Lecture 5, Noetherian rings & modules, I.

0) Modules wrapped up: free & projective modules.
1) Noetherian rings & modules
2) Hilbert's Basis theorem.

References: [AM], Chapter 6, intro to Chapter 7; [E], Section 1.4.

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

0.1) Free modules.

Let A be a commutative ring & M be an A-module.

Definition: • Elements $m_i, i\in I$, form a basis in M if $\forall m\in M$ is uniquely written as A-linear combination of $m_i, i\in I$.
• M is free if it has a basis.

Examples: 1) For any set I, $A^{\oplus I}$ is free, for a basis can take coordinate vectors $e_i, i\in I$: $e_i=(0,..,0,1,0...)$ (1 in the ith position)

2) If A is field, then every module (a.k.a. vector space) is free. If A is not a field, there are non-free modules: let $J\subset A$ be ideal, $J\neq \{0\}, A$ $\Rightarrow$ A/J is not free (over A). Indeed, for any vector e in a basis we must have $ae\neq 0$ $\forall a\in A$. But for any $e\in A/J$ we have $ae=0$ $\forall a\in J$.

Remark: Every free module is isomorphic to $A^{\oplus I}$ for some set I: choose basis $m_i \in M$ $(i \in I)$: $\varphi_{\underline{m}}: A^{\oplus I} \xrightarrow{\sim} M$.

Lemma: Every basis in $M = A^{\oplus k}$ has exactly k elements.

Proof: Assume the contrary: $\exists\, \ell \neq k$ w. $A^{\oplus k} \xrightarrow{\sim} A^{\oplus \ell}$. As in the case of fields, any A-linear map $A^{\oplus k} \to A^{\oplus \ell}$ is given by multiplication w. uniquely determined $\ell \times k$-matrix w. coeff's in A. Also for $T \in Mat_k(A)$, the map $\vec{v} \mapsto T \cdot \vec{v}: A^{\oplus k} \to A^{\oplus k}$ is invertible $\Leftrightarrow$ $\det(T) \in A$ is invertible. WLOG, assume $k > \ell$ and let isomorphisms $A^{\oplus k} \xrightarrow{\sim} A^{\oplus \ell}$, $A^{\oplus \ell} \xrightarrow{\sim} A^{\oplus k}$ be given by $T_1 \in Mat_{\ell,k}(A)$, $Mat_{k,\ell}(A)$. So $\det(T_2 T_1) = 0$ b/c rows of $T_2 T_1$ are A-linear combinations of the ℓ rows of T_1 & $\ell < k$ $\square$

0.2) Why to care about modules; projective 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 ($\mathbb{F}[x_1, \ldots x_n]$-modules).

Reason 1: modules provide a general framework for discussing 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: there's an interesting (from various perspectives) class of modules: projective ones.

Definition: An A-module P is *projective* if $\exists$ A-module P' s.t. $P \oplus P'$ is free.

Example: Free $\Rightarrow$ projective (take $P' = \{0\}$).

However, there are projective modules that aren't free, see Prob 7 in HW1.

One can ask whether, for given ring A, all of its finitely generated projective modules are free. Here's a sufficient cond'n.

Thm (Quillen, answering question of Serre): If $A = \mathbb{F}[x_1, \ldots x_n]$, where $\mathbb{F}$ is a field, then any fin. generated projective module is free.

The main reason why people care about finitely generated projective modules is that they are important geometrically (they correspond to vector bundles on affine schemes). We'll study projective modules from various perspectives.

1) Noetherian rings & modules.

A is comm've ring.

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. We are going to study the condition on modules (and the ring A itself) that guarantees that this doesn't happen).

1.1) Main definitions & examples.

Definition:

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.

Non-example: see Prob 3 in HW1 (inf. generated ideal in certain A).

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 $N_j = N_k$ $\forall j \geq k$.

Proposition: For an A-module M TFAE:

1) M is Noetherian.
2) $\forall$ 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. $N \not\subset N'$ for $N' \in X, N' \neq N$).

Proof: 2) $\Rightarrow$ 3): Let X be a set of submodules. Take $M_1 \in X$. It's not maximal $\Rightarrow \exists M_2 \in X$ w. $M_1 \subsetneq M_2$; M_2 isn't max'l $\Rightarrow \exists M_3 \supsetneq M_2$. Etc.

3) $\Rightarrow$ 2): exercise.

(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 (exercise). This N is fin. gen'd so $\exists m_1, \dots m_\ell \in N$ w. $N = \mathrm{Span}_A(m_1, \dots m_\ell)$. Now $m_i \in N_{k(i)}$ for some $k(i) \Rightarrow m_1, \dots m_\ell \in N_k$ for $k = \max\{k(i)\}$ b/c $N_{k(i)} \subset N_k$ thx to AC condition $\Rightarrow$ $N = \mathrm{Span}_A(m_1, \dots m_\ell) = N_k$ so AC (N_i) terminates at N_k.

$(2) \Rightarrow (1)$. Know: $\forall$ AC of submodules terminates. Let N be a submodule that is <u>not</u> fin generated: construct N_i's by induction: pick $m_1 \in N \rightsquigarrow N_1 = \mathrm{Span}_A(m_1) = Am_1$. Now suppose we've constructed $m_1, \dots m_i \in N$ & $N_i = \mathrm{Span}_A(m_1, \dots m_i)$. N is not fin.gen. $\Rightarrow N \neq N_i \Rightarrow \exists\, m_{i+1} \in N \setminus N_i$, set $N_{i+1} = \mathrm{Span}_A(m_1, \dots m_{i+1}) \supsetneq N_i$. So $(N_i)_{i>0}$ is AC, doesn't terminate. Contradiction. $\square$

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.

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 $A[x]$ is Noetherian.

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.

For $k > 0$, define $a_k \in A$ & $n_k \in \mathbb{Z}_{\geq 0}$ from $f_k = a_k X^{n_k} +$ lower deg. terms. By the construction, $n_1 \leq n_2 \leq \dots \leq n_k \leq \dots$ Now let $I_k = (a_1, \dots a_k) \subset A$, $k > 0$. This is an ascending chain of ideals in A. Since A is Noetherian, it must terminate. So $a_{m+1} \in (a_1, \dots a_m) \Leftrightarrow a_{m+1} = \sum_{i=1}^{m} b_i a_i$, $b_i \in A$, for some m.

Set $g_{m+1} = f_{m+1} - \sum_{i=1}^{m} b_i X^{n_{m+1} - n_i} f_i = \in I$ b/c $f_1, \dots f_{m+1} \in I$ & $n_{m+1} - n_i \geq 0$

$= \underbrace{(a_{m+1} - \sum_{i=1} b_i a_i)}_{=0} X^{n_{m+1}} +$ lower deg. terms $\Rightarrow \deg g_{m+1} < \deg f_{m+1}$

So by the choice of f_{m+1} - of minimal degree in $I \setminus (f_1, \dots, f_m)$ $g_{m+1} \in (f_1, \dots f_m) \Rightarrow f_{m+1} \in (f_1, \dots f_m)$, contradiction $\square$

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 $k \geq j\}$, $j \in \mathbb{Z}_{>0}$. 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 $f_j(2\pi\sqrt{-1}k) = 0 \ \forall k > j$ 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).

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.