

# 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  $\cdot : R \times M \rightarrow M$  and  $+$  :  $M \times M \rightarrow M$  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. Distribution.

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

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

$n \in \mathbb{Z}$ ,  $n = 1, 2, 3, \dots$ ,  $R = \mathbb{R}$ ,  $M = \mathbb{R}^n$ , 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  $R \rightarrow R$  where  $+$  and  $\cdot$  are pointwise operations.

#### Example 6'

Let  $R = \mathbb{R}$  and have  $M$  require that  $f$  is continuous, differentiable, 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.  $N \neq \emptyset$  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 identity.  
An  $R$ -algebra is a ring homomorphism  $f : R \rightarrow A$  such that

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

Example 1

If  $A$  is a ring with identity, then  $f : \mathbb{Z} \rightarrow A$  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

$f_0 : \mathbb{R}[t] \rightarrow \mathbb{R}, f_0(p) = p(0).$

Can replace  $f_0$  with  $f_1(p) = p(1)$  or any other choice.

#### Example 5

$\mathbb{H}$  are expressions of the form  $a + b\vec{i} + c\vec{j} + d\vec{k}$  with  $a, b, c, d \in \mathbb{R}$  and  $i^2 = j^2 = k^2 = -1$ .

$f : \mathbb{R} \rightarrow \mathbb{H}, f(a) = a$  is an  $\mathbb{R}$ -algebra.

What about  $g : \mathbb{C} \rightarrow \mathbb{H}$  with  $g(a + bi) = a + bi$ ?

No, since  $g(\mathbb{C}) \not\subseteq Z(\mathbb{H})$ .

### Quotient Modules and Module Homomorphisms

#### Definition: Module Homomorphism

Let  $R$  be a ring with identity and  $M_1, M_2$  be left  $R$ -modules.

An  $R$ -module homomorphism  $\phi : M_1 \rightarrow M_2$  is a function that preserves  $+$  and  $\cdot$ .

#### Example 1

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

#### Example 2

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

#### Example 3

$\text{Id}_M : M \rightarrow M$  and  $0 : M \rightarrow N$ , the identity and zero homomorphisms, are  $R$ -module homomorphisms.

#### Example 4

Let  $M = \underbrace{R \times \cdots \times R}_{n\text{-times}}, N = R$  and  $\pi_i : M \rightarrow N$  such that  $\pi_i(r_1, \dots, r_n) = r_i$ .

Consider  $\pi_1 : R \times R \rightarrow R$  with  $\pi_1(a_1, a_2) = a_1$ .

Then  $\ker(\pi_1) = \{(0, a_2) \mid a_2 \in R\}$  and  $\text{im}(\pi_1) = R$ .

#### 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  $\phi : M \rightarrow N$  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  $\phi : M_1 \rightarrow M_2$  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  $\text{im}(\phi) = \{\phi(x) \mid x \in M\}$ .

Definition: Homomorphism  $R$ -Module

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

Proposition:

$\phi : M \rightarrow N$  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  $\text{Hom}_R(M, N)$  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:

$\text{Hom}_R(M, M)$  is a ring under composition and an  $R$ -algebra under  $f : R \rightarrow \text{Hom}_R(M, M)$  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  $\phi : M \rightarrow M/N$  such that  $\ker(\phi) = N$  and  $\text{im}(\phi) = M/N$ .

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  $r \odot (x + N) = (rx) + N$ .

January 17, 2024

Definition: Quotient  $R$ -Modules

Let  $R$  be a ring with identity,  $M$  an  $R$ -module, and  $N \subseteq M$  a submodule.

The quotient module  $M/N$  is defined by taking the quotient additive group  $M/N$  and defining scalar multiplication by  $r \cdot (x + N) = rx + N$ .

Definition: Sum of Modules

For  $N_1, N_2 \subseteq M$  submodules,  $N_1 + N_2$  is the smallest submodule of  $M$  containing  $N_1$  and  $N_2$  (i.e. the module generated by  $N_1$  and  $N_2$ ).

