MAS439/MAS6320
CHAPTER 4: NAKAYAMA'S LEMMA

EVGENY SHINDER (PARTLY BASED ON NOTES BY JAMES CRANCH)

4.1. **Nilradical and Jacobson Radical.** Let R be a ring. The Nilradical of R is defined as intersection of all prime ideals:

$$Nil(R) = \bigcap_{P \subset R} P.$$

Note that $Nil(R)$ is an intersection of ideals, hence an ideal.

Proposition 4.1. *Nilradical coincides with the ideal consisting of all nilpotent elements:*

$$a \in Nil(R) \iff a^n = 0 \text{ for some } n > 0.$$

Proof. If $a^n = 0$, then since $0 \in P$ for every prime ideal, we have $a \in P$ (because P is prime). This proves one direction.

Conversely, let a be not nilpotent. We need to show that there is a prime ideal not containing P. Consider the multiplicative subset

$$U = \{a^n : n \in \mathbb{N}\} \subset R.$$

Consider the localized ring $U^{-1}R$ and take any prime ideal

$$P' \subset U^{-1}R.$$

By our basic correspondence between prime ideals in R and prime ideals in $U^{-1}R$ we see that there is a prime ideal $P \subset R$ not intersecting U. That's exactly what we were looking for! □

The Jacobson radical is defined as intersection of all maximal ideals in R:

$$J(R) = \bigcap_{m \subset R} m.$$

$J(R)$ is an ideal in R. Since every maximal ideal is prime, so that the intersection in defining $J(R)$ goes over larger set than in $Nil(R)$, we have an inclusion $Nil(R) \subset J(R)$.

Example 4.2. *If R is a local ring, then $J(R)$ is its unique maximal ideal.*

Here's an alternative characterisation:

Proposition 4.3. *Let R be a commutative ring. Then for an element $x \in R$, we have $x \in J(R)$ if and only if $1 - xy$ is a unit in R for all $y \in R$.*

Proof. We'll show firstly that if $x \in J(R)$, then $1 - xy$ is a unit. Indeed, suppose it isn't. Then let $I = (1 - xy)$, a proper ideal of R. The ideal I is contained in a maximal ideal M. Since $x \in J(R)$, we have $x \in M$, so $xy \in M$. Also $1 - xy \in M$ since $1 - xy \in I$. Hence $1 \in M$, which is a contradiction.

Now suppose that $1 - xy$ is a unit for all y, and suppose there is a maximal ideal M with $x \notin M$. Then the ideal sum $M + (x)$ (which, you'll remember, is defined to be $\{i + j \mid i \in M, j \in (x)\}$) is

Date: February 29, 2016.

a bigger ideal than M and is hence the whole of R (as M is maximal). Hence $1 \in M + (x)$, so $1 = u + xy$ for some $u \in M$ and some $y \in R$. Hence $1 - xy \in M$. But if $1 - xy$ is a unit, then $M = R$, a contradiction. □

4.2. **Matrices over rings.** Every square matrix with entries in a commutative ring has a determinant, and your favourite technique for computing the determinant will work fine.

However, not every matrix has an inverse: of course, for a general commutative ring, not even every 1×1 matrix has an inverse! We can form the adjugate matrix, however. (The *adjugate* matrix is the matrix you have immediately before you divide by the determinant to obtain the inverse: it's the transpose of the matrix of cofactors).

The same proof as usual shows that, for any square matrix A over any commutative ring whatsoever, we have

$$A \operatorname{adj}(A) = \operatorname{adj}(A)A = \det(A) \cdot I$$

where I is the identity matrix and $\operatorname{adj}(A)$ is the adjugate of A.

For example, if we have a two-by-two matrix

$$A = \begin{pmatrix} a & b \\ c & d \end{pmatrix},$$

then its adjugate is given by

$$\operatorname{adj}(A) = \begin{pmatrix} d & -b \\ -c & a \end{pmatrix}$$

and we have

$$\begin{aligned} A \operatorname{adj}(A) &= \begin{pmatrix} a & b \\ c & d \end{pmatrix} \begin{pmatrix} d & -b \\ -c & a \end{pmatrix} = \begin{pmatrix} ad - bc & 0 \\ 0 & ad - bc \end{pmatrix} \\ &= \begin{pmatrix} d & -b \\ -c & a \end{pmatrix} \begin{pmatrix} a & b \\ c & d \end{pmatrix} = \operatorname{adj}(A)A, \end{aligned}$$

and so both are equal to the determinant $\det(A) = ad - bc$ times the identity matrix. In particular, whenever we have a matrix with invertible determinant, it is invertible.

Matrices are useful with modules for the same reason that they're useful with vector spaces: they define homomorphisms of finitely generated free modules.

We'll also be needing this construction a lot:

Definition 4.4. *Let R be a commutative ring, I an ideal in R, and M an R-module. We write IM for the set*

$$IM = \{i_1 m_1 + \cdots + i_k m_k \mid i_i \in I, m_i \in M\}.$$

This is a submodule of M, since it's a subset of M and is evidently closed under addition and scalar multiplication.

Theorem 4.5 (Cayley-Hamilton)**.** *Let R be a commutative ring, and I an ideal in R. Let M be a finitely generated R-module and $\phi : M \to M$ a R-module homomorphism.*

Suppose that $\operatorname{Im}(\phi) \subset IM$. Then we can produce an equation for ϕ of the form $\phi^n + i_{n-1}\phi^{n-1} + \cdots + i_1\phi + i_0 = 0$, where all the elements i_k are in I.

