0.1 Introduction/Definitions

Modules are a generalization of vector spaces, which allow us to address many common structures in Mathematics. But it comes at a cost. There are invariants associated with vector spaces like dimension which are harder to define for modules. First I'll talk about the way modules are similar to structures we're familiar with, and then I'll discuss the differences and the tools we use to deal with these differences.

We define an R-module as the pair $(M, \cdot)$ where M is an abelian group under addition, and $\cdot : R \times M \to M$ such that for $r, s \in R$ and $m, n \in M$,

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

These are the same distributive relations between a vector space and the field we take it over, except we are now taking scalars to be in a ring R. So k-vector spaces are also k-modules for some field k. For the rest of the talk, we omit the explicit $\cdot$ unless there is ambiguity.

Example 0.1.

- Abelian groups are also $\mathbb{Z}$ modules.
- A ring R is an R-module over itself.

0.2 Operations on Modules

Given any structure, we think of substructures, and we can talk about submodules. A *submodule* N of an R-module M is a subgroup of the abelian group M, and closed under multiplication by scalars. Once we have submodules, since M is an abelian group we can take quotients by any submodule N of M, by treating N is a subgroup. So we can talk about M/N, with scalar multiplication on an equivalence class is the equivalence class of the product in M.

We now define the following common submodules:

Definition 0.2.

- $IM = \{\sum x_i m_i : x_I \in I, m_i \in M\}$. We can think of this as restricting the scalars to an ideal of the original ring. There is no analogous concept for vector spaces because the only ideals of a field are trivial.
- The *annhihilator* of a module the ideal in R, $ann(M)$ consisting of all elements $r \in R$ such that $r \cdot M = 0$. In other words, the annihilator is the largest ideal I for which $IM = 0$.
- If $m \in M$ such that $r \cdot m = 0$ for some non-zero divisor in R, we call m a *torsion element*. The collection of all torsion elements is called the *torsion submodule*. If 0 is the only torsion element (the torsion module is trivial), then the module M is *torsion free*.

Remark 0.3. If M is an R-module and I an ideal of R, then M/IM is an R/I-module.

We only need to prove that scalar multiplication is well-defined. In particular, if $\mathfrak{m}$ is a maximal ideal of R, then $M/\mathfrak{m}M$ is a $R/\mathfrak{m}$ vector space. This will be of particular use when defining modules over local rings.

We also have the direct sum of R-modules $\oplus_{i\in\mathcal{I}}M_i$ which is all finite linear combinations of elements in the M_i. That is,

$$\bigoplus_{i\in\mathcal{I}} M_i = \{\sum r_i m_i : r_i \in R, m_i \in M_i\}.$$

The direct product is a similar structure that allows for infinitely many elements. We can identify it with the set of sequences, with the i^{th} entry in M_i:

$$\prod_{i\in II} M_i = \{(m_1, m_2, \cdots) : m_i \in M_i\}.$$

0.3 Module Homomorphisms

Given any kind of structure, we also think about structure preserving maps between the two structures, homomorphisms. An R-module homomorphism $\phi : M \to N$ satisfies

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

for $r \in R$ and $x, y \in M$. We can also call ϕ R-linear.

We note that given an R-module homomorphism $\phi : M \to N$, $ker(\phi)$ and $Im(\phi)$ are submodules are M and N respectively. And with homomorphisms come the isomorphism theorems. We provide the first two here:

Theorem 0.4. *Given an R-module homomorphism from $\phi : M \to N$,*

$$M/ker(\phi) \simeq Im(\phi).$$

Moreover, if L and K are submodules of M, then

$$(L+K)/L \simeq K/(L\cap K).$$

The proof of this is analoguous to the proof for groups and rings.

Example 0.5.
- We can also show that the set of all homomorphisms from M into N, $\mathrm{Hom}(M, N)$ is an R-module.
- If $\phi : R \to S$ is a ring homomorphism, S is an R-module.
- If M is an R module and $S \subset End_R(M)$, then M is an S-module.

  Given $\sigma \in S$, define $\sigma \cdot m := \sigma(m)$.

0.4 Why Dimension is Hard

We now show why a naive extension of our idea of dimension (and a basis) of a vector space to an analogous invariant in a module fails. In a vector space, there are two common equivalent definitions of dimension:

1. The cardinality of a maximal linearly independent set.

2. The cardinality of a minimal generating set.

Recall that we say a set S is linearly independent if, given a finite sum

$$\sum a_i s_i = 0,$$

we have every $a_i = 0$.

