Lecture 6.

1) Proof of Hilbert's Basis theorem
2) Artinian modules & rings.
3) Finite length modules.

Bonuses: why did Hilbert care about the Basis thm; More on finite length modules

References: [AM], Chapter 6, Chapter 7, introduction.

1) Recall, a ring A is Noetherian if $\forall$ ideal is fin. gen'd, equiv'ly "AC condition" holds: $\forall$ AC (ascending chain) of ideals in A terminates.

Thm (Hilbert): If A is Noetherian, then $A[x]$ is Noetherian.

Proof: Notation: $I\subset A[x]$, ideal, need to show it's fin gen'd.
For $k\in \mathbb{Z}_{\geqslant 0} \rightsquigarrow A[x]_{\leqslant k}=\{\sum_{i=0}^{k} a_i x^i\in A[x]\}$ is an A-submodule of $A[x]$, $A[x]_{\leqslant k}\simeq A^{\oplus k+1}$ (as A-module)
$I_{\leqslant k}=I\cap A[x]_{\leqslant k}$, an A-submodule in $A[x]_{\leqslant k}$.
$I_k=\{a\in A \mid$ s.t. $\exists$ ax^k+ lower deg. terms $\in I\}$

Step 1: Claim: $I_k\subset A$ is an ideal. Indeed, $0\in I_k$; $a\in I_k, b\in A$ $\Rightarrow ba\in I_k$ b/c ax^k+ low. deg. terms $\in I\Rightarrow b(ax^k+\dots)\in I$; $a,a'\in I_k\Rightarrow a+a'\in I_k$ (exercise).

Step 2: $I_k\subseteq I_{k+1}$: $a\in I_k\Rightarrow ax^k+\dots\in I\Rightarrow \underbrace{x(ax^k+\dots)}_{=ax^{k+1}+\dots}\in I$
$\Rightarrow a\in I_{k+1}$.

Conclude $(I_k)_{k\geqslant 0}$ form an AC of ideals, must terminate: $\exists$ $m\geqslant 0$ s.t. $I_k=I_m$ $\forall$ $k\geqslant m$. Let $a_1,\dots a_\ell$ be generators of I_m & $f_i=a_ix^m+\dots$ be elements of $I_{\leqslant m}$ (only care about top. coeff's)

Step 3: Look at $I_{\leq m-1} \subset A[x]_{\leq m-1} \simeq A^{\oplus m}$ - finitely generated $\Rightarrow$ [A is Noeth'n] $A^{\oplus m}$ is Noetherian (Cor. from Lec 5) $\Rightarrow$ $I_{\leq m-1}$ is fin. gen'd. Pick generators $g_1, \dots, g_e \in I_{\leq m-1}$ (as A-module)

Final claim: $I = (f_1, \dots f_\alpha, g_1, \dots g_e)$

Step 4: (proof of this claim) assume the contrary: $\exists f \in I \setminus (f_1, \dots f_\alpha, g_1, \dots g_e)$. Assume that f has minimal degree among all such elements, let this deg be p. Note $p \geq m$, otherwise $f \in \mathrm{Span}_A(g_1, \dots g_e)$. So $f = ax^p +$ low. deg. terms, $a \in I_p = I_m$. $= \mathrm{Span}_A(a_1, \dots a_\alpha) \Rightarrow a = \sum_{i=1}^{\alpha} b_i a_i$

$$\underbrace{f(x) - x^{p-m} \sum_{i=1}^{\alpha} b_i f_i(x)} = (\underbrace{a - \sum_{i=1}^{\alpha} b_i a_i}_{=0}) x^p + \text{low. deg. terms}$$

$\in I$, has deg $< p \Rightarrow$ it lies in $(f_1, \dots f_\alpha, g_1, \dots g_e)$ by choice of p

$$f(x) = \underbrace{(f(x) - x^{p-m} \sum b_i f_i(x))}_{\in (f_1, \dots f_\alpha, g_1, \dots g_e)} + \underbrace{x^{p-m} \sum b_i f_i(x)}_{\in (f_1, \dots f_\alpha, g_1, \dots g_e)}$$

So $f(x) \in (f_1, \dots f_\alpha, g_1, \dots g_e)$

Contr'n w. choice of f, finishes the proof $\square$

2.1) Artinian modules

Noetherian $\Leftrightarrow$ satisfies AC condition

Definition: Let M be A-module. A descending chain (DC) of submodules is $(N_i)_{i \geq 0}$ s.t. $N_k \supseteq N_{k+1}$ $\forall k \geq 0$.

Definition: M is an Artinian A-module if $\forall$ DC of submodules terminates (DC condition)

Example: $A = \mathbb{F}$ (a field). Claim: Artinian $\Leftrightarrow$ finite dim'l.

$\Leftarrow$ is clear b/c dimensions decrease in DC's.

$\Rightarrow$ let $\dim M = \infty \Leftrightarrow M$ has basis, e_i, $i \in I$, where I is infinite. Since I is infinite $\exists$ subsets $I_1 \supsetneq I_2 \supsetneq I_3 \supsetneq \dots$ (infinite chain of subsets). Define $M_j = \mathrm{Span}_{\mathbb{F}}(e_i \mid i \in I_j)$ – a DC of subspaces that doesn't terminate.

Basic properties (compare to Propositions 1,2 from Lecture 5).

