Lecture 5, Noetherian rings & modules, I.

0) Modules: why to care and what's next?
1) Noetherian rings & modules
2) Hilbert's Basis theorem
3*) Further properties of Noetherian modules.

References: [AM], Chapter 6, intro to Chapter 7

BONUS: • Non-Noetherian rings in Complex Analysis.
• Why Hilbert cared.

0.1) Why to care about modules?

Reason 0: modules generalize various classical objects: abelian groups, vector spaces, vector spaces equipped w. linear operator ($\mathbb{F}[x]$-modules), collection of commuting operators ($\mathbb{F}[x_1, \dots x_n]$-modules).

Reason 1: modules provide a general framework for discussing (some) properties of ideals in A or A-algebras. For example, for ideals we care about whether they are principal. This is a property which only requires the module structure.

Reason 2: Modules are important from the point of Algebraic geometry. For example, an important class of modules we'll study later in this course - projective modules - geometrically correspond to vector bundles, an object of primary importance for various parts of Geometry.

0.2) What's next?

When we study vector spaces in Linear algebra, we almost always concentrate on finite dimensional ones. One can ask about an analog of finite dimensional for modules. The 1st guess is that one should work w. finitely generated modules. However such modules may have pathological behavior: a submodule in a finitely generated module may fail to be finitely generated: in Problem 2 of HW1 we have the regular module (generated by a single element) with a submodule (= ideal) that isn't fin. generated. We are going to study the condition on modules (and the ring A itself) that guarantees that this doesn't happen.

1) Noetherian rings & modules

1.1) Main definitions & examples.

Definition: Let A be a commutative ring.

i) An A-module M is Noetherian if $\forall$ submodule of M (including M) is finitely generated.

ii) A is a Noetherian ring if it's Noetherian as a module over itself, i.e. every ideal is finitely generated.

Examples:

0) Every field $\mathbb{F}$ is Noetherian ring (ideals in $\mathbb{F}$ are $\{0\}$, $\mathbb{F}=(1)$).

1) $A=\mathbb{Z}$ is Noetherian: b/c $\forall$ ideal is principal.

1.2) Equivalent characterizations of Noetherian modules.

Definition: M is A-module.

- By an ascending chain (AC) of submodules of M we mean: collection $(N_i)_{i\geq 0}$ of submodules of M s.t $N_i \subseteq N_{i+1}$ $\forall i\geq 0$: $N_1 \subseteq N_2 \subseteq N_3 \subseteq \dots$
- We say that the AC $(N_i)_{i\geq 0}$ terminates if $\exists k\geq 0$ s.t $N_j = N_k$ $\forall j\geq k$.
- If every AC terminates, we say M satisfies AC termination.

Proposition: For an A-module M TFAE:

1) M is Noetherian.

2) M satisfies AC termination $=$ $\forall$ AC of submodules of M terminates

3) $\forall$ nonempty set X of submodules of M has a maximal element w.r.t. inclusion (i.e $N\in X$ s.t. $N \not\subsetneq N'$ for $N' \in X$, $N' \neq N$).

Proof:

$(1)\Rightarrow(2)$: AC $(N_i)_{i\geq 0}$: $N_1 \subseteq N_2 \subseteq \dots \rightsquigarrow N := \bigcup_{i\geq 0} N_i$ is a submodule (e.g. if $n_1, n_2 \in N \Leftrightarrow \exists i,j \mid n_1 \in N_i, n_2 \in N_j \xRightarrow{AC} n_1, n_2 \in N_{max(i,j)} \Rightarrow n_1 + n_2 \in N_{max(i,j)} \subset N$). This N is fin. gen'd so $\exists m_1, \dots m_\ell \in N$ w. $N = Span_A(m_1, \dots m_\ell)$. Now $\exists k_i \mid m_i \in N_{k_i} \xRightarrow{AC} m_1, \dots m_\ell \in N_k$ for $k = max\{k_i\} \Rightarrow N = Span_A(m_1, \dots m_\ell) \subseteq N_k$ so AC (N_i) terminates at N_k.

