AN INTRODUCTION TO MODULES

NEIL MAKUR

Abstract. We define the notion of a module over a ring, and look at some examples of modules. We then show that modules do not necessarily have a basis, and follow this by especially looking at how abelian groups are modules over the integers. After this, we define submodules and give a few examples of submodules before turning to a few theorems about them. Then, we define quotient modules. Next, we look at module homomorphisms, and look at the example of the free module. We end by defining module isomorphisms, and proving the first isomorphism theorem for modules.

1. Defining Modules

1.1. **The Definition.** The notion of a module over a ring is similar to both that of a vector space over a field or a group action. Both are defined as a set, say S and an algebraic structure A, with a function from $A \times S$ to S. A module is defined similarly.

Definition 1.1. Given a (possibly noncommutative) ring, R, a left R-Module is an abelian group M (with operation $+$, which we call addition) with a map $\cdot : R \times M \to M$ (called scalar multiplication) defined for all $(\alpha, m) \in R \times M$, where we write $\alpha \cdot m$ to denote $\cdot(\alpha, m)$, such that the following axioms are true.

(1) $\alpha \cdot (\beta \cdot m) = (\alpha\beta) \cdot m$
(2) $(\alpha + \beta) \cdot m = \alpha \cdot m + \beta \cdot m$
(3) $\alpha \cdot (m + n) = \alpha \cdot m + \alpha \cdot n$
(4) $1 \cdot m = m$

with $\alpha, \beta \in R$ and $m, n \in M$.

Remark 1.2. The symbol "+" is used for both addition, and the addition operation of R. The use will usually be clear from context. For example, in the equation $(\alpha+\beta)\cdot m = \alpha\cdot m+\beta\cdot m$, we use $+$ for R's addition on the left hand side (adding two ring elements), and we use it for the addition on the right (adding two elements of M). However, in the equation $\alpha \cdot (m + n) = \alpha \cdot m + \alpha \cdot n$, $+$ is used only for addition.

Remark 1.3. A left R-Module is also called a "left module over R". There is also a right R-Module defined similarly ($\cdot$ maps $M \times R$ to M). In the case that R is commutative, we can make left R-Modules into right R-Modules by defining $\alpha \cdot m = m \cdot \alpha$. Anytime we say module, we will be referring to a left module, though we will assume that our rings are commutative unless otherwise stated.

We can also find some facts that are true for all modules.

Date: July 2020.

Proposition 1.4. *Given a ring R, and an R-Module M, the following are true.*

(1) $0 \cdot m = e$
(2) $-1 \cdot m = -m$
(3) $\alpha \cdot e = e$

for $\alpha \in R$ and $m \in M$

Proof. Firstly, let us consider $0 \cdot m$. This is equal to $(0+0) \cdot m = 0 \cdot m + 0 \cdot m$. Therefore, subtracting $0 \cdot m$ from both sides, we get that $0 \cdot m = e$. Next, if we consider $0 \cdot m$, we get that this is equal to $(1-1) \cdot m = 1 \cdot m + (-1) \cdot m$. Because this is the identity, we get that $-1 \cdot m = -m$. Finally, finding $\alpha \cdot e$, we see that this is equal to $\alpha \cdot (e+e) = \alpha \cdot e + \alpha \cdot e$, which means that $\alpha \cdot e = e$. ■

1.2. **Examples of Modules.** We can find many different modules over rings, which we will give some examples of here.

- If we have a (not necessarily commutative) ring R, then R is both a left and right module over itself, with $\alpha \cdot \beta$ defined as simply $\alpha\beta$ ($\alpha, \beta \in R$), and addition defined as R's addition. The distributive and associative axioms are already satisfied by the ring axioms, and the definition of 1 satisfies the last axiom.
- If we have a field k with a vector space V over k, then V is a k-Module. We can see this by noticing that the module axioms are satisfied by the definition of a vector space, and fields are rings where every nonzero element is a unit.
- We can make $\mathbb{A}_k^n$ into a module (and in fact a vector space) over k. To do this, we will define addition pointwise as

