6. Lecture 6 – Nakayama's lemma & exact sequences

Recall the definitions of local ring and finitely generated module.

Example. Recall $\mathbb{R}(x)$, the field of real rational functions, which is the ring of expressions f/g with $f, g \in \mathbb{R}[x]$ and $g \neq 0$ (up to some equivalence relation). Let $A \subset \mathbb{R}(x)$ be the subring of those elements which can be written as

$$\frac{f}{g} \qquad f \in \mathbb{R}[x], g \in \mathbb{R}[x] \setminus (x).$$

So e.g.

$$\frac{x^2}{x+1}, \frac{x^3-2x}{5x+4}, \frac{x^3-x}{x^2-x} = \frac{x^2-1}{x-1} \in A$$

since $x+1, 5x+4, x-1 \notin (x)$, while e.g. $\frac{1}{x} \notin A$. Equivalently, A is the ring of the real rational functions which can be evaluated at 0, since we get a well-defined real number $f(0)/g(0)$ if and only if $f/g \in A$.

Claim: The ring A is local, with maximal ideal

$$\mathfrak{m} = \{f/g \in A \mid f(0)/g(0) = 0\} = \{f/g \mid f \in (x), g \in \mathbb{R}[x] \setminus (x)\}.$$

The homomorphism $A \to \mathbb{R}$ given by $f/g \mapsto f(0)/g(0)$ is surjective, with kernel $\mathfrak{m}$, so $\mathfrak{m}$ is a maximal ideal, and $A/\mathfrak{m} \cong \mathbb{R}$.[5]

Let's now recall that given an ideal $\mathfrak{a}$ and an A-module M, the submodule $\mathfrak{a}M \subset M$ is the module containing all sums

$$a_1 m_1 + \cdots + a_n m_n, \qquad a_i \in \mathfrak{a}, m_i \in M.$$

Lemma (Nakayama's lemma, local version)**.** [6] *Let A be a local ring with maximal ideal $\mathfrak{m}$, and let M be a finitely generated module. If $\mathfrak{m}M = M$, then $M = 0$.*

Definition. Let $T = (b_{ij})_{1 \leq i,j \leq n}$ be an $(n \times n)$-matrix with entries in A, and let T_{ij} be the $(n \times n)$-matrix obtained by deleting row i and column j. The **adjugate** of T is the matrix $\operatorname{adj}(T) = (c_{ij})_{1 \leq i,j \leq n}$, where

$$c_{ij} = (-1)^{i+j} \det(T_{ji}).$$

Example. The adjugate of $\begin{pmatrix} a & b \\ c & d \end{pmatrix}$ is $\begin{pmatrix} d & -c \\ -b & a \end{pmatrix}$.

Theorem. *We have $T \operatorname{adj}(T) = \operatorname{adj}(T) T = \det(T) I_n$, where I_n is the $(n \times n)$ identity matrix.*

Proof of Nakayama's lemma. Let M be a module, generated by $m_1, \ldots, m_n \in M$, meaning $M = \{a_1 m_1 + \cdots + a_n m_n \mid a_i \in A\}$. We know that $\mathfrak{m}M = M$, which means that for every m_i, we have $m_i \in \mathfrak{m}M$, which means we can write

$$m_i = \sum_{j=1}^{n} b_{ij} m_j,$$

---

[5] To see that A is local, note that if $f/g \notin \mathfrak{m}$, then $f(0)/g(0) \neq 0$, so $g/f \in A$, and so f/g is a unit. Since all non-units are contained in $\mathfrak{m}$, this means $\mathfrak{m}$ is the unique maximal ideal.

