Modules over Ring and Affine Geometry
But mostly Modules

Aayush Verma

MLS01
Madhava Lecture Series, Theoretical Nexus

Contents

A note about these notes. I have assumed the knowledge of a vector space defined over a field $\mathbb{F}$. I have added a few 'Note'(s) which are not relevant and can be skipped if needed. Moreover, the section of Affine Geometry has not been written up but compared to 'Modules', it is fairly short one, so, let's cheers. I thank Purnima Tiwari for taking the notes during the lecture and lending me afterwards.

In the next version of these notes, I will add the references and some extra content about modules.

1. The Structure of Rings

Mathematics, or more exactly *biased* mathematics, is heavily about the algebraic structures and maps between them. A group is one of them.

Definition 1. *A group is a set S with a binary operation $*$ which has an associative law of composition, with the closure $S * S \to S$, having a unique identity element such that every element in S is invertible under the identity.*

A group is already a monoid (which is already in the definition). Existence of idenity and inverse is a must for groups structures. A group homomorphism ϕ between two groups G and H

$$\varphi : G \to H \tag{1}$$

is a map which preserves the group structure. In particular, it sends the identity element e_G of G to the identity element e_H of H. Moreover, as we said, the structure is preserved

$$\varphi(a *_G b) = \varphi(a) *_H \varphi(b). \tag{2}$$

One can also define a group isomorphism between G and H to be a group homomorphism of which inverse map also exists, implying φ is a bijection. Two groups are of same order[1] if they are isomorphic. There are wonderful things in group theory which include group actions, Sylow theorem and representations of groups. But we will drop the groups right here only. We will start with rings now.

Definition 2 (Ring)**.** *A ring R is also an algebraic structure, like groups, but it is defined with two binary compositions $(+, *)$ called addition and multiplication respectively. Under addition, it has following properties*

1. *R is commutative under $+$, $(a + b = b + a)\ \forall a, b \in R$.*
2. *R is associative under $+$, $(a + b) + c = a + (b + c)$.*

[1] Order of the group, in finite case, is just defined as the cardinality of its underlying set. If the underlying set is infinite, then the group is infinite too.

(3) *R admits an additive identity and every element in R is invertible under such identity. $\forall a \in R, a + e = a$ such that $a + (-a) = e$.*

Under these properties, it can be seen that $(R, +)$ forms an abelian group. Now, under multiplication, the business requires care and has following properties

(1) *$(R, *)$ forms a monoid and thus associative, $(a * b) * c = a * (b * c)$.*
(2) *R with $*$ is distributive with respect to addition*

$$a * (b + c) = (a * b) + (a * c)$$

$$(b + c) * a = (b * a) + (c * b)$$

(3) *R admits 1_R such that $a * 1_R = a$.*

The property (3) may or may not be adopted. In these notes, we will assume that 1_R exists in the ring. It is called a 'rng' when 1_R is not assumed in R.

So, in a ring R, we do not assume commutativity under $*$ nor the existence of inverses for the elements. If R admits commutative with respect to multiplication, i.e, $a*b = b*a$, then the ring is called *commutative ring.* A very easy example of commutative ring (with unity) is the ring of integers $\mathbb{Z}$. Other examples include the zero ring, set of all real valued functions It is not always necessary to work with the commutative rings. But, in this notes, we will be mostly concerned with the commutative rings. Some examples of non-commutative rings are the quaternion ring $\mathbb{H}$, $n \times n$ matrices with entries from a ring R, endomorphisms[2] of an abelian group $End(G)$. It is also called the *endomorphism ring* of G.

Like group homomorphisms, we also have ring homomorphisms between two rings R and S such that for a ring homomorphism $\varphi : R \to S$

$$\varphi(a + b) = \varphi(a) + \varphi(b), \tag{3}$$

$$\varphi(a * b) = \varphi(a) * \varphi(b) \tag{4}$$

$$\varphi(1_R) = 1_S \tag{5}$$

for all the a, b in R. We can also have a composition of ring homomorphisms like

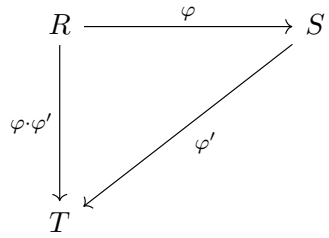
$$\varphi : R \to S, \quad \varphi' : S \to T \tag{6}$$

then

$$\varphi \cdot \varphi' : R \to T \tag{7}$$

[2]An endomorphism of a group is a group homomorphism $End : G \to G$. While an automorphism $Aut : G \to G$ is an isomorphism.

We can also draw commutative diagrams (a language which is very powerful in algebra) for these ring homomorphisms



In particular, the ring homomorphism is a mapping of the additive group of R to the additive group of S and the multiplicative group of R to the multiplicative group of S. Similarly, we can also define a ring isomorphism.