Isomorphism Theorems

Let  $M$  be a module and  $A, B, N \subseteq M$  be submodules.

### First Isomorphism Theorem

Let also  $A \subseteq B$ , then

$$(M/A) \Big/ (B/A) \simeq M/B$$

- Proof

Define  $\phi : M/A \rightarrow M/B$  as  $\phi(x + A) = x + B$ .

Then, define  $\bar{\phi} : (M/A) \Big/ (B/A) \rightarrow M/B$  as  $\bar{\phi}(y + B/A) = \phi(y)$ .

The inverse  $\psi : M/B \rightarrow (M/A) \Big/ (B/A)$  is defined by  $\psi(x + B) = (x + A) + B/A$ .

### Second Isomorphism Theorem

$$(A + B)/B \simeq A/(A \cap B)$$

- Proof

Define  $\phi : A/(A \cap B) \rightarrow (A + B)/B$  by  $\phi(x + A \cap B) = x + B$ .

Define  $\psi : (A + B)/B \rightarrow A/(A \cap B)$  by  $\psi(x + y + B) = x + A \cap B$ .

Say  $x + y = x' + y' + b$  for  $b \in B$ . Then

$$\underbrace{x - x'}_{\in A} = \underbrace{y - y' - b}_{\in B}$$

and

$$x' + A \cap B = x' + (x - x') + A \cap B = x + A \cap B$$

### Third Isomorphism Theorem

If  $\phi : M \rightarrow N$  is an  $R$ -module homomorphism, then  $M/\ker(\phi) \simeq \text{im}(\phi)$ .

- Proof

Define  $\bar{\phi} : M/\ker(\phi) \rightarrow \text{im}(\phi)$  by  $\bar{\phi}(x + \ker(\phi)) = \phi(x)$ .

This is surjective by construction.

For injectivity, if  $0 = \bar{\phi}(x + \ker(\phi)) = \phi(x)$ , then  $x \in \ker(\phi)$ .

### Fourth Isomorphism Theorem

If  $N \subseteq M$  is an  $R$ -submodule, then the map  $A \supseteq N \mapsto A/N$

$$\{R\text{-submodules of } M \text{ containing } N\} \simeq \{R\text{-submodules of } M/N\}$$

is a bijection which preserves sum and intersection.

- Compare

$$\{\text{submodules of } M \text{ contained in } N\} = \{\text{submodules of } N\}$$

IMAGE HERE

## Generators, Direct Sums and Free Modules

### Definition: Finitely Generated Submodule

If  $N_1, \dots, N_k \subseteq M$  is a finite collection of submodules, then  $M_1 + \dots + M_k$  is the smallest submodule containing  $M_1, \dots, M_k$ .

Typically elements are  $x_1 + \dots + x_k$  with  $x_i \in N_i$ .

If  $\{x_1, \dots, x_k\} = S \subseteq M$  is a finite set, the submodule generated by  $S$  is

$$Rx_1 + \dots + Rx_k$$

### Definition: Finitely Generated Module

A module  $M$  is finitely generated if it is the submodule generated by some finite set  $S \subseteq M$ .

#### Example 1

$R = M$  for any ring  $R$  (also cyclic; take  $S = \{1\}$ )

#### Example 2

Any finite dimensional vector space.

#### Example 3

$\mathbb{R}^n$  for  $n = 1, 2, 3, \dots$

#### Example 4

$\mathbb{Z}[i] = M$  over  $\mathbb{Z} = R$ . Then  $S = \{1, i\}$ .

#### Counter-example 1

Let  $M = C(\mathbb{R})$  be continuous functions  $\mathbb{R} \rightarrow \mathbb{R}$ , and  $R = \mathbb{R}$ .

#### Counter-example 2

Any infinite dimensional vector space.

### Definition: Cyclic Module

A module  $M$  is cyclic if it the submodule generated by some one element set  $S$ .

