Algebra II

January 8, 2024

How To Prove a Big Theorem

1. Reduce to a linear algebra problem.
2. Solve the linear algebra problem.

Grades

- Weekly Homework
  - For completion, graded by peers or presented. Survey to follow.
- Midterm
- Final
  - March 18, 2024
  - 4:00 PM to 7:00 PM

Office Hours

McHenry 4174
Monday / Wednesday from 1:05 PM to 2:05 PM.
E-mail ahead if arriving promptly at 1:05 PM.

Definition: Module

Let R be a ring.
A (left) R-module is a set M with binary operations $\cdot : R \times M \to M$ and $+ : M \times M \to M$ such that

1. $(M, +)$ is an Abelian group.
   (a) $\exists 0 \in M$ such that $\forall m \in M$, $m + 0 = m = 0 + m$.
   (b) $\forall m \in M$, $\exists n \in M$ such that $m + n = 0 = n + m$.
   (c) $\forall m_1, m_2, m_3 \in M$, $(m_1 + m_2) + m_3 = m_1 + (m_2 + m_3)$.
   (d) $\forall m_1, m_2 \in M$, $m_1 + m_2 = m_2 + m_1$.
2. Distibution.

$$\begin{aligned} (r_1 + r_2) \cdot m &= r_1 \cdot m + r_2 \cdot m \\ r \cdot (m_1 + m_2) &= r \cdot m_1 + r \cdot m_2 \end{aligned}$$

3. $1 \cdot m = m$ where $1 \in R$ is the multiplicative identity.

4. $(r_1 \cdot r_2) \cdot m = r_1 \cdot (r_2 \cdot m)$

   - Note that $\cdot$ may represent scalar multiplication or multiplication in the ring.

Example 1

$n \in \mathbb{Z}$, $n = 1, 2, 3, \ldots$, $R = \mathbb{R}$, $M = \mathbb{R}^n$, equipped with $+$ vector addition and $\cdot$ scalar multiplication.

Example 2

Let R be your favorite field $\mathbb{Z}/p$, $\mathbb{Q}$, $\mathbb{C}$, $\mathbb{F}_q$, $\mathbb{Q}_p$, and $M = \mathbb{R}^n$.
Similarly with rings $R = \mathbb{Z}$, $R = \mathbb{Z}[x]$, etc.

Example 3

Let $R = \mathbb{Z}$ and M be your favorite Abelian group.

Example 4

Let R be any ring (e.g. $\mathbb{Z}[x]$) and M be any left ideal (e.g. $R \cdot x + R \cdot 3$).

Example 5

Fix $\begin{pmatrix} a & b \\ c & d \end{pmatrix} \in M_{2\times 2}(\mathbb{R})$.
Let $R = \mathbb{R}[x]$, the polynomial ring, and $M = \mathbb{R}^2$ where $+$ is standard addition, and $\cdot$ is matrix multiplication.

$$x \cdot m = \begin{pmatrix} a & b \\ c & d \end{pmatrix} \cdot m$$

Example 6

Let R be any ring and M be functions $R \to R$ where $+$ and $\cdot$ are pointwise operations.

Example 6'

Let $R = \mathbb{R}$ and have M require that f is continuous, differntiable, etc.

January 10, 2024

Course website online.
Homework due Wednesday.
Today: Chapter 10 in Dummit and Foote.

Basic Definitions and Examples

Let R be a ring (usually abelian and with identity) and M be a left R-module.

Definition: Submodule

A subset $N \subseteq M$ is a R-submodule if and only if

1. it is an additive subgroup of M and
2. if $r \in R$ and $x \in N$, then $rx \in N$.

Proposition:

$N \subseteq M$ is a submodule if and only if

1. $N \neq \varnothing$ and
2. if $r \in R$ and $x, y \in N$, then $rx + y \in N$.

Example 1

If $R = \mathbb{Z}$, this is just the definition of a subgroup.

Example 2

If $R = \mathbb{R}$, this is just the definition of a real vector space.

Example 3

$\{0\}$ and M are both submodules of M.

Example 4

Let $R = \mathbb{R}[t]$, $M = R$, $N = (t-1) \cdot R$.

Example 5

Let $R = \mathbb{Z}/4$, $M = R$, $N = \{0 + \mathbb{Z}/4, 2 + \mathbb{Z}/4\}$.

Definition: R-Algebra

Let R be an abelian ring with identity and A be a ring with identitity.
An R-algebra is a ring homomorphism $f : R \to A$ such that

1. $f(1) = 1$ and
2. $f(R) \subseteq Z(A)$, the center of A.

Example 1

If A is a ring wtih identity, then $f : \mathbb{Z} \to A$ such that $f(n) = \underbrace{1 + \cdots + 1}_{n \text{ times}}$ makes A into an algebra.