  $$(a_1, a_2, \ldots, a_n) + (b_1, b_2, \ldots, b_n) = (a_1 + b_1, a_2 + b_2, \ldots, a_n + b_n),$$

  and we define scalar multiplication as

  $$\alpha \cdot (a_1, a_2, \ldots, a_n) = (\alpha a_1, \alpha a_2, \ldots, \alpha a_n)$$

  with $(a_1, a_2, \ldots a_n), (b_1, b_2, \ldots, b_n) \in \mathbb{A}_k^n$ and $\alpha \in k$. The distributive and associative requirements are satisfied by the field axioms, and the last requirement is satisfied by the definition of 1. When $k = \mathbb{R}$, we gain the familiar vector arithmetic of linear algebra.
- If R is a ring, and we define

  $$R^n = \{(a_1, a_2, \ldots, a_n) | \forall i \leq n \in \mathbb{Z}^+, a_i \in R\}.$$

  We can make this into a module similar to how we made $\mathbb{A}_k^n$ a module. This is called the "free module of rank n over R".
- If R is a ring, M is a R-Module, and I is an ideal of R such that $\alpha \cdot m = e$ for all $\alpha \in I$ and $m \in M$, we can turn M into a R/I-Module. We will do this by defining

  $$(\alpha + I) \cdot m = \alpha \cdot m$$

  for $\alpha \in R$ and $m \in M$. It is easy to check that this is well-defined. To show that the axioms are satisfied, we can look at

  $$(\alpha + \beta + I) \cdot m,$$

  and see that this is equal to

  $$(\alpha + \beta) \cdot m = \alpha \cdot m + \beta \cdot m = (\alpha + I) \cdot m + (\beta + I) \cdot m.$$

We can also see that

$$(\alpha + I) \cdot (m + n) = \alpha \cdot (m + n) = \alpha \cdot m + \alpha \cdot n = (\alpha + I) \cdot m + (\alpha + I) \cdot n,$$

and that

$$(\alpha + I) \cdot ((\beta + I) \cdot m) = (\alpha + I) \cdot (\beta \cdot m) = \alpha \cdot (\beta \cdot m) = (\alpha\beta) \cdot m = (\alpha\beta + I) \cdot m.$$

Finally, we have

$$(1 + I) \cdot m = 1 \cdot m = m.$$

1.3. **Modules Against Vector Spaces.** If we look at our definition of a module, we can see that it is identical to the definition of a vector space except that we have a ring instead of a field. This gives us the intuition that they are similar structures. However, there are large differences between them.

One difference between modules and vector spaces is that modules do not necessarily have a basis. We will show this for the specific example of $\mathbb{Q}$ over $\mathbb{Z}$. First, we will show that we can actually do this, and that $\mathbb{Q}$ is a module over $\mathbb{Z}$.

Claim 1.5. *The rationals, $\mathbb{Q}$ form a module over $\mathbb{Z}$, with scalar multiplication defined as regular multiplication, and the addition defined as regular addition.*

Proof. We know that $\mathbb{Q}$ forms an abelian group under addition. If we define $\alpha \cdot m$ with $\alpha \in \mathbb{Z}$ and $m \in \mathbb{Q}$ as regular multiplication, then we can show that the other axioms hold. We know that multiplication is associative, so we have $a(b\frac{c}{d}) = (ab)\frac{c}{d}$, with $a, b, c, d \in \mathbb{Z}$. We also know that multiplication distributes, so $(a + b)\frac{c}{d} = a\frac{c}{d} + b\frac{c}{d}$, and $a(\frac{c}{d} + \frac{e}{f}) = a\frac{c}{d} + a\frac{e}{f}$. Finally, we know that $1 \cdot \frac{a}{b} = \frac{a}{b}$. ∎

Now we are ready to show that $\mathbb{Q}$ has no basis.

