Math 6150, Problem 5

Adam Lizzi and Michael Martinez

September 24, 2009

#4. Define the radical of an R-module M by

$$\operatorname{rad}(M) = \bigcap_{N \prec M} N.$$

(a) Prove $\operatorname{rad}(R)M \subseteq \operatorname{rad}(M)$.

(b) Show that $\operatorname{rad}(M)$ consists of the nongenerators of M. That is, $m \in \operatorname{rad}(M)$ if and only if $M = \langle S \cup \{m\} \rangle$ implies $M = \langle S \rangle$. (Therefore any single element of $\operatorname{rad}(M)$ can be canceled from a generating set.)

(c) Show that if M is finitely generated and $P \subseteq \operatorname{rad}(M)$, then $M = N + P$ implies $M + N$. (Therefore in the case that M is finitely generated, any set of elements of $\operatorname{rad}(M)$ can be canceled from a generating set.) In particular, show that if $I \subset \operatorname{rad}(R)$, if M is finitely generated, and if $M = N + IM$, then $M + N$. (This is the weak form of Nakayama's lemma.)

(d) Prove that if a nonzero module is finitely generated, then $\operatorname{rad}(M)$ is proper; show this implies the weak form of Nakayama's lemma.

Proof. (a) Use the fact that the radical of a ring R is the set of all elements of R that annihilate all simple R-modules. If N is any maximal submodule of M, then the quotient M/N is a simple module, so $\operatorname{rad}(R)M/N = 0$. We can rewrite this by noting $\operatorname{rad}(R)M/N = \operatorname{rad}(R)M+N/N$. Since this quotient is the zero module, we infer $\operatorname{rad}(R)M + N \subset N$. This extra summand N is redundant, so instead write $\operatorname{rad}(R)M \subset N$. This holds for every maximal submodule $N \prec M$, so $\operatorname{rad}(R)M$ lives in the intersection of all the maximal submodues of M, defined to be $\operatorname{rad}(M)$.

(b) First say m is a nongenerator; we'll show $m \in \operatorname{rad}(M)$. Toward a contradiction, assume it isn't; then there's some maximal submodule N for which $m \notin N$. Take $S = \{N\}$, the set of all elements of N. If we enlarge S by including m, the resulting set must generate a submodule that is larger than N. Since N is maximal, it must be M itself; we've argued $\langle S \cup \{m\} \rangle = M$. Since m is a nongenerator we can cancel m from this generating set. Then $M = \langle S \rangle$, but since N is a submodule, the submodule generated by all its elements will be N itself. Then $M = N$ which isn't possible because N is proper.

In the other direction, say $m \in \operatorname{rad}(M)$. We hope that m is a nongenerator. Suppose $M = \langle S \cup \{m\} \rangle$. We hope $M = \langle S \rangle$. Again, toward contradiction assume otherwise; then $\langle S \rangle \neq M$ and the submodule generated by S must be contained in a maximal submodule N of M. This is true because M is finitely generated over $\langle S \rangle$. (In fact, it is singly generated, by just m.) Then take any $n \in M$. We may write $n = \sum r_i s_i + rm$ as an R-linear combination of the generators $S = \{s_i\}$ and m. Since $m \in \operatorname{rad}(M)$, in particular $m \in N$; therefore the right side of this expression is a sum of things in N and is again in N. This suggests everything in M is actually in N which again is false because N is proper.

(c) If $M = N + P$, then we can generate M in a rather redundant way by $M = \langle N \cup P \rangle$. Since M is also finitely generated we can write $M = \langle g_i \rangle_{i=1}^{k}$. Play these two sets of generators off against each other. Write g_i in terms of the $N \cup P$ generators: we have $g_i = n_i + p_i$ for two elements $n_i \in N$ and $p_i \in P$ (technically the n_i can be R-linear combinations of elements in N, but in that case we'll denote by n_i that linear combination; similarly for p_i). Now $M = \langle g_i \rangle = \langle n_i + p_i \rangle = \langle \{n_i\} \cup \{p_i\} \rangle$. Now we can repeatedly apply part (b) and eliminate the p_i from the generating set. Now $M = \langle \{n_i\} \rangle$. But the n_i must generate a submodule of N, implying $M \subseteq N$. And N is a maximal submodule, so $N \subseteq M$. Conclude $M = N$ as desired.

Part (a) says that if $I \subset \mathrm{rad}(R)$, then $IM \subset \mathrm{rad}(M)$. Then if $M = N + IM$, we've shown that IM can be eliminated from this expression, resulting in $M = N$; this is Nakayama's lemma.

(d) If M is simple, then the zero submodule is a proper submodule of M, and $\mathrm{rad}(M) = 0$, which is certainly proper. If M is not simple, then it contains a proper submodule P; Zorn's lemma will then guarantee a maximal proper submodule N containing P. Then $\mathrm{rad}(M) \subseteq N \subset M$, so the radical is proper. (As an alternate way to find P, we know that M is finitely generated over any one of its submodules, as it is itself finitely generated. Then each submodule is contained in a maximal submodule; in particular maximal submodules exist.)

In any case, we deduce Nakayama's lemma from this fact. Assume $M = IM$ for $I \subset \mathrm{rad}(R)$. Then $IM \subseteq \mathrm{rad}(M)$ by part (a), and we can take $N = 0$, $P = IM$ in part (c). IM then can be completely cancelled, implying $M = 0$ as we need.

$\square$