We say a set S generates M if every element in M can be expressed as a finite linear combination of elements in S. S is a minimal generating set if no finite subset of S generates M.

Let's see where this definition falls short when we consider modules. Consider $\mathbb{Z}_3$ as a $\mathbb{Z}$ module. Then every proper (nontrivial) subset is linearly dependent. So the idea of maximum cardinality of a linearly independent set doesn't make sense. Also, every nontrivial subset generates $\mathbb{Z}_3$, so we have that every generating set is linearly dependent. An analogous argument can be made for any abelian group of finite order.

We now prove the following proposition, which is an example of how the cardinality of a minimal generating set is not well-defined.

Proposition 0.6. *The integers $\mathbb{Z}$ considered as a module over itself has a minimal generating set of n elements, $n \geq 1$.*

Proof. Given n arbitrary in $\mathbb{N}$ consider distinct primes $p_1, \cdots, p_n$, and define $N = \prod_i p_i$. We claim that $S = \{N/p_1, \cdots, N/p_n\}$ form a minimal generating set. An induction proof shows that the $\gcd(N/p_1, \cdots, N/p_n) = 1$, so S is a generating set. If we omit any N/p_i from S, then each remaining element has p_i as a factor. In which case $S \setminus \{N/p_i\}$ generates $\mathbb{Z}/p_i\mathbb{Z}$, not $\mathbb{Z}$ itself. $\square$

Now that we've established that things aren't as nice, we can take two approaches. First, explore only the modules where things are nice (in our case, modules that have a basis). Second, develop tools to deal with these more general cases. The remaining part of the talk will explore a bit of both.

0.5 Free Modules

A free module is a module M with a basis (linearly independent generating set). Equivalently, a free R-module is isomorphic to the direct sum $\oplus_{i \in \mathcal{I}} M_i$, where $M_i \simeq R$. We also denote this as $R^{\{\mathcal{I}\}}$. If $|\mathcal{I}| = n$, then we write M as R^n.

We now prove the equivalence stated above. Note that if M has a basis

$e_1, \cdots, e_n, \cdots$, then M is the direct sum of submodules of the form Re_i. Conversely if M is isomorphic to $R^{\{\mathcal{I}\}}$, then its basis is formed by the "standard basis vectors": vectors with 1 in a single component and zero everywhere else.

The direct sum of free modules is free, but the direct product may not be. The following proposition below, proven by Baer in 1937, gives us a counterexample.

Proposition 0.7. *$\mathbb{Z}^\infty$ is not a free abelian group, and hence not a free $\mathbb{Z}$-module.*

PROOF.

First note that if G is a free abelian group with basis $\{e_\lambda\}_{\lambda\in\Lambda}$ and H is generated by some subset of the basis vectors indexed by $J \subset \Lambda$, then G/H is also free with basis $\{\bar{e_\lambda} : \lambda \in \Lambda \notin J\}$. So it suffices to show that a carefully chosen quotient of $\mathbb{Z}^\infty$ is not free.

Now given a $\mathbb{Z}$-module A, we define $n \in \mathbb{Z}$ to divide $a \in A$ if there exists $x \in A$ such that $a = nx$. Note that considering $\mathbb{Z}$ as a module over itself, every element has finitely many divisors. However this does not hold for $\mathbb{Q}$ as a $\mathbb{Z}$-module. We now use this generalization of divisors to prove a necessary condition for an abelian group to be free:

Lemma 0.8. *Every non-zero element of a free abelian group has finitely many divisors.*

PROOF. Let G be free and $a = \sum_\lambda n_\lambda e_\lambda$ where $\{e_\lambda\}_{\lambda\in\Lambda}$ is a basis for G. Then n divides a only if n divides some $n_\lambda \neq 0 \in \mathbb{Z}$. This admits finitely many divisors n of a. $\square$

We now construct our H mentioned in the first paragraph. Given $G = \mathbb{Z}^\infty$ suppose G has basis $\{e_\lambda\}_{\lambda\in\Lambda}$. Then we can express each s_n as

$$s_n = (0, 0, \cdots, 0, 1, 0, \cdots) = \sum_\lambda m_{\lambda,n} e_\lambda.$$

Let $B(n)$ be the set of nonzero $m_{n,\lambda}$ and B the union of all $B(n)$. Then B is countable, and $H = \langle e_\lambda \rangle_{\lambda\in B}$ is a countable free subgroup of G.