Example 2

If L/K is a field extension, then the inclusion $K \hookrightarrow L$ is a K-algebra.

Example 3

$\mathbb{Z} \hookrightarrow \mathbb{Q}$ is a $\mathbb{Z}$-algebra.

Example 4

$f_0 : \mathbb{R}[t] \to \mathbb{R}$, $f_0(p) = p(0)$.
Can replace f_0 with $f_1(p) = p(1)$ or any other choice.

Example 5

$\mathbb{H}$ are expresions of the form $a + b\vec{i} + c\vec{j} + d\vec{k}$ with $a, b, c, d \in \mathbb{R}$ and $i^2 = j^2 = k^2 = -1$.
$f : \mathbb{R} \to \mathbb{H}$, $f(a) = a$ is an $\mathbb{R}$-algebra.
What about $g : \mathbb{C} \to \mathbb{H}$ with $g(a + bi) = a + bi$?
No, since $g(\mathbb{C}) \notin Z(\mathbb{H})$.

Quotient Modules and Module Homomorphisms

Definition: Module Homomorphism

Let R be a ring with identitity and M_1, M_2 be left R-modules.
An R-module homomorphism $\phi : M_1 \to M_2$ is a function that preserves $+$ and $\cdot$.

Example 1

$R = \mathbb{Z}$ and ϕ is any homomorphism of abelian groups.

Example 2

$R = \mathbb{R}$ and ϕ is the collection of linear transformations.

Example 3

$\mathrm{Id}_M : M \to M$ and $0 : M \to N$, the identitity and zero homomorphisms, are R-module homomorphisms.

Example 4

Let $M = \underbrace{R \times \cdot \times R}_{n\text{-times}}$, $N = R$ and $\pi_i : M \to N$ such that $\pi_i(r_i, \dots, r_n) = r_i$.
Consider $\pi_i : R \times R \to R$ with $\pi_1(a_1, a_2) = a_1$.
Then $\ker(\pi_1) = \{(0, a_2) \mid a_2 \in R\}$ and $\mathrm{im}(\pi_1) = R$.

Example 5

Let M be column vectors $\begin{bmatrix} x \\ y \end{bmatrix}$ with $x, y \in \mathbb{R}$ and $R = \mathbb{R}$.
Fix $\begin{bmatrix} a & b \\ c & d \end{bmatrix}$, then define $\phi : M \to N$ as $\phi\left(\begin{bmatrix} x \\ y \end{bmatrix}\right) = \begin{bmatrix} a & b \\ c & d \end{bmatrix}\begin{bmatrix} x \\ y \end{bmatrix}$.

Definition: Module Isomorphism

An R-module isomorphism is an R-module homomorphism $\phi : M_1 \to M_2$ such that the inverse function exists and is an R-module homomorphism.

Definition: Kernel

The kernel is $\ker(\phi) = \{x \in M \mid \phi(x) = 0\}$.

Definition: Image

The image is $\mathrm{im}(\phi) = \{\phi(x) \mid x \in M\}$.

Definition: Homomorphism R-Module

$\mathrm{Hom}_R(M_1, M_2)$ is the set of all R-module homomorphisms $M_1 \to M_2$.
Equipped with pointwise addition and scalar multiplication, it forms an R-module.

Proposition:

$\phi : M \to N$ is an R-module homomorphism if and only if

$$\phi(rx + y) = r\phi(x) + \phi(y)$$

for all $x, y \in M$ and $r \in R$.

Proposition:

Pointwise addition and scalar multiplication $\mathrm{Hom}_R(M, N)$ into an R-module.

Proposition:

Composition of R-module homomorphisms is an R module homomorphism.
$M_1 \xrightarrow{\phi_1} M_2 \xrightarrow{\phi_2} M_3 \rightsquigarrow \phi_2 \circ \phi_1$.

Proposition:

$\mathrm{Hom}_R(M, M)$ is a ring under composition and an R-algebra under $f : R \to \mathrm{Hom}_R(M, M)$ with $f(r) = \phi_r$ and $\phi_r(x) = rx$.

Construction of Quotient R-Modules

Let R be a ring with identity, M be an R-module and N submodule.
We want a new module, M/N, and an R-module homomorphism $\phi : M \to M/N$ such that $\ker(\phi) = N$ and $\mathrm{im}(\phi) = M/N$.
Define an equivalence relation $\sim$ on M by $x \sim y$ if and only if $x - y \in N$.
So $x \sim 0 \iff x \in N$.
Define M/N as the set of equivalence classes for $\sim$, and write $x + N$ the equivalence class of x.
Define $(x + N) \oplus (y + N) = (x + y) + N$ and $r \odot (x + N) = (rx) + N$.