Theorem 1.6. *Treating $\mathbb{Q}$ as a module over $\mathbb{Z}$, there is no basis of $\mathbb{Q}$.*

Proof. First, we will show that a basis for $\mathbb{Q}$ can not consist of one element. If we assume that this is possible, then there is some basis, say $\frac{a}{b}$, of $\mathbb{Q}$ with $a, b \in \mathbb{Z}$, and b nonzero. Then, there is some integer, r, such that

$$r\frac{a}{b} = \frac{a}{b+1}.$$

However, this implies that $r = \frac{b}{b+1}$. Because $b \neq 0$, we have that r is not an integer. This is a contradiction, and therefore no one element can span $\mathbb{Q}$.

Now we will show that any two elements of $\mathbb{Q}$ are linearly dependent. If we have two elements of $\mathbb{Q}$, $\frac{a_1}{b_1}$ and $\frac{a_2}{b_2}$, where $a_1, b_1, a_2, b_2 \in \mathbb{Z}$ and $b_1, b_2 \neq 0$, then we want to find two nonzero integers r_1 and r_2 such that

$$r_1\frac{a_1}{b_1} + r_2\frac{a_2}{b_2} = 0.$$

If we set $r_1 = a_2b_1$, and $r_2 = -a_1b_2$ this equation is satisfied and both r_1 and r_2 are integers, and so any two rational numbers are linearly dependent, and therefore can not form a basis. Now, if we assume that we have n elements, we can write the nth element in terms of the first element, and so the set of elements is linearly dependent, and therefore can not form a basis. ∎

This shows that, although they have similar definitions, there are differences between Modules and Vector Spaces.

2. Groups as Modules Over the Integers and the Integers Modulo n

2.1. **The Integers.** If we have an abelian group, G, there are many properties relating to G and the integers, some of which we will show here.

Remark 2.1. When talking about an abelian group, we will assume that it is not the trivial group $\{e\}$.

Theorem 2.2. *Let G be an abelian group. Then G is a $\mathbb{Z}$-Module, with scalar multiplication defined as below.*

$$n \cdot g = \begin{cases} \underbrace{g + g + \cdots + g}_{n \text{ times}} & \text{if } n > 0 \\ e & \text{if } n = 0 \\ \underbrace{-g - g - \cdots - g}_{n \text{ times}} & \text{if } n < 0 \end{cases}$$

where $g \in G$, $n \in \mathbb{Z}$, and $-g$ is g's inverse.

Proof. We will check that this definition satisfies the axioms. If we want to find $n \cdot (m \cdot g)$ for $n, m \in \mathbb{Z}$ and $g \in G$, we see that this is equal to

$$n \cdot (\underbrace{g + g + \cdots + g}_{m \text{ times}}) = \underbrace{g + g + \cdots + g}_{nm \text{ times}}.$$

We can therefore rewrite this as $(nm) \cdot g$, which satisfies the first axiom. Now, if we have $(n + m) \cdot g$, we will get

$$\underbrace{g + g + \cdots + g}_{n+m \text{ times}}.$$

We can split this to get

$$\underbrace{g + g + \cdots + g}_{n \text{ times}} + \underbrace{g + \cdots + g}_{m \text{ times}} = n \cdot g + m \cdot g,$$

proving that the second axiom is satisfied. Next, let us consider $n \cdot (g+h)$ for $n \in \mathbb{Z}$, $g, h \in G$. This is equal to

$$\underbrace{(g + h) + (g + h) + \cdots + (g + h)}_{n \text{ times}}.$$

Because G is abelian, we can rewrite this as

$$\underbrace{g + g + \cdots + g}_{n \text{ times}} + \underbrace{h + h + \cdots + h}_{n \text{ times}} = n \cdot g + n \cdot h,$$

satisfying the third axiom. Finally, if we have $1 \cdot g$, this is just g, and so the last axiom is satisfied. ∎

Now let us assume that G is nonabelian. Ignoring the fact that modules must be abelian groups, let us show that this does not work. If we want to find $2 \cdot (a + b)$, we get that this is equal to $a+b+a+b$. However, by the third axiom, this is also equal to $2 \cdot a + 2 \cdot b = a+a+b+b$. A little bit of work proves that G must be abelian. Although this is interesting, it turns out that, for finite groups, we can do more.