We define a sequence $(a_n) \in \mathbb{Z}^\infty$ to be *multiplicative* if a_{n+1}/a_n is an integer that is not ± 1. We now prove that the set M of multiplicative sequences is uncountable.

PROOF. There are uncountably many sequences $(a_n) \in \mathbb{Z}^\infty$ such that $a_n > 1$. Then we can embed (a_n) in M by sending the sequence to

$$(a_1, a_2, \cdots) \to (a_1, a_1 a_2, \cdots, \prod_{i=1}^n a_i, \cdots).$$

Then M contains an uncountable subset, so M is uncountable. $\square$

Since $|M| > |H|$, choose $a = (a_n) \in M \setminus H$. Then for any n,

$$(0, 0, \cdots, a_n, a_{n+1}, \cdots) = (a_n) - a_1 s_1 - \cdots - a_n s_n = (a_n) + H.$$

Moreover, for any n, a_n divides $(0, 0, \cdots, a_n, a_{n+1}, \cdots)$, since (a_n) multiplicative. Thus a_n divides (a_n) in $\mathbb{Z}^\infty / H$ for every n. But since $\mathbb{Z}^\infty / H$ is free, the fact that (a_n) has infinitely many divisors is a contradiction.

□

We now show that if a free module M has two finite bases, the two bases have the same number of elements. This means we can associate an invariant to each free module: it's *rank*. If M does not have a finite basis we say it has infinite rank.

Theorem 0.9. *Let $\{u_1, \cdots, u_j\}$ and $\{v_1, \cdots, v_n\}$ be two bases for R. Then $j = n$.*

PROOF. The two bases induce an isomorphism ϕ between R^j and R^n. Let $\mathfrak{m}$ be a maximal ideal of R. Then by a previous remark, $R^j / \mathfrak{m} R^j$ is a k vector space, where k is the field $R/\mathfrak{m}$. Moreover, we can show that $R/\mathfrak{m}R^j = k^j$. So we have the following diagram:

$$\begin{tikzcd}
R^j \arrow[r, "\phi"] \arrow[d] & R^n \arrow[d] \\
k^j \arrow[r, "\bar{\phi}"] & k^n
\end{tikzcd}$$

□

Note that $\bar{\phi}$ is a well-defined homomorphism on the two vector spaces. For if two elements in R^j have components that differ by elements in $\mathfrak{m}$, then so will their image in R^k, since ϕ is R-linear. Thus ϕ will map two such elements to the same equivalence class in k^n. Thus $k = j$.

0.6 Finitely Generated Modules

We now weaken the condition of 'free-ness' to *finitely generated modules*. An R-module M is finitely generated if there exists a finite generating set. Notice that we do not require uniqueness or linear independence.

For example $\mathbb{Z}_3$ is finitely generated, even though it has non-unique generating sets, none of which are linearly independent.

Proposition 0.10. *M is a finitely generated R-module iff M is isomorphic to a quotient of R^n for some $n \in \mathbb{Z}_{>0}$.*

Proof. If $x_1, \cdots, x_n$ generate M, let $\phi : R^n \to M$ be defined by sending $\phi(a_1, \cdots, a_n) = a_1x_1 + \cdots a_nx_n$. This is surjective, so $M \simeq R^n/ker(\phi)$.

Conversely, suppose $\psi : M \to R^n/N$ is an isomorphism. If $\bar{e_i}$ is the image of e_i in R^n/N, let $\phi : R^n \to M$ be the surjective homomorphism that sends e_i to $\psi^{-1}(\bar{e_i})$. Then M is generated by the $\phi(e_i)$. □

We now state a form of Nakayama's Lemma:

Proposition 0.11. *If M is a finitely generated R-module and I an ideal of A contained in the Jacobson radical $J(R)$ of A, then $IM = M$ implies $M = 0$.*

Proof. First recall that the Jacobson Radical of a ring R, $J(R)$ is the intersection of all maximal ideals. We also characterize the radical as follows:

Lemma 0.12. *$x \in J(R)$ iff $1 - rx$ is a unit for all $r \in R$.*

Proof. Suppose $x \in J(R)$ but $1 - rx$ is not a unit. Then $1 - rx$ is in some maximal ideal, which must contain x. In which case 1 is in a maximal ideal.