### Theorem: Chinese Remainder Theorem

When can we find a unique integer  $x$  satisfying

$$\begin{aligned}x &\equiv a \pmod{m} \\x &\equiv b \pmod{n}\end{aligned}$$

January 22, 2024

### Definition: External Direct Product

The external direct product  $M_1 \times \dots \times M_k$  of a collection of  $R$ -modules is the Cartesian product with  $\cdot$  and  $+$  defined componentwise.

### Proposition

Let  $M_1, \dots, M_k \subseteq M$  be submodules. Then the following are equivalent:

1. The map  $M_1 \times \dots \times M_k \rightarrow M_1 + \dots + M_k$  defined as  $(x_1, \dots, x_k) \mapsto x_1 + \dots + x_k$  is an isomorphism.
2.  $M_{i_0} \cap \sum_{j \neq i} M_j = \{0\}$ .
3. Every element of  $M_1 + \dots + M_k$  can be uniquely written as  $x_1 + \dots + x_k$  with  $x_i \in M_i$ .

#### Proof 1 Implies 2

Say that for some  $i_0$  we have  $x_0 \in M_{i_0} \cap \left(\sum_{i \neq j} M_j\right)$ .

Write  $x_0 = \sum_{j \neq i_0} x_j$  with  $x_j \in M_j$ .

Consider  $(x_1, x_2, \dots, x_{i_0-1}, -x_{i_0}, x_{i_0+1}, \dots, x_k)$ , maps to  $\sum x_j - x_0 = 0$ , so  $x_j = x_i = 0$  in  $M$ .

#### Proof 2 Implies 3

Say  $x_1 + \dots + x_k = x'_1 + \dots + x'_k$  with  $x_i, x'_i \in M_i$ . Rearrange

$$x_1 - x'_1 = \overbrace{(x'_2 - x_2) + \dots + (x'_k - x_k)}^{\in \sum_{j \neq i} M_j}$$

So  $x_1 - x'_1 = 0$  and the first component is equal. Repeating the argument on all indices completes the proof.

#### Proof 3 Implies 1

#### Definition: Internal Direct Product

If the equivalent conditions hold, we say  $M_1 + \dots + M_k$  is the internal direct product of  $M_1, \dots, M_k$ .

Notation:  $M_1 \times \dots \times M_k$  or  $M_1 \oplus \dots \oplus M_k$ .

#### Chinese Remainder Theorem

For  $a, b, m, n \in \mathbb{Z}$ , if  $\gcd(n, m) = 1$ , then there exists a solution  $x \in \mathbb{Z}$  to

$$\begin{aligned} x &\equiv a \pmod{m} \\ x &\equiv b \pmod{n} \end{aligned}$$

which is unique  $\pmod{mn}$ .

Consider  $\mathbb{Z}/nm \rightarrow \mathbb{Z}/m \times \mathbb{Z}/n$  defined by  $x \pmod{nm} \mapsto (x \pmod{m}, x \pmod{n})$ .

Thus, the Chinese Remainder Theorem implies that the map is an isomorphism.

Can we realize  $\mathbb{Z}/mn$  as the internal direct product of a submodule of size  $n$  and a submodule of size  $m$ ?

#### Definition: Basis of a Module

Suppose that  $X \subseteq M$  is a subset of an  $R$ -module  $M$ . We say that  $X$  is a basis for  $M$  if and only if

1.  $X$  is a generating set of  $M$ .



2. The elements of  $X$  are linearly independent in the sense that for all but finitely many  $r(x) = 0$ ,

$$\sum_{x \in X} r(x)x = 0 \implies r(x) = 0, \forall x$$

Definition: Free Module

We say  $M$  is free if there exists a basis.

Example

$R$  any ring and  $M = \mathbb{R}^3$ .

Non-example

$R = \mathbb{Z}$  and  $M = \mathbb{Z}/3$ .

$M$  does not admit a basis.

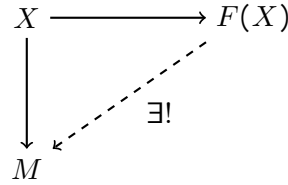
Example?

$R$  any ring and  $M = \{0\}$  admits the basis  $X = \emptyset$ .

Definition: Universal Mapping Property of Free Modules

Let  $X$  be a set.