[6] The textbook states a more general version where A is not necessarily local, where $\mathfrak{m}$ is replaced with the Jacobson radical of A.

with $b_{ij} \in \mathfrak{m}$. Letting $T = I_n - (b_{ij})$, we then get that

$$T \begin{pmatrix} m_1 \\ \cdots \\ m_n \end{pmatrix} = 0,$$

and so

$$\operatorname{adj}(T)T \begin{pmatrix} m_1 \\ \cdots \\ m_n \end{pmatrix} = 0,$$

which since $\operatorname{adj}(T)T = \det(T)I_n$ gives $\det(T)m_i = 0$ for all i. But looking at the cofactor expansion of $\det(T)$ shows that

$$\det(T) = 1 + X,$$

where all the terms of X are divisible by b_{ij}, which implies that $X \in \mathfrak{m}$. Hence $\det(T)$ is a unit, and so $\det(T)m_i = 0$ implies $m_i = 0$. Thus all the $m_i = 0$, and so $M = 0$. □

Corollary. *Let A be a local ring, and let $\phi\colon M \to N$ be a homomorphism of modules, such that $\widetilde{\phi}\colon M/\mathfrak{m}M \to N/\mathfrak{m}N$ is surjective. Then ϕ is surjective.*

Proof. The trick is to reinterpret "ϕ is surjective" as $\operatorname{cok}\phi = N/\phi(M) = 0$. Assume that $\widetilde{\phi}$ is surjective. That means $N = \phi(M) + \mathfrak{m}N$ (after some thought). We get

$$\mathfrak{m}(N/\phi(M)) = (\mathfrak{m}N + \phi(M)/\phi(M)) = N/\phi(M),$$

Since N is finitely generated, so is $N/\phi(M)$. We can then apply Nakayama's lemma to $N/\phi(M)$, and get $N/\phi(M) = 0$. □

Example. Work in $A \subset \mathbb{R}(x)$ from before. Consider the matrix

$$B = \begin{pmatrix} \frac{1+x^2}{1-x^2} & \frac{x^2}{1-x^3} \\ \frac{x^4}{2-5x} & \frac{1+x}{1-x} \end{pmatrix}$$

which gives a homomorphism of A-modules $\phi\colon A^{\oplus 2} \to A^{\oplus 2}$ by

$$\phi(f,g) = B \begin{pmatrix} f \\ g \end{pmatrix}.$$

The associated homomorphism of $\widetilde{\phi}\colon A^{\oplus 2}/\mathfrak{m}A^{\oplus 2} \to A^{\oplus}2/\mathfrak{m}A^{\oplus 2}$ can be identified with the linear map $\mathbb{R}^2 \to \mathbb{R}^2$ obtained by setting $x = 0$ in the above matrix. That map is clearly surjective, hence ϕ is.

6.1. **Exact sequences and additivity.** Given $\phi\colon M \to N$ a homomorphism, we know about $\ker\phi \subset M$, $\operatorname{im}\phi \subset N$, $\operatorname{cok}\phi = N/\operatorname{im}\phi$.

Definition. A sequence of morphisms $M_1 \xrightarrow{\phi_1} M_2 \to \cdots \to M_{n-1} \xrightarrow{\phi_{n-1}} M_n$ is **exact at** M_i, $2 \le i \le n-1$, if we have

$$\operatorname{im}\phi_i = \ker\phi_{i+1}.$$

It is **exact** A sequence of the form

$$0 \to M' \to M \to M'' \to 0$$

is called **short exact**.

Example. If $M_i = 0$, then we have $\operatorname{im}\phi_i = 0$, so $\ker\phi_{i+1}$, and exactness at M_{i+1} means simply that $\ker\phi_{i+1} = 0$, i.e. that ϕ_{i+1} is surjective. We also have $\ker\phi_{i-1} = M_{i-1}$, so exactness at M_{i-1} means that $\operatorname{im}\phi_{i-2} = M_{i-1}$, i.e. that $\operatorname{im}\phi_{i-2}$ is surjective.

Example. Let $M' \subseteq M$ be a submodule. Then the sequence

$$0 \to M' \to M \to M/M' \to 0$$

is exact, since (1) $M' \to M$ is injective, (2) $M \to M/M'$ is surjective, and (3) $\ker(M \to M/M') = \operatorname{im}(M' \to M)$.

"Up to isomorphism", every short exact sequence is of this form, meaning if

$$0 \to M_1 \to M \to M_2 \to 0$$

is short exact, them M_1 is isomorphic to some submodule $M' \subset M$, and M_2 is isomorphic to M/M'.

Example. The sequence $0 \to \mathbb{Z} \xrightarrow{\phi} \mathbb{Z} \to \mathbb{Z}/(n) \to 0$ is exact, where $\phi(k) = nk$.

Example. The sequence $0 \to \mathbb{Z}/(2) \to \mathbb{Z}/(4) \to \mathbb{Z}/(2) \to 0$ is exact, where $\mathbb{Z}/(2)$ is the inclusion $1 \mapsto 2$.

Example. Let V be the $\mathbb{R}$-vector space of all smooth vector fields on $\mathbb{R}^3$, and let W be the $\mathbb{R}$-vector space of all functions on $\mathbb{R}^3$. The sequence

$$0 \to \mathbb{R} \xrightarrow{a \mapsto f(x)=a} W \xrightarrow{\nabla} V \xrightarrow{\nabla\times} V \xrightarrow{\nabla\cdot} W \to 0$$

is exact.

Example. For any modules M and N, the sequence

$$0 \to M \to M \oplus N \to N \to 0$$

is exact, where $M \to M \oplus N$ is the map $m \mapsto (m, 0)$ and $M \oplus N \to N$ is the map $(m, n) \to n$.

We can break up exact sequences into short ones, as follows: If $M_{i-1} \to M_i \to M_{i+1}$ is an exact sequence, we can take $0 \to \operatorname{im}(\phi_{i-1}) \to M_i \to \operatorname{im}(\phi_i) \to 0$ as a short exact sequence. This motivates the following definition

Definition. A function from some set of modules to an abelian group G is called **additive** if for all short exact sequences

$$0 \to M' \to M \to M'' \to 0$$

we have $\nu(M) = \nu(M') + \nu(M'')$.

Example. If M', M, M'' are finite-dimensional vector spaces, then $\dim(-)$ is additive, since we can extend a basis for M' to a basis for M, and the new elements give a basis for M'' after projection.

Example. If M', M, M'' are finite abelian groups, then $\nu(M) = |M|$, the number of elements of M, is an additive function to the group $\mathbb{Q}_{>0}$ with the operation of multiplication, since Lagrange's theorem says that for subgroups $M' \subset M$ we always have

$$|M| = |M'||M/M'|.$$

Theorem. *Let* $0 \to M_1 \to M_2 \to \cdots \to M_n \to 0$ *be an exact sequence, and let* ν *be an additive function. Then*

$$\sum (-1)^i \nu(M_i) = 0$$

Proof. We have $\nu(M_i) = \nu(\operatorname{im}\phi_i) + \nu \operatorname{im}(\phi_{i-1})$. Inserting this in $\sum(-1)^i\nu(M_i)$ everything cancels to give 0. □

Example. In an exact sequence of vector spaces $0 \to V_1 \to V_2 \to \cdots \to V_n \to 0$, we have $\sum(-1)^i \dim V_i = 0$.

Example. Given an exact sequence

$$0 \to M_1 \to \cdots \to M_n \to 0$$

of finite $\mathbb{Z}$-modules, we have

$$\prod_{i=1}^{n} |M_i|^{(-1)^i} = 1.$$

Definition. A diagram of modules and homomorphisms between them is called **commutative** if the composed maps between any two modules agree.

Example. The diagram

$$\begin{array}{ccc} M & \xrightarrow{f} & M' \\ \downarrow{\scriptstyle i} & & \downarrow{\scriptstyle g} \\ N & \xrightarrow{h} & N' \end{array}$$

is commutative if $g \circ f = h \circ i$.

Lemma (The snake lemma)**.** *Given modules and homomorphisms that fit into the following commutative diagram*

$$\begin{array}{ccccccccc} 0 & \longrightarrow & M' & \longrightarrow & M & \longrightarrow & M'' & \longrightarrow & 0 \\ & & \downarrow{\scriptstyle \phi'} & & \downarrow{\scriptstyle \phi} & & \downarrow{\scriptstyle \phi''} & & \\ 0 & \longrightarrow & N' & \longrightarrow & N & \longrightarrow & N'' & \longrightarrow & 0, \end{array}$$

we get an exact sequence of modules

$$0 \to \ker\phi' \to \ker\phi \to \ker\phi'' \to \operatorname{cok}\phi' \to \operatorname{cok}\phi \to \operatorname{cok}\phi'' \to 0$$