$(2)\Rightarrow(3)$: Pick $M_1 \in X$; if it's not maximal w.r.t. $\subseteq$, pick $M_2 \supsetneq M_1$, if M_2 isn't maximal, pick $M_3 \supsetneq M_2$, etc. We arrive at AC of submodules that doesn't terminate.

$(3)\Rightarrow(1)$: Let N be a submodule of M. Let X be the set of all finitely generated submodules of N & N' be its maximal el't. If $N'=N$, we are done. Otherwise let $m_1,\dots m_k \in N'$ be generators & pick $m_{k+1}\in N\setminus N'$. Set $N'':=\mathrm{Span}_A(m_1,\dots,m_{k+1})$. Then $N''\supsetneq N'$ & N'' is fin. generated which contradicts the maximality of N'. $\square$

Corollary: Every nonzero Noetherian ring has a maximal ideal.

Proof: The set $\{I\subset A \mid \text{ideals} \neq A\}$ has a max el't by (3).

2) Hilbert basis theorem.

2.1) Statement & proof

It turns out that there are a lot of Noetherian rings, in fact most rings we are dealing with are Noetherian. The following is a basic result in this direction.

Thm (Hilbert, 1890)
If A is Noetherian, then so is $A[x]$

Proof: Let $I\subset A[x]$ be an ideal. Assume it's not finitely generated. We construct a sequence of elements $f_1,\dots f_k,\dots \in I$ as follows: $f_1\neq 0$ is an element of I with minimal possible degree. Once $f_1,\dots f_{k-1}$ are constructed, we choose $f_k\in I\setminus(f_1,\dots f_{k-1})$ (this set is nonempty b/c $I\neq(f_1,\dots f_{k-1})$) - again of minimal possible degree. Let $d_i := \deg f_i$ & $a_i\neq 0$ be the coefficient of x^{d_i} in f_i: $f_i=a_ix^{d_i}+\text{lower deg. terms}$.

We need two observations about the process:

I) If $g \in I$ & $\deg g < \deg f_k \Rightarrow g \in (f_1, \dots f_{k-1})$ – otherwise we choose g instead of f_k ($\forall k$)

II) $d_k \geq d_{k-1}$ $\forall k$ – same reason

Now let $I_k = (a_1, \dots a_k) \subset A$, $k \geq 0$. This is an ascending chain of ideals in A. Since A is Noetherian, it must terminate. So $a_{m+1} \in (a_1, \dots a_m)$ for some $m \Rightarrow a_{m+1} = \sum_{i=1}^m b_i a_i$, $b_i \in A$. Set

$$g := f_{m+1} - \sum_{i=1}^m b_i x^{d_{m+1}-d_i} f_i$$

By II), $d_{m+1} \geq d_i \Rightarrow x^{d_{m+1}-d_i} \in A[x]$ & $f_j \in I$ $\forall j = 1, \dots m+1$. So $g \in I$.

But $g = \underbrace{(a_{m+1} - \sum_{i=1}^m b_i a_i)}_{=0} x^{d_{m+1}}$ + lower deg. terms $\Rightarrow \deg g < d_{m+1}$. By I), $g \in (f_1, f_2, \dots f_m)$

$$\Rightarrow f_{m+1} = g + \sum_{i=1}^m b_i x^{d_{m+1}-d_i} f_i \in (f_1, \dots f_m), \text{ contradiction } \square$$

2.2) Finitely generated algebras.

We proceed to a generalization of the Hilbert basis Thm.

Definition: Let B be a (commutative) A-algebra (= ring w. fixed homomorphism from A) Then B is called finitely generated (as an A-algebra) if $\exists\, b_1, \dots b_k \in B$ s.t. $\forall b \in B$ $\exists\, F \in A[x_1, \dots x_k]$ s.t. $b = F(b_1, \dots b_k)$.