Conversely if $x \notin M$, M maximal in R, then $\langle x \rangle + M = \langle 1 \rangle$, so we have $rx + m = 1$ for some $r \in R$ and $m \in M$. Then $1 - rx \in M$ and is not a unit. □

The proof of Nakayama's lemma now follows. Let $e_1, \cdots, e_n$ be a minimal generating set of M. Since $IM = M, e_n \in IM$. So there exists $x_i \in I$ such that

$$e_n = \sum x_i e_i, \qquad (1 - x_n)e_n = x_1e_1 + \cdots + x_{n-1}e_{n-1}.$$

But $x_n \in I \subseteq J(R)$, so $1 - x_n$ is a unit by the previous lemma. Thus e_n is generated by $e_1 + \cdots + e_{n-1}$, contradicting minimality of the generating set. □

While Nakayam's lemma seems innocuous, it has many applications in the theory of finitely generated modules and local rings. We demonstrate one such application here, by showing how to find a minimal generating set for a finitely generated module M.

Lemma 0.13. *If M finitely generated over R and $N \leq M$, and $M = N + J(R)M$, then $M = N$.*

Proof. Apply Nakayama to M/N. If $J(R)M/N = M/N$, then $M = N + J(R)M$. Then $M/N = 0$ iff $M = N$. □

Lemma 0.14. *If M is a finitely generated module over R and the images of elements $m_1, \cdots, m_n$ of M in $M/J(R)M$ generated $M/J(R)M$ as an R-module, then $m_1, \cdots, m_n$ generated M as an R-module.*

Proof. Let $N = \sum_i Rm_j$. Then since the $\{\bar{m}_i\}$ generate $M/J(R)M$, $M = \sum Rm_i + J(R)M$, which implies that $M = \sum_i Rm_i$. □

If $(R, \mathfrak{m}, k)$ is a local ring, then its Jacobson radical is $\mathfrak{m}$. The above lemma states that a basis of k can be lifted into a generating set for M.

Note that if N and M/N are finitely generated, so is M. However, just M may be finitely generated but have submodules that are not. The classical example is $M = \mathbb{Z}[\{x_i\}_{i=1}^{\infty}]$, the polynomial ring in countably many variables.

This motivates the importance of studying modules whose submodules are also finitely generated: Noetherian modules.

0.7 Noetherian Modules

A Noetherian module is a module whose submodules are all finitely generated. A ring R is Noetherian if it is a Noetherian module over itself. That is, every ideal of R is finitely generated. We now prove the following characterization for Noetherian rings:

Proposition 0.15. *Let M be an R-module. Then the following are equivalent:*

a) Every non-empty set of submodules in M has a maximal element.

b) Every ascending chain of submodules in M terminates.

c) Every submodule in M is finitely generated.

Proof. *a)* $\leftrightarrow$ *b)*. If (M_n) is an ascending chain of submodules, then it has a maximal element, M_N, at which the sequence terminates. If some collection $\{M_\alpha\}_{\alpha \in \mathcal{A}}$ of submodules does not have a maximal element, we can construct a non-terminating chain.

a) $\rightarrow$ *c)*. Let N be a submodule of M, and S the set of all finitely generated submodules of N. Since $0 \in S$, S is nonempty and thus has a maximal element, N_0, by *a)*. It suffices to show $N_0 = N$. If not, then the submodule $N_0 + \langle x \rangle$ is finitely generated and strictly contains N_0, for any $x \notin N_0$. This contradicts maximality, so $N = N_0 \in S$.

c) $\rightarrow$ *a)*. Let $M_1 \subseteq M_2 \subseteq \cdots$ be an ascending chain of submodules of M. Then their union is also a submodule of M, which then admits a finite list of generators $x_1, \cdots, x_n$. Let M_{max} be the element of minimum index containing all the generators. Then M_{max} is where this chain terminates. □

We also have the descending chain condition. A module that satisfies the descending chain condition is called Artinian. Artinian rings, especially, are simple. We give a few examples of why without proof.

Proposition 0.16. *a) Every prime ideal of an Artin ring is maximal*

b) An Artin ring only finitely many maximal ideals.

c) An Artin ring is Noetherian.

0.8 Length of a Module

We now introdue an invariant for general modules. A *composition series* of a module is a sequence of submodules of the form

$$0 = M_0 \subsetneq M_1 \subsetneq \cdots \subsetneq M_n = M$$

such that M_i/M_{i-1} has no nontrivial submodules.

