A proof of Krull-Schmidt’s theorem for modules

M. G. Mahmoudi

November 18, 2012

The aim of this note is to provide a proof of Krull-Schmidt theorem for modules. Here $R$ denotes a ring with unity.

**Definition 1.** An $R$-module $M$ is said to be indecomposable if it satisfies the following equivalent conditions:

1. $M$ can not be decomposed as a direct sum of two nonzero modules.
2. The only idempotents of the endomorphism ring of $M$ are 0 and 1.

For the proof of the equivalence of (1) and (2), it suffices to observe that for every idempotent $e \in \text{End}(M)$, the sum $M = e(M) + (\text{id} - e)(M)$ is direct.

**Theorem 2.** (Fitting’s lemma) Let $M$ be an $R$-module and let $\varphi : M \to M$ be an $R$-module homomorphism.

(a) If $M$ is noetherian then there exists a positive integer $n$ such that $\ker \varphi^n \cap \text{im} \varphi^n = 0$.
(b) If $M$ is artinian then there exists a positive integer $n$ such that $M = \ker \varphi^n + \text{im} \varphi^n$.
(c) If $M$ is a module of finite length (i.e., both artinan and noetherian), then there exists a positive integer $n$ such that $M = \ker \varphi^n \oplus \text{im} \varphi^n$.

**Proof.** (a) We have $\ker \varphi \subset \ker \varphi^2 \subset \cdots$. As $M$ is noetherian, there exists a positive integer $n$ such that $\ker \varphi^n = \ker \varphi^{n+1} = \cdots$. We claim that $\ker \varphi^n \cap \text{im} \varphi^n = 0$. If $x \in \ker \varphi^n \cap \text{im} \varphi^n$ then there exists $y \in M$ such that $x = \varphi^n(y)$. It follows that $\varphi^{2n}(y) = \varphi^n(x) = 0$. So $y \in \ker \varphi^{2n} = \ker \varphi^n$. Thus $x = \varphi^n(y) = 0$.
(b) We have $\text{im} \varphi \supset \text{im} \varphi^2 \supset \cdots$. As $M$ is noetherian, there exists a positive integer $n$ such that $\text{im} \varphi^n = \text{im} \varphi^{n+1} = \cdots$. We claim that $M = \ker \varphi^n + \text{im} \varphi^n$.

To see this, let $x \in M$ be an arbitrary element. As $\text{im} \varphi^n = \text{im} \varphi^{2n}$, there exists an element $y \in M$ such that $\varphi^n(x) = \varphi^{2n}(y)$. Write $x = (x - \varphi^n(y)) + \varphi^n(y)$. It suffices to show that the term $x - \varphi^n(y)$ is in $\ker \varphi^n$. In fact we have $\varphi^n(x - \varphi^n(y)) = \varphi^n(x) - \varphi^{2n}(y) = 0$.

The assertion (c) follows from (a) and (b).

**Corollary 3.** Let $M$ be an indecomposable $R$-module of finite length then every endomorphism of $M$ is either nilpotent or isomorphism. In particular the set of non-invertible elements of $\text{End}(M)$ is closed under addition.

**Proof.** Let $f \in \text{End}(M)$. By Fitting’s lemma, there exists a positive integer $n$ such that $M \simeq \ker \varphi^n \oplus \text{im} \varphi^n$. As $M$ is indecomposable, we either have $\ker \varphi^n = 0$ and $\text{im} \varphi^n = M$ or $\ker \varphi^n = M$ and $\text{im} \varphi^n = 0$. In the former case, $\varphi$ is an isomorphism and in the latter case $\varphi^n = 0$ and $\varphi$ is nilpotent.

For the second assertion, let $f$ and $g$ be two non-invertible elements of $\text{End}(M)$.
We must show that $h := f + g$ is also a non-invertible element of $End(M)$. Otherwise $h$ is invertible, so we obtain $id = h^{-1}f + h^{-1}g$. As $f$ is non-invertible, so is $h^{-1}f$ and by previous Corollary, $h^{-1}f$ is nilpotent and so $id - h^{-1}f = h^{-1}g$ is invertible, so is $g$, contradiction.

**Lemma 4.** Let $M$ be a nonzero $R$-module and let $N$ be an indecomposable $R$-module. Suppose that $f : M \to N$ and $g : N \to M$ be two $R$-module homomorphisms such that $g \circ f : M \to M$ is an isomorphism. Then $f$ and $g$ are isomorphism as well.