We say that an  $R$ -module  $F(X)$  and a set map  $\phi_{\text{can}} : X \rightarrow F(X)$  satisfies the universal property of the free  $R$ -module on  $X$  if for all set maps  $X \rightarrow M$  into an  $R$ -module  $M$ , there exists a unique  $R$ -homomorphism.



Existence

When  $X = \{1, 2, \dots, n\}$ , define  $F(R) = R^n$  and  $\phi_{\text{can}} : X \rightarrow R^n$  as

$$\begin{aligned} \phi_{\text{can}}(1) &= (1, 0, \dots, 0) \\ \phi_{\text{can}}(2) &= (0, 1, \dots, 0) \\ &\vdots \\ \phi_{\text{can}}(n) &= (0, 0, \dots, 1) \end{aligned}$$

Why does this satisfy the universal mapping property?

Let  $\phi : X \rightarrow M$  be given. We want  $\tilde{\phi} : F(X) \rightarrow M$  such that

$$\begin{aligned} \phi &= \tilde{\phi} \circ \phi_{\text{can}} \\ r_1 \phi(1) &= \tilde{\phi}(r_1, 0, \dots, 0) \\ r_2 \phi(2) &= \tilde{\phi}(0, r_2, \dots, 0) \\ &\vdots \\ r_n \phi(n) &= \tilde{\phi}(0, 0, \dots, r_n) \end{aligned}$$

So define  $\tilde{\phi}(r_1, \dots, r_n) = r_1\phi(1) + \dots + r_n\phi(n)$

Uniqueness

If  $\phi_{\text{can}} : X \rightarrow F(X)$  and  $\phi'_{\text{can}} : X \rightarrow F'(X)$  satisfy the universal mapping property, then there exists a unique isomorphism  $F(X) \xrightarrow{\sim} F'(X)$  such that

$$\begin{array}{ccc} & X & \\ \phi_{\text{can}} \swarrow & & \searrow \phi'_{\text{can}} \\ F(X) & \xrightarrow{\sim} & F'(X) \end{array}$$

Definition: Tensor Product

Given two modules,  $M$  and  $N$ , we want a new module  $M \otimes N$  that plays the roll of multiplication. Compare with  $\oplus$  and addition.

January 24, 2024

Recall: Free Module

Given a set  $X$ , a set map  $\phi_{\text{can}} : X \rightarrow F(X)$  into an  $R$ -module  $F(X)$  is a free module on  $X$  if we can always fill in the following dotted arrow uniquely:

$$\begin{array}{ccc} X & \xrightarrow{\phi_{\text{can}}} & F(X) \\ \phi \downarrow & \swarrow \tilde{\phi} & \\ M & & \end{array}$$

For  $X = \{1, 2, \dots, n\}$ , take  $F(X) = \mathbb{R}^n$  and

$$\begin{aligned} \phi_{\text{can}}(1) &= (1, 0, \dots, 0) \\ \phi_{\text{can}}(2) &= (0, 1, \dots, 0) \\ &\vdots \\ \phi_{\text{can}}(n) &= (0, 0, \dots, 1) \end{aligned}$$

Definition: Universal Property of Free Module

The universal property says

$$\text{Hom}_{\text{set}}(X, M) = \text{Hom}_R(F(X), M)$$

or a homomorphism out of  $F(X)$  is uniquely determined by what it does to the standard basis.

Definition: Torsion

Let  $R$  be an integral domain, e.g.  $\mathbb{Z}$ , and  $M$  be an  $R$ -module.

Then  $x \in M$  is torsion if  $r \cdot x = 0$  for  $r \neq 0$ .

Definition: Torsion Set

The set of torsion elements  $\text{Tor}(M) \subseteq M$  is a submodule.

Definition: Torsion-Free Quotient

The torsion-free quotient of  $M$  is  $M/\text{Tor}(M)$ .

The torsion-free quotient is an example of a tensor product  $M \otimes_{\mathbb{Z}} \mathbb{Q}$ .

