Juan Serratos

Modules: A Naive Introduction (Rough Draft)

May 27, 2021

Springer

Contents

Preface

From my current experience, there seems to be a lacking ability, at least from the authors I've read, in a way to explain, in a pedagogical/student focused way, the ideas behind Module Theory. Once you've gotten past the basics, or possibly the intermediate, topics of (Commutative or Non-commutative) Ring Theory, your next object of study is typically Module Theory, but a large sum of books will explain these basics in a less forgiving manner — the object at hand is without a doubt complex. However, I believe that there should be a resource (which might well exists, however, I have seen it) that goes about talking and explaining module theory in a forgiving way since the initial start in learning the topic is one of the hardest hurdles to get past, like when first starting to learn pure mathematics — the start was maybe the hardest part of *doing* it, but once you've gotten into the flow, you can keep moving at better paces. I can't stress this enough, this is just my experience, so you might already well be moving through learning about Finite Projective Modules, Representation Theory, (co)Homology, or some other topic that uses the richness of the subject, and in which case this text isn't likely for you.

Moreover, it should be noted that I've only partly learned about Module Theory — knowing about projective, injective, and flat modules — and so I'm no expert, but I think the fact I'm eighteen years old and naive brings about a way of explanation that will help assist in getting a rough start/footing in Module Theory.

Now, I believe that I'm only going to be assuming knowledge of rudimentary ring and groups, but knowledge of fields and their algebraic extensions is solid preparation.

Recalling Rings

1

Definition 1. A **ring** is an abelian group R with the usual operation of *multiplication,* i.e., $(a, b) \mapsto ab$, and an "identity element" 1, satisfying for all $a, b, c \in R$:

$$\begin{aligned} a(bc) &= (ab)c \ \text{ (associative)} \\ a(b+c) &= ab + ac \ \text{ (distributivity)} \\ (a+b)c &= ab + bc \\ 1a &= a1 = a \ \text{ (identity)} \end{aligned}$$

Definition 2. A ring R is called **commutative** if it also satisfies the axiom that $ab = ba$ for all $a, b \in R$.

The rings we will be working with throughout this short manuscript will be commutative, and so if not stated explicitly, you can assume the ring is commutative (and unital). Further whenever we use the symbol A without explanation, you should and may assume that this is a commutative ring.

Definition 3. Let R and S be commutative rings. A function $\varphi\colon R \to S$ is called a **ring homomorphism** if for all $a, b \in R$

$$\begin{aligned} \varphi(a+b) &= \varphi(a) + \varphi(b), \\ \varphi(ab) &= \varphi(a)\varphi(b), \text{and} \\ \varphi(1) &= 1. \end{aligned}$$

A subset $\mathfrak{a}$ of a ring A is called an **ideal** if it satisfies that for every $x, y \in \mathfrak{a}$, then $x + y \in \mathfrak{a}$, and if $x \in \mathfrak{a}$ and $r \in A$, then $xr \in \mathfrak{a}$. For any commutative ring A, it is clear that the set $\{0\}$ is an ideal of A, which we will refer to as the **trivial** ideal. The set A is also always an ideal of A; we say that is not a *proper* ideal since it is not a proper subset of A.

It is worthwhile to compare these two notions of an ideal of a ring and a subring; they are related, but with subtle and important differences. Both an ideal $\mathfrak{a}$ and a subring S of a ring A are subsets of A which are subgroups under addition and are stable under multiplication. However, each has an additional property: for an ideal it is the absorption property, i.e., $xr \in \mathfrak{a}$ for all $x \in \mathfrak{a}$ and $r \in A$. For instance, the integers $\mathbb{Z}$ are a subring of the rational numbers $\mathbb{Q}$, but are clearly not an ideal, since $1/21 = 1/2$, which is not an integer. On the other hand a subring has a property that an ideal usually lacks, namely it must contain the unity 1 of R. For instance, the subset $2\mathbb{Z} = \{2n|n \in \mathbb{Z}\}$ is an ideal of $\mathbb{Z}$ but is not a subring.

Definition 4. Let I be an ideal of a ring R. A **coset** of I is a set of the form

$$a + I = \{a + i \mid i \in I\},$$

where $a \in R$. The element a is called a **representative** of the coset $a + I$.

Theorem 1 (Basic Properties of Cosets). *Let I be an ideal of a ring R. Let $a, b \in R$. Then the cosets of I have the following basic properties:*

1. $a + I = I$ if and only if $a \in I$;
2. $a + I = b + I$ if and only if $a - b \in I$;
3. $a + I = b + I$ if and only if $(a - b) + I = I$;
4. the two cosets $a + I$ and $b + I$ are either disjoint or equal.