Example 1. *For the ring of (rational) integers $\mathbb{Z}$ and ring of even integers $2\mathbb{Z}$, see if the homomorphism $\varphi : \mathbb{Z} \to 2\mathbb{Z}$ is a bijection or not.*

Ideals.

Definition 3 (Ideal)**.** *An ideal of a Ring I is a subset of R such that*

$$ir \in I, \forall i \in I, r \in R \tag{8}$$

but this is a definition for commutative rings. In general, we have a left ideal and a right ideal. Eq. (8) is the definition of the left ideal, I is a right ideal when

$$ri \in I \tag{9}$$

and I is a two-sided ideal when it is both a left ideal and a right ideal (which is in the case of commutative rings).

A good example in the ring of integers $\mathbb{Z}$ is just $2\mathbb{Z}$

$$ir \in 2\mathbb{Z}, i \in 2\mathbb{Z}, r \in \mathbb{Z} \tag{10}$$

Moreover, an ideal is an additive subgroup of R and it relies on the structure of the ring since it is a subset of the ring. There are special types of ideals like principal ideals, prime ideals, maximal ideals.

Definition 4. *A ring R is called Noetherian when its ideals chains are written in ascending order and at some point, they saturate*

$$I_1 \subset I_2 \subset I_3 \cdots I_{n-1} \subset I_n = I_{n+1} \tag{11}$$

Definition 5 (Simple Rings)**.** *A ring which has only two ideals contained in the ring which are $\{0\}$ (zero ideal) and $\{1\}$ (the ring itself) is called* **simple ring**.

To see how $\{1\}$ ideal is the ring itself, let us do the following. Let $\{1\}$ be an ideal of the ring R then $\{1\} \in I$ then it immediately follows that

$$\{1\}R = R \in I \tag{12}$$

and thus $\{1\}$ ideal is the ring itself.

We would now introduce the concept of fields which have same crux of algebraic structures.

Definition 6. *A Field $(\mathbb{F}, +, *)$ is a set with the following properties under $+$*

1. *$(\mathbb{F}, +)$ is an abelian group and thus commutative.*
2. *There are many properties that can be deduced from $(\mathbb{F}, +)$ being an abelian group such that existence of identity, additive inverses and associativity.*

and under composition $*$

1. *$(\mathbb{F}, *)$ is commutative thus $ab = ba$ where $a, b \in F$.*
2. *There is an identity $1_{\mathbb{F}}$ and every element is invertible with respect to this identity.*
3. *It is distributive with respect to $+$*

$$a * (b + c) = (a * b) + (a * c)$$

Examples of Fields are the $\mathbb{R}$, and $\mathbb{Z}_n$ (since $\mathbb{Z}$ does not necessarily form a field).

Exercise 1. *$\mathbb{Z}_n$ is the quotient ring $\mathbb{Z}/n\mathbb{Z}$. Show that $\mathbb{Z}/n\mathbb{Z}$ forms a field only when n is a prime*[3]*.*

Note. *It is another good exercise to see that for a ring R, the quotient ring R/I, where $I \in R$ an ideal, is a field only when I is the maximal ideal of ring R.*

Theorem 1. *A Field $\mathbb{F}$ is a simple and commutative ring.*

Proof. Let $\mathbb{F}$ be a field and $I \subset F$. Let $a \in I$ and $a^{-1} \in \mathbb{F}$. Then $aa^{-1} \in I$ and we know that in a field $\mathbb{F}$ we have $aa^{-1} = 1$ thus $1 \in I$. It can be understood from Def. 6 that $1 \in I$ implies that field $\mathbb{F}$ is the ideal itself. It can be checked that there does not exist any other ideal except the zero ideal, of course.

We took a commutative ring R in order to satisfy

$$aa^{-1} = a^{-1}a = 1 \tag{13}$$

which is essential in a field. Thus it is found that a ring forms a field when it is commutative and simple[4]. □

[3] Thus $\mathbb{Z}_2$ will be a field but $\mathbb{Z}_6$ will not, it is good to find out why this happens.

[4] The idea of 'simple' structure also exists in Lie algebras or plain group theory

Example 2. *Show for a ring R, we have $a * 0 = 0$.*

It is easy to see that. Let $X = a * 0$ then X must be in the ring

$$\begin{aligned} X &= a * 0 \\ X + 0 &= a * (0 + 0) \\ X + 0 &= (a * 0) + (a * 0) \quad (\textit{Using distributive property}) \\ X + 0 &= X + X \implies X = 0 \end{aligned}$$

Example 3. *Show for a ring R that $-(ab) = -a(b) = a(-b)$ is the additive inverse of ab.*

Let $ab \in R$ then

$$ab + X = 0$$

Let $-ab$ be the X

$$\begin{aligned} ab + (-ab) &= a(b + (-b)) \quad (\textit{Using distributive property}) \\ &= a(0) = 0 \end{aligned}$$

1.1. **Modules over Ring.** Now, we are about to define the modules over a ring and see how it is a generalization of the vector spaces which are defined over a field.