**Proof.** As $g \circ f$ is isomorphism we obtain that $g$ is surjective and $f$ is injective. Consider the exact sequence $0 \to M \to N \to \ker f \to 0$ and $0 \to \ker g \to N \to M \to 0$. As $g \circ f$ is isomorphism, these sequence split. So $N \simeq M \oplus \ker f \simeq \ker g \oplus M$. As $N$ is indecomposable, it follows that $\ker f = 0$ and $\ker g = 0$. Thus $f$ is surjective and $g$ is injective.

**Theorem 5.** (Krull-Schmidt) Let $M$ be an $R$-module and let $M \simeq U_1 \oplus \cdots \oplus U_m \simeq V_1 \oplus \cdots \oplus V_n$ be two decomposition of $M$ where $U_i$’s and $V_j$’s are indecomposable $R$-modules. Then $m = n$ and after a rearrangement of indices we have $U_i \simeq V_i$ for every $i$.

**Proof.** Let $\varphi : U_1 \oplus \cdots \oplus U_m \to V_1 \oplus \cdots \oplus V_n$ be an $R$-module isomorphism. We prove the result by induction on $m + n$. If $m + n = 2$ then $m = n = 1$ and the conclusion is immediate. Let $\pi_i : U_1 \oplus \cdots \oplus U_m \to U_i$ and $\pi'_j : V_1 \oplus \cdots \oplus V_n \to V_j$ be the canonical projections and let $\iota_i : U_i \to U_1 \oplus \cdots \oplus U_m$ and $\iota'_j : V_j \to V_1 \oplus \cdots \oplus V_n$ be the canonical injections.

Consider the endomorphism $\rho_{ij}$ of $U_i$ which is the composition of $\pi'_j \circ \varphi \circ \iota_i : U_i \to V_j$ and $\pi_i \circ \varphi^{-1} \circ \iota'_j : V_j \to U_i$.

If there exist two indices $i$ and $j$ such that $\rho_{ij}$ is an isomorphism (say $i = j = 1$) then we have an isomorphism $\pi'_1 \circ \varphi \circ \iota_1 : U_1 \simeq V_1$ as well. It follows that $\varphi' := (\oplus_{r=2}^m \pi'_r) \circ \varphi \circ (\oplus_{s=2}^n \iota'_s) : (\oplus_{r=2}^m U_r) \to (\oplus_{s=2}^n V_s)$ is an isomorphism. For the injectivity: suppose that $(0, u_2, \cdots, u_m)$ is in the kernel of this maps. So $\pi'_s(\varphi(0, u_2, \cdots, u_m)) = 0$ for $r = 2, \cdots, n$. So we have $\varphi(0, u_2, \cdots, u_m) = (v_1, 0, \cdots, 0)$. It follows that $\varphi(0, u_2, \cdots, u_m) = \iota'_1(v_1)$. By applying the map $\pi_1 \circ \varphi^{-1}$ on both sides we get $0 = \pi_1 \circ \varphi^{-1} \circ \iota'_1(v_1)$. As $\varphi \circ \varphi^{-1} \circ \iota'_1$ is isomorphism we obtain $v_1 = 0$ so $\varphi(0, u_2, \cdots, u_m) = (0, 0, \cdots, 0)$ and so $(u_2, \cdots, u_m) = (0, \cdots, 0)$. For the surjectivity: as $\varphi'$ is injective so $\ell(\oplus_{r=2}^m U_r) = \ell(\varphi'(\oplus_{r=2}^m U_r))$. On the other hand $\ell(\oplus_{r=2}^m U_r) = \ell(\oplus_{s=2}^n V_s)$ it follows that $\varphi'(\oplus_{r=2}^m U_r) = \oplus_{s=2}^n V_s$ so $\varphi'$ is surjective.

We may now use the induction hypothesis to concludes the result.

If for every $j$, $\rho_{ij}$ is not isomorphism then by previous Corollary $\rho_{ij}$ is nilpotent and so $\sum_{j=1}^m \rho_{ij}$ is nilpotent as well. But $\sum_{j=1}^m \rho_{ij} = id_{U_i}$, contradiction.

M. G. MAHMoudi,
DEPARTMENT OF MATHEMATICAL SCIENCES, SHARIF UNIVERSITY OF TECHNOLOGY, P. O. BOX 11155-9415, TEHRAN, IRAN.

E-mail address: mmahmoudi@sharif.ir