Proof. Let $m_1, \ldots, m_k$ be a set of generators for M (we did say that M was finitely generated). Since $\operatorname{Im}(\phi) \subset IM$, we can write each $\phi(m_i)$ as a sum of the form $j_1 n_1 + \cdots + j_l n_l$ where $j_i \in I$ and $n_i \in M$.

However, all those n_i's can be written as a sum of multiples of the m_i's, since the m_i's generate M. Multiplying out, we can write

$$\phi(m_i) = a_{i1}m_1 + \cdots + a_{ik}m_k,$$

for each $i = 1, \ldots, k$ and some coefficients $a_{ij} \in I$.

We can regard that as a matrix equation: if we let δ_{ij} be the coefficients of the identity matrix (1 if $i = j$ and 0 otherwise), we can write

$$\sum_{j=1}^{n} (\delta_{ij}\phi - a_{ij})m_j = 0.$$

The determinant of the matrix (with coefficients in R) whose ij-th entry is $\delta_{ij}\phi - a_{ij}$ is hence zero, as we can see by multiplying by the adjugate matrix. If we expand that determinant out, we get a polynomial in ϕ with coefficients in I being zero, exactly as we needed. □

Corollary 4.6. (a) *If M is a finitely generated R-module and $\alpha : M \to M$ is a surjective homomorphism, then α is an isomorphism.*

(b) *If $M = R^n$, the free R-module of rank n, then any set of n generators is linearly independent*

(c) *The rank is well-defined, that is if $R^m \simeq R^n$, then $n = m$*

Proof. (a) We regard M as an $R[t]$-module where t acts by

$$t \cdot m := \alpha(m),$$

so that a general polynomial $f(t) = \sum_{k=0}^{n} a_k t^k$ acts as

$$f(t) \cdot m := \sum_{k=0}^{n} a_k \alpha^k(m).$$

Now we apply the Cayley-Hamilton Theorem to M, $\phi = id : M \to M$ and $I = (t) \subset R[t]$. M is finitely-generated as an R module, so is obviously finitely generated as an $R[t]$-module as well. Since α is surjective, $IM = tM = \alpha M = M$. All the assumptions of the Cayley-Hamilton Theorem are satisfied and we obtain that

$$(id + i_{n-1} + \cdots + i_0)(m) = 0 \text{ for all } m \in M.$$

Since the i_j's belong to $I = (t)R[t]$, it follows that there exists a polynomial $p(t)$ such that

$$1 - tq(t) \in R[t]$$

acts by zero on M. This means that $1 - \alpha q(\alpha) = 0$, and we get that $q(\alpha)$ is the inverse of α.

(b) The set of n generators $m_1, \ldots, m_n$ define a surjective map

$$\beta : R^n \to M = R^n.$$

By part (a), β must be an isomorphism which is equivalent to the set $m_1, \ldots, m_n$ being R-linear independent.

(c) Assume $m \leq n$, call the isomorphism $\phi : R^m \to R^n$ and consider the images of $e_1, \ldots, e_m \in R^m$

$$v_1 = \phi(e_1), \ldots, v_m = \phi(e_m) \in R^n.$$

Since ϕ is an isomorphism, these m elements generate R^n. Even though this is quite peculiar, there is no contradiction so far!

Now add $m - n$ zero elements to make the generating set to have size n:

$$v_1, \ldots, v_m, 0, \ldots, 0.$$

By assumption these generate R^n, but are not linearly independent unless $m = n$. □

Remark 4.7. *Of course, we could ask whether ϕ being injective implies that it's bijective, but that's not true. For example, the homomorphism $f : \mathbb{Z} \to \mathbb{Z}$ of $\mathbb{Z}$-modules defined by $f(x) = 2x$ is an injection but not a surjection of finitely generated modules.*

4.3. **Nakayama's Lemma.** Nakayama's Lemma is a series of results saying that finitely-generated modules are not so very different to finite-dimensional vector spaces.

We need some preparatory work based on the Cayley-Hamilton Theorem.

Lemma 4.8. *Let R be a commutative ring, and let M be a finitely generated R-module. Let I be an ideal of R such that $IM = M$. Then there exists $r \in I$ such that $(1 - r)M = 0$.*

Proof. Take ϕ to be the identity in Theorem 4.5 above.

This gives us an identity of the form

$$(1 + i_{n-1} + \cdots + i_1 + i_0)m = 0,$$

valid for all $m \in M$ where the coefficients lie in I. We obtain what we need by putting $r = -i_{n-1} - \cdots - i_1 - i_0$. □

Theorem 4.9 (Nakayama's Lemma)**.** *Let R be a commutative ring, I be an ideal contained in the Jacobson radical of R and M a finitely-generated R-module.*

(a) *If $IM = M$, then $M = 0$.*
(b) *If $N \subset M$ is a submodule such that $IM + N = M$, then $N = M$*
(c) *If $m_1, \ldots, m_n \in M$ have images in M/IM that generate it as an R-module, then $m_1, \ldots, m_n$ generate M as an R-module*

Proof. (a) We wish to use Lemma 4.8 above. This gives us that $(1-r)M = 0$ for some $r \in I \subset J(R)$. By Proposition 4.3, $1 - r$ is a unit in R, and hence $(1 - r)M = M$, and so $M = 0$.

(b), (c) This is left for the homework assignment.

□

Example 4.10. *For a possibly useful example, consider $R = \mathbb{Z}_{(7)}$. This ring has Jacobson radical equal to its unique maximal ideal (7). This says then that if $(7)M = M$ for any finitely-generated module M, then $M = 0$.*

Note that $(7)M = 7M$, the multiples of 7. So this tells us that multiplying by 7 cannot be surjective on any nontrivial finitely-generated $\mathbb{Z}_{(7)}$-module.