A Non-slick Proof of the Jordan Hölder Theorem

E.L. Lady

This proof is an attempt to approximate the actual thinking process that one goes through in finding a proof before one realizes how simple the theorem really is.

To start with, though, we motivate the Jordan-Hölder Theorem by starting with the idea of **dimension** for vector spaces.

The concept of dimension for vector spaces has the following properties:

(1) If $V = \{0\}$ then $\dim V = 0$.
(2) If W is a proper subspace of V, then $\dim W < \dim V$.
(3) If $V \neq \{0\}$, then there exists a one-dimensional subspace of V.
(4) $\dim(U \oplus W) = \dim U + \dim W$.
(5) If $\bigcup_I W_i$ is a *chain* of subspaces of a vector space, then $\dim \bigcup W_i = \sup\{\dim W_i\}$.

Now we want to use properties (1) through (4) as a model for defining an analogue of dimension, which we will call **length**, for *certain* modules over a ring. These modules will be the analogue of finite-dimensional vector spaces, and will have very similar properties.

The axioms for length will be as follows.

Axioms for Length. Let R be a fixed ring and let M and N denote R-modules. Whenever $\operatorname{length} M$ is defined, it is a cardinal number.

(1) If $M = \{0\}$, then $\operatorname{length} M$ is defined and $\operatorname{length} M = 0$.
(2) If $\operatorname{length} M$ is defined and N is a proper submodule of M, then $\operatorname{length} N$ is defined. Furthermore, if $\operatorname{length} M$ is finite then $\operatorname{length} N < \operatorname{length} M$.
(3) For $M \neq 0$, $\operatorname{length} M = 1$ if and only if M has no proper non-trivial submodules. (In this case, M is called a **simple** module.)
(4) If N is a submodule of M, then $\operatorname{length} M$ is defined if and only if $\operatorname{length} N$ and $\operatorname{length} M/N$ are both defined and in this case, $\operatorname{length} M = \operatorname{length} N + \operatorname{length} M/N$.

Note that it was necessary to modify Axioms (3) and (4) from the vector-space case. This is because every vector space contains a simple (i. e. one-dimensional) subspace, but many modules do not contain a simple submodule. And secondly, a subspace of a vector space is always a direct summand, but a submodule of a module need not be a direct summand.

We will be interested only in modules having finite length, leaving open the question of whether it is possible to define length in such a way that some modules have infinite length.

The axioms we have given enable us to prove that many familiar properties of finite-dimensional vector spaces will hold for modules with finite length. For instance,

Theorem. Let M be an R-module with finite length and let φ be an endomorphism of M. The the following conditions are equivalent:

(1) φ is an isomorphism from M onto itself.
(2) φ is a monomorphism.
(3) φ is surjective.
(4) There exists an endomorphism $\psi\colon M \to M$ such that $\psi\varphi = 1_M$.
(5) There exists an endomorphism ψ of M such that $\varphi\psi = 1_M$.

Partial Proof: Let φ be a monomorphism from M into M. Then $\varphi(M) \approx M$. Therefore $\operatorname{length}\varphi(M) = \operatorname{length} M$. (This may not be self-evident at this point, but it will become clear later.) But since $\varphi(M) \subseteq M$ it then follows from Axiom (2) that $\varphi(M) = M$. Thus φ is surjective.

Conversely, suppose that φ is surjective. Then $\varphi(M) = M$, so that $\operatorname{length}\varphi(M) = \operatorname{length} M$. But by Axiom (4), $\operatorname{length} M = \operatorname{length}\varphi(M) + \operatorname{length}\operatorname{Ker}\varphi$. Therefore, $\operatorname{length}\operatorname{Ker}\varphi = 0$ (since the lengths are all finite), which implies that $\operatorname{Ker}\varphi = 0$ (otherwise we get a contradiction to Axiom (2)). Therefore φ is monic. ☑

Exercises. (1) Finish the proof of the theorem above.

(2) Prove that the implication (4)⇒(2) is true for all modules, whether or not they have finite length. Likewise prove that (5)⇒ (3) for all modules.

(3) Prove that assertion (2) does not imply assertion (3) for the case when $M = \mathbb{Z}$, considered as a $\mathbb{Z}$-module.

(4) Prove that assertion (3) does not imply assertion (2) for the $\mathbb{Z}$-module $M = \mathbb{Q}/\mathbb{Z}$.

(5) Prove that if M is the $\mathbb{Z}$-module obtained by taking the direct sum of a countably infinite number of copies of $\mathbb{Z}$,

$$M = \bigoplus_{1}^{\infty} \mathbb{Z},$$

then for M, assertion (2) does not imply assertion (3) nor conversely.

The axioms given above are actually strong enough to force the definition of length on us, at least in the finite length case.

Theorem. For $\ell < \infty$, an R-module M has length ℓ if and only if there is a chain of submodules

$$0 = M_0 \subsetneq M_1 \subsetneq \ldots \subsetneq M_{\ell-1} \subsetneq M_\ell = M$$

such that each M_i is a maximal proper submodule of M_{i+1}.