Hence $\varphi: A[x_1, \dots x_k] \longrightarrow B$, $F \mapsto F(b_1, \dots b_k)$, is surjective. So B is fin gen'd A-algebra $\Leftrightarrow \exists\, k \mid B \simeq$ a ring quotient of $A[x_1, \dots x_k]$

Corollary: Let A be Noetherian & B be a finitely generated A-algebra. Then B is a Noetherian ring.

Proof: Use Hilbert's Thm k times to see that $A[x_1, \dots x_k]$ is Noetherian. Let $I \subset B$ be ideal, need to show it's fin. gen'd
$J := \varphi^{-1}(I) \subset A[x_1, \dots x_k]$ is ideal so $J = (F_1, \dots F_\ell)$. But then
$I = \varphi(J) = (\varphi(F_1), \dots \varphi(F_\ell))$ is finitely generated $\square$

Since fields & $\mathbb{Z}$ are Noetherian rings, any finitely generated algebra over those are Noetherian. This is one (but not the only) source of Noetherian rings.

3) Further properties of Noetherian modules.

Let A be a ring (may not be Noetherian) & M be A-module.
The following result compares the property of being Noetherian for M & its subs & quotients.

Proposition: Let $N \subset M$ be a submodule. TFAE

(1) M is Noetherian

(2) Both N, M/N are Noetherian.

We'll prove it in the next lecture, for now let's deduce a Corollary.

Corollary: Assume A is Noetherian. TFAE:

a) M is Noetherian

b) M is finitely generated.

Proof:

a) $\Rightarrow$ b) follows from definition of Noetherian modules

b) $\Rightarrow$ a): we do induction on the number of generators, k, of M. If $k=1$, then $M = \mathrm{Span}_A(m_1) \Leftrightarrow A \twoheadrightarrow M$ via $a \mapsto am_1$. Since A is Noetherian, so is M by (1) $\Rightarrow$ (2) of Proposition.

Now suppose every A-module generated by k elements is Noetherian & $M = \mathrm{Span}_A(m_1, \ldots m_{k+1})$. Take $N = \mathrm{Span}_A(m_1, \ldots m_k) \subset M$, Noetherian by induction. Note that M/N is generated by $m_i + N$ ($i = 1, \ldots k+1$) by Rem. 2) in Sec 3.1 of Lec 4. But only $m_{k+1} + N \neq 0$, so M/N is spanned by one elt hence Noetherian. By (2) $\Rightarrow$ (1) of Proposition, M is Noetherian. $\square$

BONUS I: Non-Noetherian rings in Complex analysis.

Most of the rings we deal with in Commutative algebra are Noetherian. Here is, however, a very natural example of a non-Noetherian ring that appears in Complex analysis.

Complex analysis studies holomorphic (a.k.a. complex analytic or complex differentiable) functions. Let $Hol(\mathbb{C})$ denote the set of holomorphic functions on $\mathbb{C}$. These can be thought as power series that absolutely converge everywhere.

$Hol(\mathbb{C})$ has a natural ring structure - via addition & multiplication of functions.

Proposition: $Hol(\mathbb{C})$ is not Noetherian

Proof: We'll produce an AC of ideals: $I_j = \{f(z) \in Hol(\mathbb{C}) \mid f(2\pi\sqrt{-1}k) = 0 \ \forall$ integer $k \geq j\}$, $j \in \mathbb{Z}_{\geq 0}$. It's easy to check that all of these are indeed ideals. It is also clear that they form an AC (when we increase j we relax the condition on zeroes). We claim that $I_j \subsetneq I_{j+1}$ hence this AC doesn't terminate & $Hol(\mathbb{C})$ is not Noetherian. Equivalently, we need to show that, for each j, there $f_j(z) \in Hol(\mathbb{C})$ such that $f_j(2\pi\sqrt{-1}k) = 0 \ \forall k \geq j$ while $f_j(2\pi\sqrt{-1}j) \neq 0$.

