

Commutative Algebra and Algebraic Geometry — Lecture 2

Martin Svanberg

October 9, 2018

Noetherian rings

Noetherian rings can also be defined for noncommutative rings. For noncommutative rings you have the left ACC and the right ACC and equivalent for DCC, left ACC gives left Noetherian and vice versa. There exist rings that are left Noetherian but not right Noetherian.

In the noncommutative case, some properties may still exist in some form but are often more complicated.

Lemma 1. Noetherian rings are closed under quotients. That is R Noetherian $\implies R/I$ Noetherian for every ideal $I \in R$.

Proof.

Recall. ideals in $\{R/I\} \leftrightarrow \{\text{ideals in } R \text{ containing } I\}$ are in bijection due to the isomorphism theorems. $I \subset J \subset R$.

$$\begin{aligned} J/I &\leftrightarrow J \\ \delta &\mapsto \pi^{-1}(\delta) \end{aligned}$$

Let $\pi : R \rightarrow R/I$.

$$\pi^{-1}(\text{Ascending chain in } R/I) = \text{Ascending chain in } R$$

If right side chain is stationary then left side chain is stationary.

Lemma 2. TFAE (The following are equivalent):

1. R is Noetherian (ACC)
2. Every nonempty set of ideals in R has a maximal element under inclusion \subset .

3. Every ideal is finitely generated.

Recall. Zorn's lemma.

Any proper ideal is contained in a maximal ideal. Let (X, \leq) be a partially ordered set. A chain in X is a subset $Y \subset X$ is linearly ordered, $\forall y_1, y_2 \in Y$ either $y_1 \leq y_2$ or $y_2 \leq y_1$. An upper bound for a chain Y is a $z \in X$ st $z \geq y \forall y \in Y$. An upper bound does not have to be in the chain, but has to be in the set.

Zorn's lemma: Assume X is a poset. If every chain has an upper bound, then X has a maximal element.

Zorn's lemma is equivalent to the axiom of choice.

Proof.

1 \implies 2. Use Zorn. Let $x = \{I \subset R \mid I \text{ ideals in } R\}$ and \leq is inclusion. R Noetherian \implies every chain has an upper bound.

2 \implies 3. This is a standard argument. Let $J \in R$ be an ideal. We want to show that J is finitely generated. Let $X = \{I \subset J \mid I \text{ finitely generated}\}$. X is nonempty because the zero ideal is contained in there. By 2), X has a maximal element under inclusion, called J_{max} . If J is finitely generated, then it is in X and so $J = J_{max}$. By definition $J_{max} \subset J$. Assume there is an $x \in J$ st $x \notin J_{max}$. We know J_{max} is finitely generated, so we can write it as generated by $J_{max} = (x_1, \dots, x_n)$ for $x_j \in R$. $(J_{max}, x) = (x_1, \dots, x_n, x)$ is finitely generated. $x \in J \implies (x_1, \dots, x_n)$ finitely generated which contradicts that J_{max} is maximal.

3 \implies 1. Want to show ACC. Let $J_1 \subset \dots \subset J_n$ ascending chain of ideals in R . Union of two ideals is in general not an ideal.

Let $I = \cup_{n \geq 1} J_n$. Ideals are not closed under unions, but chains of ideals are. So I is an ideal. So I is a finitely generated ideal. So $I = (x_1, \dots, x_n)$ for $x_j \in R$. For all I there are n_i st $x_i \in J_{n_i} \forall 1 \leq i \leq n$. Let $N = \max n_i$. Then the chain stabilizes at that point (or maybe earlier). Then $x_1, \dots, x_n \in J_N \implies I_N = I \implies I_N = I_{N+k} \forall k \geq 1$, that is, the chain is stationary.

□

Theorem 1. Hilbert basis theorem. R Noetherian implies $R[x]$ Noetherian.

Proof. (Hilbert's basis theorem)

Let $I \subset R[x]$. Want to show I is finitely generated.

Define $\text{Lead}(a_d x^d + \dots + a_1 x + a_0) = a_d$.

Let $L = \{\text{Lead}(f) \mid f \in I\} \cup \{0\}$. Let $L_d = \{\text{Lead}(f) \mid f \in I, \deg f = d\} \cup \{0\}$.

Claim: L and every L_d is an ideal in R .

