$, we need to check if a_L is an R-module endomorphism. Recall that for $a \in R$, the map $a_L : M \to M$ is defined by:
$a_L(m) = am \quad \text{for all } m \in M.$

An R-module endomorphism is a map $\varphi : M \to M$ that satisfies the following condition for all $r \in R$ and $m \in M$:
$\varphi(rm) = r\varphi(m).$

Let's check if a_L satisfies this condition.

Check $a_L \in \text{End}_R M$:

For $a \in R$, a_L is defined by $a_L(m) = am$. We need to verify if a_L respects the R-module structure:
$a_L(rm) = ra_L(m) \quad \text{for all } r \in R \text{ and } m \in M.$

Compute both sides of the equation:

1. **Left-hand side:**
   $a_L(rm) = a(rm)$
2. **Right-hand side:**
   $ra_L(m) = r(am)$

Since M is an R-module, the right-hand side follows the associativity of the R-module action:
$a(rm) = (ar)m = r(am) = ra_L(m)$

Thus:
$a_L(rm) = ra_L(m)$

This shows that a_L respects the R-module structure.

Conclusion

Since a_L satisfies the condition $\varphi(rm) = r\varphi(m)$ for an R-module endomorphism, we have:
$a_L \in \mathrm{End}_R M$.

Therefore, for any $a \in R$, the map a_L, defined by $a_L(m) = am$ for all $m \in M$, is indeed an element of $\mathrm{End}_R M$.

7

A module M is called irreducible if $M \neq 0$ and 0 and M are the only submodules of M. Show that M is irreducible if and only if $M \neq 0$ and M is cyclic with every non-zero element as generator.

To prove that a module M is irreducible if and only if $M \neq 0$ and M is cyclic with every non-zero element as a generator, we will proceed in two directions:

1. Show that if M is irreducible, then $M \neq 0$ and M is cyclic with every non-zero element as a generator.
2. Show that if $M \neq 0$ and M is cyclic with every non-zero element as a generator, then M is irreducible.

1. Irreducibility implies cyclic with every non-zero element as a generator

Assume M is an irreducible module.

- **Non-zero condition**: By definition, $M \neq 0$.
- **Cyclic condition**: We need to show that M is cyclic and every non-zero element is a generator.

Let $m \in M$ be a non-zero element. Consider the submodule generated by m, denoted by Rm. Since M is irreducible, the only submodules of M are 0 and M. Therefore, Rm must be either 0 or M. Because $m \neq 0$, $Rm \neq 0$. Hence, $Rm = M$.

This shows that every non-zero element $m \in M$ generates M, making M cyclic with m as a generator.

2. Cyclic with every non-zero element as a generator implies irreducibility

Assume $M \neq 0$ and M is cyclic with every non-zero element as a generator.

- **Non-zero condition**: Given.
- **Irreducibility**: We need to show that the only submodules of M are 0 and M.

Let N be a non-zero submodule of M. Since $N \neq 0$, there exists a non-zero element $n \in N$. By assumption, n is a generator of M. Therefore, $Rn = M$.

Since $n \in N$ and N is a submodule, $Rn \subseteq N$. Thus, $M \subseteq N$ because $Rn = M$. Therefore, $N = M$.

This shows that the only submodules of M are 0 and M, making M irreducible.

Conclusion

Combining the two directions, we have shown that M is irreducible if and only if $M \neq 0$ and M is cyclic with every non-zero element as a generator.