Consider the function $f(z) = e^z - 1$. This function is periodic with period $2\pi\sqrt{-1}$. Also $f(z) = \sum_{i=1}^{\infty} \frac{1}{i!} z^i$. So $z=0$ is an order 1 zero of $f(z)$. Since $2\pi\sqrt{-1}$ is a period, every $2\pi\sqrt{-1}k$

$(k \in \mathbb{Z})$ is an order 1 zero. We set
$f_j(z) = (e^z - 1)/(z - 2\pi\sqrt{-1}j)$. This function is still holomorphic on the entire $\mathbb{C}$, we have $f_j(2\pi\sqrt{-1}j) \neq 0$ & $f_j(2\pi\sqrt{-1}k) = 0$ for $k \neq j$. $\square$

BONUS II: Why did Hilbert care about the Basis theorem

Hilbert was interested in Invariant theory, one of the central branches of Mathematics of the 19th century. Let G be a group acting on fin. dim $\mathbb{C}$-vector space V by linear transformations, $(g,v) \mapsto gv$. We want to understand when two vectors v_1, v_2 lie in the same orbit.

Definition: A function $f: V \to \mathbb{C}$ is *invariant* if f is constant on orbits: $f(gv) = f(v)$ $\forall g \in G, v \in V$.

Exercise: $v_1, v_2 \in V$ lie in the same orbit $\Leftrightarrow f(v_1) = f(v_2)$ $\forall$ invariant function f. (we say: G-invariants separate G-orbits).

Unfortunately, all invariant functions are completely out of control. However, we can hope to control polynomial functions. Those are functions that are written as polynomials in coordinates of v in a basis (if we change a basis, then coordinates change via a linear transformation, so if a function is a polynomial in one basis, then it's a polynomial in every basis). The $\mathbb{C}$-algebra

of polynomial functions will be denoted by $\mathbb{C}[V]$, if $\dim V = n$, then a choice of basis identifies $\mathbb{C}[V]$ with $\mathbb{C}[x_1, \dots x_n]$.
By $\mathbb{C}[V]^G$ we denote the subset of G-invariant functions in $\mathbb{C}[V]$.

Exercise: It's a subring of $\mathbb{C}[V]$.

Example 1: Let $V = \mathbb{C}^n$, $G = S_n$, the symmetric group, acting on V by permuting coordinates. Then $\mathbb{C}[V]^G$ consists precisely of symmetric polynomials.

Example 2: Let $V = \mathbb{C}^n$ & $G = \mathbb{C}^\times$ ($= \mathbb{C} \setminus \{0\}$ w.r.t. multiplication)
Let G act on V by rescaling the coordinates: $t.(x_1, \dots x_n) = (tx_1, \dots tx_n)$. We have $f(x_1, \dots x_n) \in \mathbb{C}[V]^G \Leftrightarrow f(tx_1, \dots tx_n) = f(x_1, \dots x_n)$ $\forall\, t \in \mathbb{C}^\times$, $x_1, \dots x_n \in \mathbb{C}$. This is only possible when f is constant.

As Example 2 shows polynomial invariants may fail to separate orbits. However, to answer our original question, it's still worth to study polynomial invariants.

Premium exercise: When G is finite, the polynomial invariants still separate G-orbits.

Now suppose we want to understand when, for $v_1, v_2 \in V$, we have $f(v_1) = f(v_2)$ $\forall\, f \in \mathbb{C}[V]^G$ It's enough to check this for generators f of the $\mathbb{C}$-algebra $\mathbb{C}[V]^G$. So a natural question is whether this algebra is finitely generated.

Hilbert proved this for "reductive algebraic" groups G – he didn't know the term but this is what his proof uses. Finite groups are reductive algebraic and so are $GL_n(\mathbb{C})$, the group of all nondegenerate matrices, $SL_n(\mathbb{C})$, matrices of determinant 1, $O_n(\mathbb{C})$, orthogonal matrices, and some others (for these infinite groups one needs to assume that their actions are "reasonable" – in some precise sense). Later, mathematicians found examples, where the algebra of invariants are not finitely generated (counterexamples to Hilbert's 14th problem) for non-reductive groups.

Basis theorem is an essential ingredient in Hilbert's proof of finite generation. For more details on this see [E], 1.4.1 & 1.5.; 1.3 contains some more background on Invariant theory.