By definition, $L = \cup_{d \geq 1} L_d$. L_d is an ideal: WTS that $ar + b \in L_d \forall a, b \in L_d, r \in R$. $a, b \in L_d \implies \exists f, g \in I, \deg f = \deg g = d$ and $\text{Lead } f = a, \text{Lead } g = b$. Then, $\text{Lead } (rf - g) = ar - b$ iff $ar - b$ is nonzero.

L is an ideal: $a, b \in L \implies \exists f, g \in I$ st $\text{Lead } f = a, \text{Lead } g = b$. Let $d = \deg f$ and $e = \deg g$. Still want $rf - g$, but want degrees to be the same so we can multiply by x^e and x^d : $rfx^e - gx^d$ so they both have degree $d + e$. Then the leading term will again be $ar - b$ so long as $ar - b$ is nonzero.

R Noetherian implies L, L_d all finitely generated. $L(a_1, \dots, a_n)$ and $L_d = (a_{d,1}, \dots, a_{d,n})$ for some $a_i, a_j \in R$. $a_i \in L_d$ implies there is $f_i \in I$ st $\text{Lead } f_i = a_i$. $a_{d,j} \in L_d$ implies there is $f_{d,j}$ st $\deg f_{d,j} = d$ and $\text{Lead } f_{d,j} = a_{d,j}$.

Let $e_i = \deg f_i$ and $N = \max e_i$. N will truncate the infinitely many d s. By using N , we set $I' = (f_1, \dots, f_n, f_{d,1}, \dots, f_{d,n}, \dots)$ or $I' = (f_{i,1}, \dots, f_{d,j} \mid 1 \leq i \leq n, 1 \leq d \leq N)$ which is a finite set. Claim: $I' = I$. It is clear that $I' \subset I$ since all generators have been constructed as elements of I .

Assume $f \in I, f \notin I'$. Pick f of minimal degree d .

Case I. $d \geq N$.

$$a = \text{Lead } (f) \in L \implies a = \sum a_i r_i \quad r_i \in R$$

$$g = r_1 x^{d-e_1} f_1 + \dots + r_n x^{d-e_n} f_n$$

$$\deg g = d$$

$$\text{Lead } g = a_1 r_1 + \dots + a_n r_n = a \neq 0$$

Consider $f - g \in I$. Then $\deg(f - g)$ contradicts minimality of f unless it is zero.

Case II. $d < N$. Let $a = \text{Lead } f \in L_d$. Use generators for L_d . So $a = \sum_{j=1}^n s_j a_{d,j}$ $s_j \in R$. Define $g = s_1 f_{d,1} + \dots + s_n f_{d,n} \in I'$ and $\text{Lead } g = a$ and $\deg g = d$ and $f - g$ contradicts minimality as before, i.e. it will have a smaller degree.

□

Modules

Not in Ch. 15 of Dummit and Foote. Ch. 10 covers it.

Modules are like ring actions, much like groups act on sets. Let R be a commutative ring with 1. An R -module is a set M with maps $+$: $M \times M \rightarrow M$,

$(a, b) \mapsto a + b$ and $- : a \mapsto -a$. These make M an abelian group under $+$. Then there is a map $R \times M \rightarrow M$ st $(r, m) \mapsto rm$. Restrictions on action map:

$$\begin{aligned} r(m + n) &= rm + rn \\ (r + s)(m) &= rm + sm \\ (rs)(m) &= r(sm) \\ 1m &= m \forall r, s \in R \quad m, m \in M \end{aligned}$$

Remark: you can also have left/right modules for noncommutative R .

Example 1. Any vector space is a module. If R is a field then an R -module is an R -vector space.

Another way of looking at modules is as a generalization of vector spaces from fields to rings.

Example 2. \mathbb{Z} -modules are Abelian groups over the integers. The action is powering but in additive notation.

Example 3. $k[x]$ -modules is the same thing as pairs (V, T) with V a vector space over k and $T : V \rightarrow V$ a linear map. $f(x) = a_n x^n + \dots + a_0$ acts on $v \in V$ by $a_n T^n(v) + \dots + a_1 T(v) + a_0$ where $T^n(v) = T(T(\dots T(v)))$

Example 4. k a field and G is a finite group. $k[G]$ is a group ring G/k . $k[G]$ is a ring, commutative $\iff G$ abelian. $k[G]$ -modules $\leftrightarrow (V, \rho)$, $\rho : G \rightarrow G(V)$ (representation theory)

ACC and DCC make sense for M using submodules.

Example 5. R is an R -module and a submodule of R -as-a-module is just an ideal.

Next time: Kinds of modules. Projective and injective modules. Affine algebraic sets.