PROOF: ($\Rightarrow$): If M_i is a maximal submodule of M_{i+1}, then M_{i+1}/M_i is a simple module and therefore by Axiom (3) $\text{length}\, M_{i+1}/M_i$ is defined and $\text{length}\, M_{i+1}/M_i = 1$. Therefore, by Axiom (4), if $\text{length}\, M_i$ is defined then $\text{length}\, M_{i+1}$ is also defined and $\text{length}\, M_{i+1} = \text{length}\, M_i + 1$. This enables us to start at the bottom of the chain and inductively work our way up, showing that $\text{length}\, M_i = i$ for each i, and in particular, $\text{length}\, M = \ell$.

($\Leftarrow$): If $M \neq 0$ then $0 \subsetneq M$, and so by Axiom (2), if $\text{length}\, M$ is defined then $\text{length}\, M > 0$.

Now if $\text{length}\, M = 1$, then M must be a simple module, otherwise M has a proper non-trivial submodule N and $0 < \text{length}\, N < \text{length}\, M$, a contradiction. This shows that the theorem is valid for modules of length 1.

Now suppose inductively that for a certain $\ell > 1$, whenever the length of a module is defined and less then ℓ, then there exists a chain of the prescribed type. Now suppose that $\text{length}\, M$ is defined and $\text{length}\, M = \ell$.

Since $\ell > 1$, $M \neq 0$ and M is not simple. Therefore M has a proper non-trivial submodule N. By Axiom (2), $\text{length}\, N < \ell$. Say $\text{length}\, N = r$. Then by Axiom (4), $0 \neq \text{length}\, M/N = \ell - r < \ell$. Therefore we may apply the induction hypothesis to N and M/N to get chains

$$0 \subsetneq N_1 \subsetneq \ldots \subsetneq N_{r-1} \subsetneq N_r = N$$

and

$$0 = \frac{N}{N} \subsetneq \frac{M_{\ell-r+1}}{N} \subsetneq \ldots \subsetneq \frac{M_{\ell-1}}{N} \subsetneq \frac{M_\ell}{N} = \frac{M}{N}$$

with the desired property. Here, in the second chain we have used the fact that every submodule of M/N has the form X/N, where X is a submodule of M containing N. We have also chosen to start the numbering of the second chain with the subscript $\ell - r + 1$. Since the length of the chain is $\ell - r$ (as we saw by applying the induction hypothesis to M/N), arithmetic shows that the final subscript will be ℓ, as indicated.

Piecing these two chains together, we see that for a module M with $\operatorname{length} M = \ell$, there will in fact be a chain

$$0 \subsetneq N_1 \subsetneq \ldots \subsetneq N_{r-1} \subsetneq N = M_{\ell-r} \subsetneq M_{\ell-r+1} \subsetneq \cdots \subseteq M_{\ell-1} \subsetneq M,$$

as required. ☑

This theorem shows that the axioms we have chosen for length force us to define $\operatorname{length} M$, in the finite case, as the length(!) of a maximal chain of submodules of M.

There is one slight glitch, however. It is conceivable that there might some module over some ring having two maximal chains of submodules with different lengths. If this happens, then the concept of length is simply undefinable.

However the Jordan-Hölder Theorem assures us that we are safe from such a catastrophe.

Jordan-Hólder Theorem. Suppose that M is an R-module and that there exists a chain

$$0 = M_0 \subsetneq M_1 \subsetneq \ldots \subsetneq M_\ell = M$$

where each M_i/M_{i-1} is a simple R-module. Then any other chain of this sort will have the same length ℓ, and have the same set of simple quotient modules M_i/M_{i-1}, although not necessarily in the same order. Furthermore, irrespective of the condition on the quotient modules, there does not exist any strictly ascending chain of submodules of M with length greater than ℓ. (In particular, there cannot exist an infinite ascending chain.)

Note. Saying that each M_i/M_{i-1} is a simple module is just another way of saying that there do no exist any submodules strictly between M_{i-1} and M_i. (WHY?)

Set-up of Proof. We need to consider two chains

$$0 \subsetneq M_1 \subsetneq M_2 \subsetneq \ldots \subsetneq M_\ell = M$$
$$0 \subsetneq N_1 \subsetneq N_2 \subsetneq \ldots \subsetneq N_k = M$$

where the quotients are all simple modules. We must then prove that necessarily $k = \ell$ and furthermore the family of simple quotients M_i/M_{i-1} is the same as the family N_i/N_{i-1} (counting multiplicities).

Suppose inductively that the theorem is true for all modules for which there exists a chain of length smaller than ℓ.

Case 1. Now if $M_i = N_j$ for some i, j such that $0 \neq M_i = N_j \neq M$, then the induction hypothesis applied to M_i shows that $i = j$. Furthermore, the induction hypothesis can be applied to $M/M_i = M/N_i$ to show that $k - i = \ell - i$. This is because of the following standard fact.