Definition: Universal Property of Tensor Product

A bilinear map  $\phi_{\text{can}} : M \times N \rightarrow T$  is a tensor product of  $M$  and  $N$  if we can always uniquely fill in the dotted line

$$\begin{array}{ccc} M \times N & \xrightarrow{\phi_{\text{can}}} & T \\ \downarrow \phi & \swarrow \exists! R\text{-homomorphism} & \\ P & & \end{array}$$

Said differently,

$$\text{Bi}_R(M, N; P) = \text{Hom}_R(T, P)$$

Example

$$\det(e_1, e_2) \in \text{Bi}_{\mathbb{R}}(\mathbb{R}^2, \mathbb{R}^2; \mathbb{R}) = \text{Hom}_{\mathbb{R}}(T, R) \ni \tilde{\phi}$$

Where  $\tilde{\phi}$  is defined below.

How to construct  $T$  for  $R = \mathbb{R}$  and  $M = N = \mathbb{R}^2$ ?

If  $\phi : M \times N \rightarrow P$  is bilinear, then

$$\begin{aligned} \phi(xe_1 + ye_2, x'e_1 + y'e_2) &= x\phi(e_1, x'e_1 + y'e_2) + y\phi(e_2, x'e_1 + y'e_2) \\ &= xx'\phi(e_1, e_1) + xy'\phi(e_1, e_2) + x'y\phi(e_2, e_1) + yy'\phi(e_2, e_2) \end{aligned}$$

Define  $T$  to be a free  $\mathbb{R}$ -vector space with the basis  $e_1 \otimes e_1, e_1 \otimes e_2, e_2 \otimes e_1$  and  $e_2 \otimes e_2$ .

Define  $\phi_{\text{can}} : M \times N \rightarrow T$  as

$$\begin{aligned} \phi_{\text{can}}(xe_1 + ye_2, x'e_1 + y'e_2) &= xx'(e_1 \otimes e_1) + xy'(e_1 \otimes e_2) + x'y(e_2 \otimes e_1) + yy'(e_2 \otimes e_2) \\ &= (xe_1 + ye_2) \otimes (x'e_1 + y'e_2) \end{aligned}$$

So now we may construct

$$\tilde{\phi} = \begin{cases} e_1 \otimes e_1 = 0 \\ e_1 \otimes e_2 = 1 \\ e_2 \otimes e_1 = -1 \\ e_2 \otimes e_2 = 0 \end{cases}$$

such that

$$\tilde{\phi}(A(e_1 \otimes e_1) + B(e_1 \otimes e_2) + C(e_2 \otimes e_1) + D(e_2 \otimes e_2)) = B - C$$

## Tensor Product

What can we prove about the tensor product without constructing it?

1.  $T$  is unique up to isomorphism.
2. Write  $v \otimes w \in T$  for  $\phi_{\text{can}}(v, w)$ . The elements  $v \otimes w$  generate  $M \otimes N$ .

Proof of 1

Say  $\phi_{\text{can}} M \times N \rightarrow T$  and  $\phi'_{\text{can}} M \times N \rightarrow T'$  satisfy the universal property. Then there exists a unique homomorphism  $\phi : T \rightarrow T'$  satisfying

$$\begin{array}{ccc} M \times N & \xrightarrow{\phi_{\text{can}}} & T \\ \phi'_{\text{can}} \downarrow & \swarrow \phi & \\ & T' & \end{array}$$

Similarly, there exists a unique  $\phi' : T' \rightarrow T$  satisfying the inverted diagram. How can we show that

$$T \xrightarrow{\phi} T' \xrightarrow{\phi'} T \equiv T \xrightarrow{\text{id}} T$$

Construct

$$\begin{array}{ccccc} & & M \times N & \xrightarrow{\phi_{\text{can}}} & T \\ & & \downarrow \phi'_{\text{can}} & \swarrow \phi & \\ M \times N & \xrightarrow{\phi'_{\text{can}}} & T' & & \\ \downarrow \phi_{\text{can}} & \swarrow \phi' & & & \\ & T & & & \end{array}$$