Proof. (1.) Suppose $a + I = I$. So we want to show that $a \in I$, and so we proceed as follows: Since $a+I = I$, then a must be zero since $0+I = \{0+i = i \mid i \in I\}$. Moreover, since $0 \in I$ — easily seen by property (ii) — then $a = 0 \in I$. Conversely, suppose $a \in I$. Our goal now is to show that both sets are contained in one another, i.e., $a+I \subseteq I$ and $I \subseteq a+I$. Take $a+b \in a+I$, where $b \in I$. We need to show that $a + b \in I$. But I is an ideal, and bot ha and b are elements of I, so $a + b \in I$. Thus $a + I \subseteq I$. On the other hands, let $c \in I$. We must sow that $c \in a + I$. Since I is an ideal, $-a \in I$, and so $c-a \in I$. Hence, we have $c = a+(c-a) \in a+I$, as desired. Thus, $I \subseteq a+I$. We can now conclude that $a + I = I$.

(2.) First, we assume that $a + I = b + I$. Since

$$a = a + 0 \in a + I = b + I,$$

we see that $a \in b + I$. Therefore, we can write $a = b + i$ for some $i \in I$. But then $a - b = i \in I$, and $a - b \in I$, as desired. Conversely, assume that $a - b \in I$. Then $a - b = i$, for some $i \in I$. In order to show that the two sets $a + I$ and $b + I$ are equal, we show that each is contained in the other. First, we take $a + c \in a + I$, where $c \in I$. So $a + c = (b + i) + c = b + (i + c) \in b + I$, since $i + c \in I$. Thus, $a + I \subseteq b + I$. At this stage we could prove containment

in the other direction with a similar argument. However, it is easier to notice that $a - b \in I$ implies that $b - a \in I$. Hence, the preceding argument goes through with b and a interchanged. Thus, $b + I \subseteq a + I$. We conclude that $a + I = b + I$.

(3.) Follows directly from the preceding two proposition.

(4.) Suppose $a + I$ and $b + I$ are not disjoint, i.e., $(a + I) \cap (b + I) \neq \varnothing$. Then $a + I$ and $b + I$ have a common element; let x denote that element. Then we can write $x = a + i$, for some $i \in I$, and also write $x = b + j$, for some $j \in I$. Thus $x = a + i = b + j = x$, and so $a - b = j - i \in I$ since $j, i \in I$ and $j - i \in I$ (closure). By (2.), $a - b \in I$ implies that $a + I = b + I$, and therefore the two cosets are equivalent. We can conclude that if these two cosets are not disjoint, then they are equal. □

Proposition 1. *Let R be a commutative ring with $1 \neq 0$. Then R is a field if and only if it has no proper nontrivial ideals.*

Proof. (Should be noted that what the author means by "no proper nontrivial ideals" is that R's ideals aren't R and $\{0\}$.) Suppose R is a field. Assume for contradiction that I is a proper nontrivial ideal of R; that is, $I \neq R$ and $I \neq \{0\}$. Then there exists some element $a \in I$ such that $a \neq 0$. Since R is a field, a^{-1} exists. Then $1 = a^{-1}a$ where $a^{-1} \in R$ and $a \in I$, implying that, by (ii) of Definition 6, $1 = a^{-1}a \in I$. So, for the real kicker, since $1 \in I$, then for all $r \in R$, we must have that $r = r1 \in I$, once again courtesy of (ii) of Definition 6, and so $I = R$ — a contradiction.

Conversely, suppose R has no proper nontrivial ideals. Then an ideal I of R is either $I = \{0\}$ or $I = R$. Let $a \in R$ and $a \neq 0$. Consider the following set:

$$I = \{ra \mid r \in R\}$$

Firstly, I is nonempty since $a = 1a \in I$. Take any $x, y \in I$. Then $x = r_1 a$ and $y = r_2 a$ for some $r_1, r_2 \in R$. Then $x \pm y = r_1 a \pm r_2 a = (r_1 \pm r_2)a$ so $x \pm y \in I$. Moreover, for all $r \in R$, $rx = rr_1 a = (rr_1)a$, so $rx \in I$. Thus I is an ideal of R. By assumption that R has no proper nontrivial ideals, we must have that $I = R$. Noting that $a = 1a \in I$, and $1 = 1a \in I$ where $1 \in R$ and $a \in I$, then $1 = ra$ for some $r \in R$ (simply since $1 \in I$). This implies that a is invertible, and so R is a field. □

Typically, if R is a commutative ring, and for any $a \in R$, we use the notation

$$Ra = \{x \in R \mid x = ra \text{ for some } r \in R\} = \{ra \mid \text{for some } r \in R\}.$$

The previous proof showed that Ra is an ideal of R that contains a. From the definition of an ideal, it's clear that any ideal that contains an a, i.e., $a \in I$, must contain Ra, and so we are justified in saying that Ra is the smallest ideal that contains a.