2.2. **The Integers Modulo n.**

Theorem 2.3. *If G is an abelian group of order n, then it is a $\mathbb{Z}/n\mathbb{Z}$-Module with scalar multiplication defined the same way as with $\mathbb{Z}$.*

Proof. We have already shown that G is a $\mathbb{Z}$-Module. Therefore, we only need to show that the action of two numbers that are congruent modulo n on some element are equal (that it is well-defined). To do this, let us suppose that we have $a \cdot g$, and $(a+bn) \cdot g$ where $a, b \in \mathbb{Z}$ and $g \in G$. We want to show that these are equal. We can rearrange the second equation to get $a \cdot g + b \cdot (n \cdot g)$. By Lagrange's Theorem, we know that $\underbrace{g + g + \cdots + g}_{|G| \text{ times}} = |G| \cdot g = n \cdot g = e$. Therefore, we can turn our equation into $a \cdot g + b \cdot e = a \cdot g$, which is what we wanted to show. ∎

This theorem can in fact be generalized more.

Theorem 2.4. *Let G be an abelian group such that $n \cdot g = e$ for all $g \in G$ and some $n \in \mathbb{Z}^+$. Then, G is a $\mathbb{Z}/n\mathbb{Z}$-Module.*

Proof. We must once again only show that this is well defined. If we take $a \cdot g$ and $(a+bn) \cdot g$, we get that the latter is equal to $a \cdot g + b \cdot (n \cdot g) = a \cdot g + b \cdot e = a \cdot g$ by the definition of n. ∎

Theorem 2.3 is a special case of this, where $n = |G|$. Note that we did not specify that n must be the smallest such value. We can, however, find a relationship between the smallest possible value, and all of the possible values.

Theorem 2.5. *Let $n_0 \in \mathbb{Z}^+$ be the smallest value such that $n_0 \cdot g = e$ for all $g \in G$ where G is abelian. Then $n \cdot g = e$ for every g if and only if n is a multiple of n_0.*

Proof. Let us suppose that $n = bn_0$. Then we get

$$n \cdot g = \underbrace{g + g + \cdots + g}_{n \text{ times}} = \underbrace{n_0 \cdot g + n_0 \cdot g + \cdots + n_0 \cdot g}_{b \text{ times}} = \underbrace{e + e + \cdots + e}_{b \text{ times}} = e.$$

To show the other way, we can consider the sum of n gs. If we let $0 \leq n' < n_0$ be n reduced modulo n_0, then this is equivalent to finding the sum of n' gs. If we want our sum of n gs to be the identity, then our sum of n' gs must also be the identity. However, we know that $n' < n_0$, and the definition of n_0 states that there are no smaller nonzero lengths of sums to get the identity. Therefore, we have that $n' = 0$, or that $n \equiv 0 \pmod{n_0}$. ∎

We also have a way of computing n_0. Namely, $n_0 = \operatorname{lcm}(|g_1|, |g_2|, \ldots, |g_{|G|}|)$ where all elements of G are represented as a g_i. This is fairly easy to check, as this value works, and if we have a number (say, n_1) below this value, then there some element (g_0) whose order does not divide n_1, and so $n_1 \cdot g_0 \neq e$.

Let us look at the example of the Klein-4 group, which is defined as the group of order 4 such that $g^2 = e$ for all of its elements (This is abelian, see [DF04, §1.1, Problem 25]). It is also isomorphic to $\mathbb{Z}/2\mathbb{Z} \times \mathbb{Z}/2\mathbb{Z}$.

Example. The Klein-4 group has order 4, and thus is a $\mathbb{Z}/4\mathbb{Z}$-Module. However, this particular group has the property that all elements have order ≤ 2, and is thus also a $\mathbb{Z}/2\mathbb{Z}$-Module. The group is also a vector space over $\mathbb{Z}/2\mathbb{Z}$, as 2 is prime, and thus $\mathbb{Z}/2\mathbb{Z}$ is a field.

