Fitting's lemma

Canonical name	FittingsLemma
Date of creation	2013-03-22 17:29:26
Last modified on	2013-03-22 17:29:26
Owner	CWoo (3771)
Last modified by	CWoo (3771)
Numerical id	9
Author	CWoo (3771)
Entry type	Theorem
Classification	msc 16D10
Classification	msc 16S50
Classification	msc 13C15
Synonym	Fitting lemma
Synonym	Fitting decomposition theorem
Defines	Fitting's decomposition theorem

Theorem 1 (Fitting Decomposition Theorem)**.** *Let R be a ring, and M a finite-length module over R. Then for any $\phi \in \mathrm{End}(M)$, the endomorphism ring of M, there is a positive integer n such that*

$$M = \ker(\phi^n) \oplus \mathrm{im}(\phi^n).$$

Proof. Given $\phi \in \mathrm{End}(M)$, it is clear that $\ker(\phi^i) \subseteq \ker(\phi^{i+1})$ and $\mathrm{im}(\phi^i) \supseteq \mathrm{im}(\phi^{i+1})$ for any positive integer i. Therefore, we have an ascending chain of submodules

$$\ker(\phi) \subseteq \cdots \subseteq \ker(\phi^i) \subseteq \ker(\phi^{i+1}) \subseteq \cdots,$$

and a descending chain of submodules

$$\mathrm{im}(\phi) \supseteq \cdots \supseteq \mathrm{im}(\phi^i) \supseteq \mathrm{im}(\phi^{i+1}) \supseteq \cdots.$$

Both chains must be finite, since M has finite length. Therefore, we can find a positive integer n such that

$$\begin{cases} \ker(\phi^n) = \ker(\phi^{n+1}) = \cdots, \text{ and} \\ \mathrm{im}(\phi^n) = \mathrm{im}(\phi^{n+1}) = \cdots. \end{cases}$$

If $u \in M$, then $\phi^n(u) \in \mathrm{im}(\phi^n) = \mathrm{im}(\phi^{2n})$. Therefore, $\phi^n(u) = \phi^{2n}(v)$ for some $v \in M$. Write $u = (u - \phi^n(v)) + \phi^n(v)$. Applying the ϕ^n to the first term, we get $\phi^n(u - \phi^n(v)) = \phi^n(u) - \phi^{2n}(v) = 0$, so it is in $\ker(\phi^n)$. The second term is clearly in $\mathrm{im}(\phi^n)$. So

$$M = \ker(\phi^n) + \mathrm{im}(\phi^n).$$

Furthermore, if $u \in \ker(\phi^n) \cap \mathrm{im}(\phi^n)$, then $u = \phi^n(v)$ for some $v \in M$. Since $\phi^{2n}(v) = \phi^n(u) = 0$, $v \in \ker(\phi^{2n}) = \ker(\phi^n)$. Therefore, $u = \phi^n(v) = 0$. This shows that we can replace $+$ in the equation above by $\oplus$, proving the theorem. $\square$

Stated differently, the theorem says that, given an endomorphism ϕ on M, M can be decomposed into two submodules M_1 and M_2, such that ϕ restricted to M_1 is nilpotent, and ϕ restricted to M_2 is an isomorphism.

A direct consequence of this decomposition property is the famous Fitting Lemma:

Corollary 1 (Fitting Lemma)**.** *In the theorem above, ϕ is either nilpotent ($\phi^n = 0$ for some n) or an automorphism iff M is indecomposable.*

Proof. Suppose first that M is indecomposable. Then either $\ker(\phi^n) = 0$ or $\operatorname{im}(\phi^n) = 0$. If $n = 1$, then the lemma is proved. Suppose $n > 1$. In the former case, any $u \in M$ is the image of some v under ϕ^n, so $u = \phi(\phi^{n-1}(v))$ and therefore ϕ is onto. If $\phi(u) = 0$, then $\phi^n(u) = \phi^{n-1}(\phi(u)) = 0$, so $u = 0$. This means u is an automorphism. In the latter case, $\phi^n(u) = 0$ for any $u \in M$, so ϕ is nilpotent.

Now suppose M is not indecomposable. Then writing $M = M_1 \oplus M_2$, where M_1 and M_2 as proper submodules of M, we can define $\phi \in \operatorname{End}(M)$ such that ϕ is the identity on M_1 and 0 on M_2 (ϕ is a projection of M onto M_1). Since both M_1 and M_2 are proper, ϕ is neither an automorphism nor nilpotent. $\square$

Remark. Another way of stating Fitting Lemma is to say that $\operatorname{End}(M)$ is a local ring iff the finite-length module M is indecomposable. The (unique) maximal ideal in $\operatorname{End}(M)$ consists of all nilpotent endomorphisms (and its complement consists of, of course, the automorphisms).