We define the *length* of M $\ell(M)$ as the minimum length of a composition series of M. We now prove the following:

Proposition 0.17. *Any two composition series of an R-module M have the same length. Moreover given any series in M, we can extend it to a composition series.*

Proof. Let M have a composition series of length n. So $\ell(M) \leq n$. We first claim that if $N \subsetneq M$, then $\ell(N) < \ell(M)$. Let $\ell(M) = \ell \leq n$. Then there exists a composition series $M = M_\ell \supsetneq \cdots \supsetneq M_0 = \{0\}$. This induces the sequence

$$N = N \cap M_\ell \supsetneq \cdots \supsetneq N \cap M_0 = \{0\}.$$

We must show the above sequence is a composition series.

By the second isomorphism theorem,

$$(N \cap M_i)/(N \cap M_{i-1}) \simeq ((N \cap M_i) + M_{i-1})/M_{i-1}$$

is a submodule of M_i/M_{i-1}. This is sufficient to show the above quotient is simple, and we have a composition series.

Now we show that the induced series on N must have a redundant module. Suppose not. Then $(N \cap M_i) + M_{i-1} \simeq M_i$. We can then use induction to show that $N \cap M_i \simeq M_i$ for all N. In particular, $N = M$, a contradiction.

Now if $M = M_k \supsetneq \cdots \supsetneq M_0 = \{0\}$ is another composition series of M, then

$$\ell = \ell(M) > \ell(M_{k-1}) > \cdots > \ell(M_0),$$

which shows that $\ell \geq k$. But by the minimality definition of length, $\ell \leq k$. This gives us equality. $\square$

If M does not have a composition series of finite length, we say $\ell(M) = \infty$.

Example 0.18.
- The composition series of an Abelian group G is a composition series of G as a $\mathbb{Z}$-module.
- If V is a vector space, $\ell_k(V) = dim(V)$.
- $\mathbb{Z}[x_1, x_2, \cdots]$ has infintie length as a $\mathbb{Z}$ module.
- $\mathbb{Z}$ is finitely generated as a $\mathbb{Z}$-module, but also has infinite length.

So being finitely generated is not enough to have finite length. We now consider when a module does have finite length:

Proposition 0.19. *An R-module M has finite length iff it is both Noetherian and Artinian.*

PROOF. If $\ell(M) = n$, then any ascending/descending chain terminates after at most n elements.

If M is both Noetherian and Artinian then the set of proper submodules has a maximal element (unless $M = 0$ in which case we are done) M_1. Similarly the set of proper submodules of M_1 is either empty, or has a maximal element M_2. We continue this decreasing sequence until it terminates, since the module is Artinian. □

In particular, the Artinian rings are exactly the rings that have finite length.

0.9 Exact Sequences

Another tool we use to study modules is the concept of an *exact sequence*. Consider a sequence of R-module homomorphisms $\{d_i\}$ of R-modules $\{M_i\}$ of the form

$$\cdots \xrightarrow{d_{n+2}} M_{n+1} \xrightarrow{d_{n+1}} M_n \xrightarrow{d_n} M_{n-1} \xrightarrow{d_{n-1}} \cdots \tag{0.1}$$

such that $d_i d_{i+1} = 0$. That is, $Im(d_{i+1}) \subseteq ker(d_i)$. We call the above sequence a *complex*. The d_n are called differentials, and the image of the differential d_n are called n-boundaries. If equality holds for some n, that is $Im(d_{i+1}) = ker(d_i)$, the sequence is *exact* at M_i. If a complex is exact at every module, it is an *exact sequence*.

Proposition 0.20. *The sequences:*

$$0 \longrightarrow M' \xrightarrow{f} M \textit{ is exact iff } f \textit{ is injective}$$

$$M \xrightarrow{g} M'' \longrightarrow 0 \textit{ is exact iff } g \textit{ is surjective}$$

$$0 \longrightarrow M' \xrightarrow{f} M \xrightarrow{g} M'' \longrightarrow 0$$

is exact iff f is injective, g is surjective, and $M/M' \simeq M''$.

Proposition 0.21. *The sequence*

$$M' \xrightarrow{\alpha} M \xrightarrow{\beta} M'' \longrightarrow 0 \tag{0.2}$$

is exact if and only if

$$0 \longrightarrow Hom(M'', N) \xrightarrow{\bar{\beta}} Hom(M, N) \xrightarrow{\bar{\alpha}} Hom(M', N) \tag{0.3}$$

is exact for any R-module N.