3. Submodules and Quotient Modules

3.1. **Submodules.** Similar to how groups, rings and fields can contain smaller versions of the same algebraic structure, there are also submodules, which are defined as below.

Definition 3.1. Let R be a ring, and M be a R-Module. A subgroup, N, of M is a submodule of M if $\alpha \cdot n \in N$ for all $\alpha \in R$ and $n \in N$.

Remark 3.2. Similar to subgroups, subrings, and subfields, submodules form modules in and of themselves.

3.2. **Examples of Submodules.**

- If we have an abelian group, G, with $H \leq G$, then H forms a submodule of G (over $\mathbb{Z}$). We can check the requirements. We already know that H is a subgroup of G, and that G is a $\mathbb{Z}$-Module, so we only need to check that it is closed under scalar multiplication. If we have $n \in \mathbb{Z}$, and $h \in H$, then $n \cdot h = \underbrace{h + h + \cdots + h}_{n \text{ times}}$. This must also be in H, because H is closed under addition.
- Treating a ring R as an R-Module, the ideals of R are submodules of R. We can see this by noticing that ideals are abelian groups using addition (multiply by 0 and -1 to get identity and inverses respectively). Ideals are also defined to be closed under multiplying by elements of R, which is our definition of scalar multiplication.
- If R is a noncommutative ring, then left ideals are submodules of R as a left R-Module, and the right ideals are submodules of R as a right R-Module.
- Given a ring R, and an R-Module $M \neq \{e\}$, then M is guaranteed to have at least two submodules. Namely M itself, and $\{e\}$ (called the trivial submodule).
- If we have the free module of rank n over R for some ring R, then obvious submodules are given by the elements where select components are zero (for example, $(0, 0, a_3, \ldots, 0)$ has all components as zero except for a_3). If we have i components that are zero, then there are $n - i$ nonzero elements. We can get the intuition that this is isomorphic to the free module of rank $n - i$ over R, although we have not defined module isomorphisms yet.

3.3. **Theorems Involving Submodules.** There are two theorems about submodules that we will prove here.

Theorem 3.3. *If M is an R-Module, and N is a submodule of M, then $|N|$ divides $|M|$.*

Proof. We know that $N \leq M$, by the definition of a submodule. We also know that, by Lagrange's Theorem, if $H \leq G$, then $|H|$ divides $|G|$. Therefore, we can say that $|N|$ divides $|M|$. ■

We also have a way of telling whether or not we have a submodule.

Theorem 3.4 (The Submodule Criterion)**.** *Let R be a ring and M an R-Module. Given $N \subseteq M$, it is a submodule of M if and only if $N \neq \emptyset$, and $x + \alpha \cdot y \in N$ for all $\alpha \in R$ and $x, y \in N$.*

Proof. If N is a submodule, then $e \in N$, so $N \neq \emptyset$. It is also closed under scalar multiplication and addition, so $x + \alpha \cdot y \in N$ for all $\alpha \in R$ and $x, y \in N$. To show the other way, let us assume our two criterion. If we let $\alpha = -1$, then we get that $x - y \in N$ for all $x, y \in N$, which is exactly the criterion for being a subgroup. Now, if we let $x = e$, then we also have that N is closed under scalar multiplication, proving that it is a submodule of M. ■

3.4. **Quotient Modules.** Quotient modules are also defined similarly to groups.

Definition 3.5. Let R be a ring, M be an R-Module, and $N \leq M$ be a submodule of M. The quotient module M/N is the group M/N (treating M and N as abelian groups) with scalar multiplication defined as

$$\alpha \cdot (m + N) = \alpha \cdot m + N$$

for all $\alpha \in R$ and $m + N \in M/N$.

We can check that this is well-defined. If we have that $m+N = m'+N$, then $m-m' \in N$, and so $\alpha \cdot (m - m')$ is also in N. Therefore, $\alpha \cdot m + N = \alpha \cdot m' + N$.