Fact. If K is a submodule of an R-module M, then the submodules of M/K are precisely those of the form X/K, where $K \subseteq X \subseteq M$, and furthermore distinct submodules X yield distinct submodules of M/K.

Case 2. If Case 1 does not apply, suppose that there exist N_i and M_j such that

$$0 \neq N_i \subseteq M_j \neq M.$$

It follows that $N_1 \subseteq M_{\ell-1}$ (WHY?). Now, if possible, insert additional modules called L_i between $N_1 \subseteq M_{\ell-1}$. By the induction hypothesis applied to $M_{\ell-1}$, this cannot be done indefinitely, and eventually we get a series

$$0 \subsetneq N_1 \subseteq L_2 \subsetneq \ldots \subsetneq L_s \subsetneq M_{\ell-1}$$

where all the quotient modules are simple. By the induction hypothesis (applied to $M_{\ell-1}$), this chain must have length $\ell - 1$ (so that $s = \ell - 2$), and we get the same quotient modules for the two chains. Now we can apply Case 1 to the two chains

$$0 \subsetneq N_1 \subsetneq L_2 \subsetneq \ldots \subsetneq L_{\ell-2} \subsetneq M_{\ell-1} \subsetneq M$$
$$0 \subsetneq N_1 \subsetneq N_2 \subsetneq \ldots \subsetneq N_{k-2} \subsetneq N_{k-1} \subsetneq M$$

(since they have the module N_1 in common) to see that $k = \ell$ and that the theorem holds in this case.

Case 3. The only case left is that where $N_1 \not\subseteq M_{\ell-1}$. But this is actually also a special case. Note that by the assumption made on the chains, N_1 is a simple module. But $N_1 \cap M_{\ell-1} \subseteq N_1$, so if $N_1 \not\subseteq M_{\ell-1}$ it follows that $N_1 \cap M_{\ell-1} = 0$.

Notice also that if $N_1 \not\subseteq M_{\ell-1}$ then $M_{\ell-1} \subsetneq N_1 + M_{\ell-1}$. But $M_{\ell-1}$ is by assumption a maximal proper submodule of M. Therefore $N_1 + M_{\ell-1} = M$, and since we have already seen that $N_1 \cap M_{\ell-1} = 0$, it follows that $M = N_1 \oplus M_{\ell-1}$. Therefore $M/N_1 \approx M_{\ell-1}$. Now there is a strictly ascending (WHY?) chain

$$0 = N_1/N_1 \subsetneq N_2/N_1 \subsetneq \ldots \subsetneq N_k/N_1 = N/N_1$$

of submodules of N/N_1 with length $k - 1$, and the isomorphism $M/N_1 \approx M_{\ell-1}$ maps this to a strictly increasing chain of submodules of $M_{\ell-1}$. By the induction hypothesis, these two chains must have the same length: $k - 1 = \ell - 1$. Moreover, there is an isomorphism between the quotient modules in each case (although not necessarily in the same order).

The proof in this final case now follows easily. ☑

Many of the most important application of linear algebra involve finite-dimensional vector spaces. But it turns out that, over most rings which are not fields, modules with finite length are fairly uncommon. For instance, if we consider the ring $\mathbb{Z}$ as a module over itself, then certainly this seems a rather small module, by the standards of module theory. And yet $\mathbb{Z}$ does not have finite length as a $\mathbb{Z}$-module.

In fact, there is a strictly decreasing chain of submodules of $\mathbb{Z}$ (i. e. ideals) as follows:

$$\mathbb{Z} \supsetneq 2\mathbb{Z} \supsetneq 4\mathbb{Z} \supsetneq 8\mathbb{Z} \supsetneq 16Z \supsetneq 32\mathbb{Z} \supsetneq \ldots .$$

Now if $\mathbb{Z}$ were to have finite length, then the length of each ideal in this chain would be strictly smaller than the length of the one preceding it. But this would yield an infinite strictly descending chain of natural numbers, which is impossible. (The natural numbers are well ordered.)

Later on, we will see that (using terms yet to be defined) a module over a commutative noetherian ring has finite length if and only if it is finitely generated and all its associated prime ideals are maximal ideals. (To get some idea of what this means, consider the example of an abelian group, thought of as a $\mathbb{Z}$-module. The associated primes for an abelian group G are the ideals generated by those prime numbers p such that G has an element of order p, and also the zero ideal in the case that G has non-zero elements of infinite order. This is not the most enlightening possible example, since all the non-zero prime ideals of $\mathbb{Z}$ are maximal ideals, however it is the only one simple enough to give at this point. The result stated above implies that the abelian groups having finite length as $\mathbb{Z}$-modules are precisely those groups with finite order.)

Since modules with finite length are so rare, we need to search out less stringent finiteness conditions which, when they exist for a module, will guarantee at least some of the nice behavior known for finite-dimensional vector spaces.