Note that $R1$ consists of all of R, since every element $r \in R$ can be expressed in the form $r1$. Thus R is the smallest ideal (in fact, the only ideal) that contains the identity of R.

Definition 5. Let R be a commutative ring, and let $a \in R$. The ideal

$$Ra = \{x \in R \mid x = ra \text{ for some } r \in R\} = \{ra \mid \text{for some } r \in R\}$$

is called the **principal ideal** generated by a. The notation $\langle a \rangle$ or (a) will also be used.

An integral domain in which every ideal is a principal ideal is called a **principal ideal domain**.

Theorem 2. *$\mathbb{Z}$ is a principal ideal domain.*

Proof. Let J be an ideal of $\mathbb{Z}$. If $J = \{0\}$, then $J = \langle 0 \rangle$ is a principal ideal domain. Thus we suppose $I \neq \{0\}$. Hence J contain an element a such that $a \neq 0$. As both a and $-a$ belong to J, we can suppose $a > 0$. Hence J contains at least one positive integer, namely a.

We let m denoted the smallest positive integer in J. Dividing a by m, we obtain integers q and r such that $a = mq + r$ and $0 \leq r < m$. As $a \in J$ and $m \in J$, we have $r = a - mq \in J$, but we said $r < m$ and m is the smallest element in J; thus contradicts the minimality of m unless $r = 0$, in which case $a = mq$, so $J = \langle m \rangle = m\mathbb{Z}$. □

Let J be an ideal of the commutative ring R. Then J is a subgroup of the underlying additive group of R, and so, from group theory, the cosets of J in R determine a factor group R/J, in which again is an abelian group.

Proposition 2. *Let I be an ideal of the commutative ring R. The operation defined on the abelian group R/I by setting*

$$(a + I) \cdot (b + I) = ab + I,$$

for $a, b \in R$, is a binary operation.

Proof. To show that the binary operation is well-defined, let $a, b \in R$. If $c \in a + I$ and $d \in b + I$, then by definition $a - c \in I$ and $b - d \in I$. Multiplying $a - c$ by b and $b - c$ gives us an element that still belongs to I. Then using the distributive property and adding, we obtain $(ab - cb) + (cb - cd) = ab - cd$, and this is an element of I, showing that $cd \in ab + I$. Thus the definition of the operation $\cdot$ is independent of the choice of representatives of the cosets, and so it is a well-defined operation on the factor group R/I. □

Given any ideal, we can now construct a factor ring relative to the ideal. This parallels the construction of a factor group relative to a normal subgroup.

Theorem 3. *If I is an ideal of the commutative ring R, then R/I is a commutative ring under the operations defined for $a, b \in R$ by*

$$(a+I)+(b+I)=(a+b)+I \text{ and } (a+I)\cdot(b+I)=ab+I$$

Proof. □

Remark 1. The coset $1+I=\{1+i \mid i \in I\}$ is a multiplicative identity for R/I.

Definition 6. Let I be an ideal of the commutative ring R. The ring R/I is called the **factor ring** of R modulo I.

It should be emphasized that the elements of the quotient ring are the cosets $a+I$, where $a\ inR$. The zero element of the quotient ring is $0+I=I$, and the multiplicative identity is $1+I$.

Proposition 3. *Let I be an ideal of the commutative ring R.*

(a) *The natural projection $\pi\colon R \to R/I$ defined by $\pi(a)=a+I$ for all $a \in R$ is a ring homomorphism, and* $\ker(\pi)=I$.

(b) *There is a one-to-one correspondence between the ideals of R/I and ideals of R that contain I. The correspondence is defined as follows: to each ideal J of R/I we assign the ideal $\pi^{-1}(J)$ of R; to each ideal J of R that contains I we assign the ideal $\pi(J)$ of R/I.*

Proof. For (a): Suppose $a, b \in R$. Then $\pi(a+b)=(a+b)+I=(a+I)+(b+I)=\pi(a)+\pi(b)$. Similarly, $\pi(ab)=ab+I=(a+I)\cdot(b+I)=\pi(a)\pi(b)$. Lastly, $\pi(1)=1+I$, which is the identity for R/I. Moreover, $\ker(\pi)=\{a \in R \mid \pi(a)=0+I=I\}=I$. □

.0.1 Prime Ideals and Maximal Ideals: