MATH 899: Algebraic Geometry

Nayeong Kim

Spring 2022

Contents

Introduction

This note is written by Nayeong Kim based on the lecture MATH 899 by Prof. Serkan Hosten.

1. Cayley-Hamilton Thm and Nakayama's Lemma

Reminder: Modules

The reference of this reminder section is [1] and [2].

Modules and module homomorphisms

Let us consider a commutative ring R with 1. An R-module is an Abelian group M with a multiplication map

$$R \times M \to M, \quad \text{written } (f, m) \mapsto f \cdot m$$

satisfying following properties:
(i) $f \cdot (m \pm n) = f \cdot m \pm f \cdot n$, (ii) $(f \pm g) \cdot m = f \cdot m \pm g \cdot m$, (iii) $(fg) \cdot m = f \cdot (g \cdot m)$, (iv) $1_R \cdot m = m$ for all $f, g \in R$ and $m, n \in M$.
A subset $N \subset M$ is a submodule if $f \cdot m + g \cdot n \in N$ for all $f, g \in R$ and $m, n \in M$. Furthermore, R-module homomorphism $\phi : M \to N$ is a map between R-modules M, N that is R-linear which means that $\phi(f \cdot m + g \cdot n) = f \cdot \phi(m) + g \cdot \phi(n)$ for all $f, g \in R$ and $m, n \in M$.

Isomorphism theorems

Let us remind isomorphism theorems for R-modules.

Theorem 1. Isomorphism theorems for R-modules
(1) If $L \subset M \subset N$ are submodules then

$$N/M = (N/L)/(M/L).$$

(2) If N is a module, and $L, M \subset N$ are submodules then

$$(M + N)/L = M/(M \cap L).$$

Induced $R[x]$-module by R-module homomorphism

If ϕ is an R-module endomorphism on M, $p(\phi)$ is also an R-module endomorphism where $p(x) \in R[x]$. Hence we can consider an R-module M as $R[x]$-module with the action $p(x) \cdot m = p(\phi) \cdot m$ where $p(x) \in R[x]$ and $m \in M$.

1.1. Cayley-Hamilton Theorem

In linear algebra courses, we proved Cayley-Hamilton theorem for linear operators between vector spaces using concepts of generalized eigen spaces. Cayley-Hamilton theorem can be generalized for some R-module homomorphisms. Consider an R-module M which is (finitely) generated by $m_1, \cdots, m_n$. An R-module homomorphism $\phi : M \to M$ can be represented by a matrix $A = (a_{ij})$ which has its entries in R because ϕ is determined by $\phi(m_j) = \sum_{k=1}^n a_{jk} m_k$.

Definition 1. Determinant of a Matrix
The determinant of an $n \times n$ matrix $A = (a_{jk})$ is

$$\det A = \sum_{\sigma \in S_n} \mathrm{sign}(\sigma) a_{1\sigma(1)} \cdots a_{n\sigma(n)}.$$

Definition 2. Characteristic Polynomial
Let R be a commutative ring. Let A be an $n \times n$ matrix with entries in R. Then the polynomial $p_A(x) := \det(xI_n - A)$ is called the characteristic polynomial of A.

Proposition 1. $p_A(x)$ is a monic polynomial of degree n with coefficients in R.

Proof. Since $xI_n - A$ has its entries in $R[x]$, $p_A(x) = \det(xI_n - A)$ is in $R[x]$. From the definition, each $a_{k\sigma(k)}$ has a degree at most 1 when $k = \sigma(k)$. (Otherwise, the entry is a constant in R.) Hence the identity element of S_n has the unique term with degree n and the term is $(x - a_{11}) \cdots (x - a_{nn})$ which is a monic polynomial of degree n. Hence $p_A(x)$ is a monic polynomial of degree n. □

Theorem 2. Cayley-Hamilton Theorem
Let M be a finitely generated R-module. Let $\phi : M \to M$ be an R-module homomorphism. If $p(x)$ is the characteristic polynomial of any matrix representing ϕ, then $p(\phi) = 0$.

Proof. Suppose that M has a generating set $m_1, \cdots, m_n$ and ϕ is represented by an $n \times n$ matrix $A = (a_{jk})$ where $\phi(m_j) = \sum_{k=1}^n a_j k m_k$. Hence we have that $\sum_{k=1}^n \delta_{jk}\phi - a_{jk} m_k = 0$ for all j where $\delta_{jk} = 1$ when $j = k$ and $\delta_{jk} = 0$ otherwise. Consider a matrix Δ having jkth entry: $\delta_{jk}\phi - a_{jk}$. Then $\Delta m_j = 0$ for all j. Recalling that $\mathrm{adj}\Delta \cdot \Delta = \det \Delta I_n$[1]. Therefore $\det(\Delta) m_j = 0$ for all j. Since $\det(\Delta) = p(\phi)$ where $p(x)$ is the characteristic polynomial of A, it is proved that $p(\phi) = 0$. □

Corollary 1. A complex number λ is an eigenvalue of T if and only if λ is a root of the characteristic polynomial of T.

Proof. ($\Rightarrow$) Let $p(x)$ be the characteristic polynomial of T. With Cayley-Hamilton theorem, $p(T) = 0$. Let v be an eigenvector of T having eigenvalue λ. Then $p(T)v = p(\lambda)v$ hence $p(\lambda)v = 0$. Since v is a nonzero vector, we have $p(\lambda) = 0$ which implies that λ is a root of $p(x)$.
($\Leftarrow$) Let λ be a root of the characteristic polynomial $p(x)$ of T. Hence $0 = p(\lambda) = \det(\lambda I_n - A)$ where A is a matrix representing T. Hence $\lambda I_n - A$ is not invertible, which implies that there exists a nonzero vector $v \in \mathrm{null}(\lambda I_n - A)$. Then v is an eigenvector having eigenvalue λ. □

Exercise 1. Let V be a finite-dimensional vector space over the field F and T a linear operator on V. the minimal polynomial of T is the monic polynomial that generates the annihilator of an $F[x]$-module induced by T. Prove that the minimal polynomial of T divides the characteristic polynomial of T.

Solution. Let $p(x)$ be the characteristic polynomial of T and $q(x)$ be the minimal polynomial of T. Since $p(x)$ annihilates V, from the definition of the minimal polynomial, p has larger degree than q. Hence we can get the remainder $r(x)$ by dividing p by q: $p = q \cdot q' + r$. Since $r(T) = p(T) - q(T) \cdot q'(T) = 0$, $r(x)$ must be 0 because it contradicts to the fact that q is the minimal polynomial otherwise. As a result, q divides p. □

[1] The adjoint matrix of Δ is C^T where C has M_{jk} jkth entry where M_{jk} is the determinant of the $(n-1) \times (n-1)$ matrix which removed jth row and kth column from Δ.

1.2. The Determinant Trick

Theorem 3. Let M be a finitely generated R-module, generated by n elements, and $\phi : M \to M$ an R-module endomorphism. Suppose I is an ideal of R such that $\phi(M) \subset IM$. Then

$$\phi^n + a_1\phi^{n-1} + \cdots + a_{n-1}\phi + a_n = 0$$

for some $a_i \in I$ where $i = 1, \cdots, n$.

Proof. With the premise, we have $M = (m_1, \cdots, m_n)$ where $m_1, \cdots, m_n \in M$. For each j, we can write $\phi(m_j) = b_j \cdot n_j$ for some $b_j \in I$ and $n_j \in M$ because $\phi(M) \subset IM$. We can write n_j as an R-linear combination of $m_1, \cdots, m_n$: $n_j = r_{j1} \cdot m_1 + \cdots r_{jn} \cdot m_n$. Then $A = (a_{jk})$ is a matrix representing ϕ where $a_{jk} = b_j r_{jk}$. Every entry of A is in I because b_js are in I. The characteristic polynomial $p(x)$ of A has coefficients in I. With theorem 2, $p(x)$ has degree n and $p(\phi) = 0$. □

Exercise 2. Show that the coefficients a_i mentioned in the proof are in I^i for $i = 1, \cdots, n$.

Solution. Let $A = (a_{jk})$ be the matrix mentioned in the proof of theorem 3. Considering x and a_{jk}s as variables, the each entry of $xI_n - A$ has total degree 1. Hence the determinant is a homogeneous polynomial with a total degree n. Therefore each term $a_k\phi^{n-k}$ has total degree n. It implies that a_k has total degree of k considering a_{jk}s as variables. Considering a_{jk} as elements in I, we can conclude that $a_k \in I^k$. □

Corollary 2. Let M be a finitely generated R-module and I an ideal of R. If $M = IM$, then there exists an element $s \in R$ such that $s + I = 1 + I$ in R/I and $s \cdot M = 0$.

Proof. Let us consider the identity map id_M on M. By theorem 3, we have some $a_1, \cdots, a_n \in I$ such that $id_M^n + a_1 id_M^{n-1} + \cdots + a_n = 0$. Since the action of $id_M^n + a_1 id_M^{n-1} + \cdots + a_n$ on M (as an $R[x]$-module) is the same as the action of $s = 1 + a_1 + \cdots + a_n$ on M (as an R-module), we have $(1 + a_1 + \cdots + a_n) \cdot m = 0$ for all $m \in M$. Furthermore, we have $a_1 + \cdots + a_n \in I$ hence $s + I = 1 + I$ in R/I. □

Theorem 3 and corollary 2 are known as the determinant trick.

1.3. Nakayama's Lemma

Definition 3. Local Ring
A local ring is a commutative ring with a unique maximal ideal.

Proposition 2. A ring is local if and only if the set of non-units forms an ideal.

Proof. ($\Rightarrow$) Take any non-unit $a \in R$. Then aR is an ideal of R. Furthermore, aR is a proper ideal of R because $1 \in R$ is not in aR. By the premise, we have a unique maximal ideal I. Since aR is a proper ideal and I is the unique maximal ideal, we have $aR \subset I$. Hence all non-unit elements are in I. Also, there are no units in I because it is a proper ideal. Therefore we can conclude that the set of non-units of R is the unique maximal ideal I.
($\Leftarrow$) Let I be any proper ideal of R. There are no units in I. Hence I is in the set of non-units. Since the set of non-units is a maximal ideal of R and any proper ideal is in the set, we can conclude that the set of non-units is the unique maximal ideal of R. Therefore R is a local ring. □

Theorem 4. Nakayama's Lemma
Let R be a local ring with maximal ideal I, and let M be a finitely generated module. If $M = IM$, then M is the zero module.

Proof. Since $M = IM$, we can apply the determinant trick. By corollary 2, we have some $s \in R$ such that $s + I = 1 + I$ and s annihilates M. Since $s + I = 1 + I$, $s \notin I$ hence s is a unit in R. For any m, we have $m = s^{-1}s \cdot m = 0$. Hence M is the zero module. □

Corollary 3. Let R be a local ring with maximal ideal I. Let M be an R-module and N a submodule of M. If M/N is finitely generated and $M = N + IM$, then $M = N$.

Proof. The hypothesis $M = N + IM$ implies that $M/N = I(M/N)$. By Nakayama's Lemma, M/N is the zero module, which implies that $M = N$. □

Corollary 4. Let R be a local ring with maximal ideal I and let M be a finitely generated R-module. Then $\{m_1, \cdots, m_k\}$ is a minimal generating set of M if and only if $m_1 + IM, \cdots, m_k + IM$ is a vector space basis of the R/I-module M/IM. In particular, every minimal generating set of M has the same cardinality.

Proof. ($\Rightarrow$) Since $m_1, \cdots, m_k$ generates M, it is clear that $m_1 + IM, \cdots, m_k + IM$ generates M/IM which is a vector space over R/I. (Recall that R/I is a field because R is a local ring.) We will show that this set is also linearly independent. Suppose that $\bar{r_1}(m_1 + IM) + \cdots + \bar{r_k}(m_k + IM) = 0$ for some $\bar{r_1}, \cdots, \bar{r_k} \in R/I$ where $\bar{r_j} = r_j + I$. Then $r_1m_1 + \cdots r_km_k$ is in IM. Suppose that some r_j is a unit. Then $m_j = r_j^{-1}(r_1m_1 + \cdots + r_{j-1}m_{j-1} + r_{j+1}m_{j+1} + \cdots + r_km_k)$. This contradicts that $\{m_1, m_2, \cdots, m_k\}$ is a minimal generating set. Hence all r_js are non-units which are in I. Hence $\bar{r_1} = \cdots = \bar{r_k} = \bar{0}$. Therefore we can conclude that $m_1 + IM, \cdots, m_k + IM$ are linearly independent.
($\Leftarrow$) Let N be the submodule of M generated by $m_1, \cdots, m_k$. Then $I(M/N) = (IM + N)/N$. Since $IM + N$ is a submodule of M and the projected image in M/IM is the same as $(IM + N)/IM$. By the premise, $(IM + N)/IM = M/IM$, which implies that $IM + N = M$. Therefore we have $I(M/N) = M/N$. By corollary 3, we can conclude that $M = N$ and M is generated by $m_1, m_2, \cdots, m_k$. It is also minimal because of the linear independence of $m_1 + IM, \cdots, m_k + IM$ in the R/I-module M/IM.
Since any basis of a finite dimensional vector space has the same size, we can conclude that every minimal generating set of M has the same cardinality. □

Reference

1. Undergraduate Commutative Algebra Chapter 2 Modules, Reid
2. Introduction to Commutative Algebra Chapter 2 Modules, Atiyah and MacDonald
3. Lecture Note of MATH 850, Prof. Serkan Hosten