Proof. For brevity, we show exactness at the center module. Suppose (1) is exact, and consider $f \in Im(\beta)$. Then $\bar{\alpha}(\bar{\beta}(f)) = f \circ \beta \circ \alpha = 0$, using the fact that $Im(\alpha) \subset \ker(\beta)$.

For the reverse containment, given some $f \in ker(\bar{\alpha})$, define $g : M'' \to N$ by setting $g(m'') = f(\beta^{-1}(m''))$. The pre-image is always non-empty since β is surjective. And given $m, n \in M$ such that $\beta(m) = \beta(n) = m''$, $m - n \in ker(\beta) = Im(\alpha)$, so $f(m-n) = 0$, by our assumption that $f \circ \alpha = 0$. Then g is well-defined, and $g \circ \beta = f$. That is, $f \in Im(\bar{\beta})$. Thus $ker(\bar{\alpha}) = Im(\bar{\beta})$.

Conversely, if (2) is exact, $\beta \circ \alpha = \bar{\alpha}(\bar{\beta}(id) = 0$, by exactness at (2).

Let $N = M/\alpha(M')$ and π the canonical projection from M. Then $\pi \in ker(\bar{\alpha}) = Im(\bar{\beta})$, so there exists some ψ such that $\phi = \psi \circ \beta$. Then $Im(\alpha) = ker(\phi) \supseteq ker(\beta)$. □

Proposition 0.22. *Let*

$$0 \longrightarrow M' \xrightarrow{\alpha} M \xrightarrow{\beta} M'' \longrightarrow 0$$

be an exact sequence of R-modules. Then M is Noetherian (Artinian) iff M' and M'' are Noetherian (Artinian).

Proof. If $L'_1 \subseteq L'_2 \subseteq \cdots$ is an ascending chain in M', then $\alpha(L'_1) \subseteq \alpha(L'_2) \subseteq \cdots$ is an ascending chain in M that terminates at some $\alpha(L'_n)$. By injectivity of α, we have termination of the original sequence in M'. Similarly if $L''_1 \subseteq L''_2 \subseteq \cdots$ in M'', their pre-image forms another ascending chain in M. By surjectivity of β, this termination is preserved when we send it back.

Conversely, if (L_n) is a non-terminating chain in M', then by injectivity of α the chain $(\alpha^{-1}(L_n))$ does not terminate either. □

We can also use exact sequences to determine the length of a module.

Proposition 0.23. *If*

$$0 \longrightarrow M' \xrightarrow{\alpha} M \xrightarrow{\beta} M'' \longrightarrow 0$$

is an exact sequence, then $\ell(M') + \ell(M'') = \ell(M)$.

Proof. Let (L'_i) and (L''_i) be composition series in M' and M'' respectively. If either are infinite, then M is not Noetherian by the previous theorem, and $\ell(M)$ is infinite. In this case we are done. Suppose $L'_n = M'$ and $L''_m = M''$. First note that

$$0 \subseteq \alpha(L'_1) \subseteq \cdots \subseteq \alpha(L'_n) = \beta^{-1}(L''_0) \subseteq \beta^{-1}(L''_1) \subseteq \cdots \subseteq \beta^{-1}(M'') = M$$

is a series in M. Note that the equality follows directly from exactness. For the above equality is equivalent to saying $Im(\alpha) = ker(\beta)$. Furthermore, note that there are no nontrivial modules between each module in the sequence. There are none between the $\{\alpha(L'_i)\}$ otherwise taking pre-images(with injectivity of α) would contradict simplicity in M'. There are none between the $\{\beta^{-1}(L''_i)\}$ or else taking images (with surjectivity) would contradicit simplicity in M''. Thus we have constructed a composition series of M of length $n+m$. The proposition follows. $\square$

Corollary 0.24. *If N is a submodule of M, then $\ell(N) + \ell(M/N) = \ell(M)$. In particular, if $\phi : M \to M'$ is an R-module homomorphism, then*

$$\ell(ker(\phi)) + \ell(Im(\phi)) = \ell(M).$$

PROOF. Note that given any submodule in N, the sequence

$$0 \longrightarrow N \longrightarrow M \longrightarrow M/N \longrightarrow 0$$

is exact. Then use additivity of length. $\square$