Remark 3.6. If we treat a ring as a module over itself, quotienting the ring (as a module) will have the same effect as quotienting the ring (in both cases, we divide the ring into equivalence classes). Furthermore, it would be nice if, for any equivalence class that we divide the ring into, that equivalence class is kept when we treat the ring as a module over itself. From here, we can see that we use ideals rather than subrings in quotient rings because ideals are submodules of rings (when the rings are acting as modules over themselves), whereas subrings are not submodules of the rings, and we thus cannot quotient out by them. We can also see that there is no concept of a quotient field, because submodules of a field (when it is a module over itself) are only the trivial submodule, and the field itself (the ideals contain units, and are therefore the entire field, see [DF04, §7.4, Proposition 9]).

4. Module Homomorphisms and Isomorphisms

4.1. **Homomorphisms.** Just like having quotients and other similarities with groups, modules also have homomorphisms, defined as follows.

Definition 4.1. Let R be a ring, and M and N be R-Modules. A function $\phi : M \to N$ is a homomorphism if the following conditions are satisfied.

(1) $\phi(m_1 + m_2) = \phi(m_1) + \phi(m_2)$
(2) $\phi(\alpha \cdot m) = \alpha \cdot \phi(m)$

for all $m, m_1, m_2 \in M$, and $\alpha \in R$.

We can also define the kernel and image predictably.

Definition 4.2. Let R be a ring, and M and N be R-Modules, with a homomorphism $\phi : M \to N$. The kernel of ϕ (denoted $\ker(\phi)$) is the set $\{m \in M | \phi(m) = e_N\}$.

Definition 4.3. Let R be a ring, and M and N be R-Modules, with a homomorphism $\phi : M \to N$. The image of ϕ (denoted $\mathrm{im}(\phi)$) is the set $\{n \in N | \exists m \in M | \phi(m) = n\}$.

We can also show that both the kernel and image of a homomorphism form modules (in fact, submodules of M and N respectively).

Proposition 4.4. *If R is a ring with M and N as R-Modules such that there is a homomorphism $\phi : M \to N$, then $\ker(\phi)$ and $\mathrm{im}(\phi)$ are submodules of M and N respectively.*

Proof. We know that $\ker(\phi)$ forms a subgroup of M. Therefore, we must only show that it is closed under scalar multiplication. If we let $m \in \ker(\phi)$, we must show that $\alpha \cdot m \in \ker(\phi)$. Let us find $\phi(\alpha \cdot m)$ for some $\alpha \in R$. This is equal to $\alpha \cdot \phi(m) = \alpha \cdot e_N = e_N$, so $\alpha \cdot m \in \ker(\phi)$. Therefore, $\ker(\phi)$ is a submodule of M. To show that $\mathrm{im}(\phi)$ is a submodule of N, we will

first notice that $\text{im}(\phi) \leq N$, and so we only need to check that it is closed under scalar multiplication. If we have $n \in \text{im}(\phi)$ with $n = \phi(m)$, then $\alpha \cdot n = \alpha \cdot \phi(m) = \phi(\alpha \cdot m)$ for every $\alpha \in R$. Therefore, $\text{im}(\phi)$ is closed under scalar multiplication, and forms a submodule of N. ■

The ways of checking the injectivity and surjectivity of a homomorphism from groups also carry over.

Proposition 4.5. *Let R be a ring, M and N be R-Modules, and $\phi : M \to N$ be a homomorphism. Then ϕ is injective if and only if $ker(\phi) = \{e_M\}$, and ϕ is surjective if and only if $im(\phi) = N$.*

The proof of this is nearly identical to the proof of this for groups, and so we omit it.

4.2. **Homomorphisms of the Free Module.** Let us consider the free modules of differing rank over R. We can create may homomorphisms out of these.

Proposition 4.6. *The function $\pi_i : R^n \to R$ defined by*

$$\pi_i(a_1, a_2, \ldots, a_n) = a_i$$

is a surjective homomorphism.