Definition 7. *A module over ring is defined when a set M which is an abelian group $(M, +)$ and its associated ring R has the following property*

$$R \times M \to M. \tag{14}$$

This is the definition of a left R-module. One similarly defines a right R-module with the map $M \times R \to M$. When R is commutative the left R-modules and $R-$modules are same. The operation in $R \times M \to M$ is called 'scalar multiplication' such that the following are true for scalars $x, y \in R$ and $a, b, c \in M$

$$\begin{aligned} x \cdot (a + b) &= (r \cdot a) + (r \cdot b) \\ (x + y) \cdot a &= (x \cdot a) + (y \cdot a) \\ (x \cdot y) \cdot a &= x \cdot (y \cdot a) \\ 1 \cdot a &= a \end{aligned}$$

The difference between the modules and the ideals are that the modules need not be the subset of the ring. In fact, every ideal is a module but the converse need not to be true. A module is also an abelian group. A ring is a module over itself.

A bimodule (R, S) is the a module M which a left R-module and right S-module.

Note. *A module over ring R can be localized to points (prime ideals $\mathfrak{p}$) of the spectrum of the ring.*

$$M_R \to M_{\mathfrak{p} \in SpecR} \tag{15}$$

Support of a module is given by

$$SuppM_R = \{\mathfrak{p} \in SpecR, M_{\mathfrak{p}} \neq 0\} \tag{16}$$

So basically it consists of all the prime ideals which does not make modules vanish after localization.

Let us define the **torsion of a module**. It is defined to be

$$\mathsf{tor}(M) = \{m : rm = 0, r \neq 0\} \tag{17}$$

which is the collection of all m which are annihilated by r. A module is called torsion-free if $rm = 0$ is only possible when r is a zero divisor and $r = 0$ or $m = 0$. For an integrable domain (a ring where the only zero-divisor is zero), we have torsion-free modules. It is important that module have a definition of torsion and it makes them a little different to the vector spaces which are defined over field.

Our goal is to understand how modules over ring is a generalization of vector spaces defined over field. It is likely that someone is tempted to investigate into the similarity in the definition of the modules and vector spaces, especially the scalar multiplication which is crucially defined in both. At last, we wish to see the following theorem.

Theorem 2. *A module M defined over a ring R is a vector space if R is a commutative ring and a field (of course, which implies that it is commutative), where the scalars (in $\mathbb{F} \times V \to V$) are from the R.*

We hope to discuss the above two theorems. Let us compare with what we have with modules over ring and vector spaces over fields.

TABLE 1. The Dictionary.

Modules over R	**Vector Space over $\mathbb{F}$**
$M \times R \to M$	$V \times \mathbb{F} \to V$
Scalars come from the ring and division is not allowed since they are not invertible.	Scalars come from the field and they are invertible, i.e, $aa^{-1} = 1$ where $a, a^{-1} \in \mathbb{F}$.
The concept of a linear independent set is not always applicable and sometimes, we may not have any independent set in a module. Instead. we have a definition of the torsion of module.	Linear independent sets exist in a vector space and provide definition to further things like *basis*.
Similarly, a basis is hard to define for a module. And it need to have to define a basis. Same applies for the concept of dimension. When a module admits a basis and is finitely-generated, it is called **free module**.	A basis always exists and thus the concept of a dimension.
Just like vector spaces, we can define the tensor products between the modules.	Tensor products between vector spaces are defined.
Direct sum and direct product can always be defined.	Direct sum and direct product between vector spaces are clearly defined.

Theorem 3. *A vector space is a $\mathbb{F}-$module which is torsion-free.*

Proof. Let V be a module defined over the field $\mathbb{F}$. The torsion submodule of the V is

$$\mathsf{tor}(V) = \{v; \alpha v = 0, v \neq 0, \alpha \in \mathbb{F}\} \tag{18}$$

Now, let us see what is the torsion of V. We can start with

$$\alpha v = 0 \tag{19}$$

and since α is a scalar in $\mathbb{F}$ so there exists a^{-1}, we multiply a^{-1} from

$$a^{-1}av = 0 \tag{20}$$

and since $a^{-1}a = 1$ we have

$$1v = 0 \implies v = 0 \tag{21}$$

such that the there is no torsion and V is a torsion-free module. □

Using the table, we can see the modules are clearly a generalization of vector spaces. A vector space is a free module which has a field for scalars.

Now, a module is an abelian group, it shares many properties of the groups like cyclic property, center, order, and so on.

2. Affine Geometry

Will be updated soon- AV