Proof. If we find $\pi_i((a_1, a_2, \ldots, a_n)+(b_1, b_2, \ldots, b_n))$, we see that this is equal to $\pi_i(a_1+b_1, a_2+b_2, \ldots, a_n + b_n) = a_i + b_i$, which is equal to $\pi_i(a_1, a_2, \ldots, a_n) + \pi_i(b_1, b_2, \ldots, b_n)$, proving (1). Now, if we find $\pi_i(\alpha \cdot (a_1, a_2, \ldots, a_n))$, we see that we get $\pi_i(\alpha a_1, \alpha a_2, \ldots, \alpha a_n) = \alpha a_i$. This is equal to $\alpha \cdot \pi_i(a_1, a_2, \ldots, a_n)$, proving that π_i is a homomorphism. We can also see that every $\alpha \in R$ is mapped to by $(\alpha, \alpha, \ldots, \alpha)$, which shows that π_i is surjective. ■

We can also generalize this homomorphism.

Proposition 4.7. *If we have $A = \{i_1, i_2, \ldots, i_k\}$ with distinct elements, then the function $\pi_A : R^n \to R^k$ with $k \leq n$ for some ring R defined by*

$$\pi_A(a_1, a_2, \ldots, a_n) = (a_{i_1}, a_{i_2}, \ldots, a_{i_k})$$

is a surjective homomorphism.

The proof is similar to that of Proposition 4.6, and so it is left as an exercise for the reader.

We can also create an injective homomorphism $\pi : R^n \to R^k$ where $k \geq n$ given by $\pi(a_1, a_2, \ldots, a_n) = (a_1, a_2, \ldots, a_n, 0, 0, \ldots, 0)$. There are in fact $\frac{k!}{(n-k)!}$ possibilities for this type of homomorphism (of course, some of these may not be distinct under certain circumstances).

4.3. **Isomorphisms.** We can also define isomorphisms quite predictably.

Definition 4.8. Let R be a ring, and M and N be R-Modules. If we have a homomorphism $\phi : M \to N$, we call it an isomorphism if it is bijective.

Example. The Klein-4 group and $\mathbb{Z}/2\mathbb{Z} \times \mathbb{Z}/2\mathbb{Z}$ are isomorphic (both have order 4, and have the property that $2 \cdot g = e$ for all g, which uniquely determines the group). They are also both abelian, and can thus be considered $\mathbb{Z}$-Modules. It is trivial to check that the action of elements of $\mathbb{Z}$ commute with the isomorphism, and so we can create a module isomorphism between them.

Example. More generally, if G and H are abelian groups with $G \cong H$ and isomorphism ϕ, then, treating them as $\mathbb{Z}$-Modules, the isomorphism between them is a module isomorphism. We can see this by noticing that $\phi(n \cdot g) = \phi(\underbrace{g + g + \cdots + g}_{n \text{ times}}) = \underbrace{\phi(g) + \phi(g) + \cdots + \phi(g)}_{n \text{ times}} = n \cdot \phi(g)$.

4.4. **The Isomorphism Theorem.** We have seen that many theorems and definitions carry over to modules. This is no different for the isomorphsim theorem.

Theorem 4.9. *If R is a ring and M and N are modules with a homomorphism $\phi : M \to N$, then*

$$M/ker(\phi) \cong im(\phi)$$

Proof. By the isomorphism theorem for groups, we know that $\psi : M/\ker(\phi) \to \text{im}(\phi)$ defined by $\psi(m + \ker(\phi)) = \phi(m)$ is well-defined, and is a group isomorphsim. Therefore, we must show that this function works with scalar multiplication. We can show this fairly easily, as below.

$$\psi(\alpha \cdot (m + \ker(\phi))) = \psi(\alpha \cdot m + \ker(\phi)) = \phi(\alpha \cdot m) = \alpha \cdot \phi(m) = \alpha \cdot \psi(m + \ker(\phi))$$

for all $\alpha \in R$ and $m \in M$. ■

References

[DF04] David Steven Dummit and Richard M Foote. *Abstract algebra*, volume 3. Wiley Hoboken, 2004.
[Pou10] Dylan Poulsen. Modules: An introduction. 2010.