Proposition 1: For A-module M TFAE:

1) M is Artinian

2) $\forall$ nonempty set of submodules of M has a <u>minimal</u> el-t (w.r.t. $\subset$)

Proposition 2: M is A-module, $N \subset M$ is an A-submodule. TFAE:

1) M is Artinian.

2) Both N & M/N are Artinian.

Proofs: repeat those in Noeth'n case (exercise).

2.2) Artinian rings.

Definition: A ring A is <u>Artinian</u> if it's Artinian as A-module.

Examples: 1) Any field is Artinian.

2) Let $\mathbb{F}$ be a field, A be an $\mathbb{F}$-algebra s.t. $\dim_{\mathbb{F}} A < \infty$. Then A is Artinian ring (b/c A-submodule is a subspace).

3) $A = \mathbb{Z}/n\mathbb{Z}$ Artinian (b/c it's a finite set so every DC of subsets terminates)

4) Let A be a domain. Then A is Artinian $\Rightarrow$ A is a field. Indeed, let $a \in A$ be noninvertible:

$(a) \supsetneq (a^2) \supsetneq (a^3) \supsetneq \ldots$ a DC of ideals that doesn't terminate.

b/c a is not divisible by a^2: $a = a^2 b \Rightarrow 1 = ab$

Thm: Every Artinian ring is Noetherian.

For proof, see [AM], Prop 8.1 - Thm 8.5 (comments: nilradical $= \sqrt{0} =$ $= \bigcap$ all prime ideals by Prop. 1.8, Jacobson radical $= \bigcap$ all max. ideals).

3) Finite length modules.

Thm motivates us to consider modules that are both Noetherian (AC condition) & Artinian (DC condition) so satisfy ("AC/DC" condition). They admit an equivalent charact'n.

Definition: Let M be an A-module.

i) Say that M is simple if $\{0\} \neq M$ are the only two submodules of M.

ii) Let M be arbitrary. By a filtration (by submodules) on M we mean $\{0\} = M_0 \subset M_1 \subset M_2 \subset \ldots \subset M_k = M$ (finite AC of submodules).

iii) A Jordan-Hölder (JH) filtr'n is a filtr'n $\{0\} = M_0 \subsetneq M_1 \subsetneq M_2 \subsetneq \ldots \subsetneq M_k = M$ s.t. M_i / M_{i-1} is simple $\forall i$. (so a JH filtr'n is "tightest possible")

iv) M has finite length if a JH filtr'n exists.

Proposition: For an A-module M TFAE:

1) M is Artinian & Noetherian.
2) M has finite length.

Proof: $2) \Rightarrow 1)$: M has fin. length $\rightsquigarrow$ JH filtr'n $\{0\} = M_0 \subsetneq M_1 \subsetneq M_2 \subsetneq \ldots \subsetneq M_k = M$. We prove by induction on i that M_i is Artinian & Noetherian.

Base: $i=1$: M_1 is simple $\Rightarrow$ Artinian & Noetherian.

Step: $i-1 \rightsquigarrow i$: M_{i-1} is Art'n & Noeth'n, so is M_i/M_{i-1} b/c it's simple. $\Rightarrow$ by Prop'ns 2 from this lecture & Lec 5 $\Rightarrow M_i$ is Artinian & Noetherian. Use this for $i=k \rightsquigarrow M_i = M$.

So $2) \Rightarrow 1)$.

$1 \Rightarrow 2)$: M is Artinian & Noetherian. Want to produce a JH filtr'n. By induction: $M_0 = \{0\}$.

Suppose we've constr'd $M_i \subset M$. Need M_{i+1}.

Note: M/M_i is Artinian & therefore $\forall$ nonempty set of submodules has a min el't. Assume $M_i \neq M$. Consider the set of all <u>nonzero</u> submodules of M/M_i. It's $\neq \emptyset$ so has a min'l element, N. This N must be simple. Now take M_{i+1} to be the preimage of N under $M \twoheadrightarrow M/M_i$.

So $M_{i+1}/M_i \simeq N$, simple.

We've got is an AC $M_0 \subsetneq M_1 \subsetneq M_2 \subsetneq \ldots$, it must terminate b/c M is Noeth'n. So we've got a JH filtr'n $\square$

BONUS 1: 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 <u>invariant</u> 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 $f(x_1, \dots x_n) \in \mathbb{C}[V]^G \iff f(tx_1, \dots tx_n) = f(x_1, \dots x_n)$ $\forall\, t \in \mathbb{C}^\times$, $x_1, \dots x_n \in \mathbb{C}$. 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.

BONUS 2: Here are some more results on finite length modules. Now A is a noncommutative unital ring and M is its finite length module - all definitions we've made still make sense

Jordan-Hölder thm: For two JH filtrations $\{0\}=M_0\subsetneq M_1\subsetneq\ldots\subsetneq M_k=M$ & $\{0\}=M_0'\subsetneq M_1'\subsetneq\ldots\subsetneq M_\ell'=M$ have $k=\ell$ & the collection $(M_i/M_{i-1})_{i=1}^k$ coincides with $(M_i'/M_{i-1}')_{i=1}^k$ up to a permutation.

Now here's another uniqueness statement that looks similar to the JH theorem but is of different nature.

Definition: We say M is <u>indecomposable</u> if it's not isomorphic to the direct sum of nonzero modules

Exercise: Let M be a finite length module. Then it's isomorphic to the direct sum of some indecomposable modules.

Krull-Schmidt theorem. Let M be a finite length A-module. Let $M\simeq N_1\oplus\ldots\oplus N_k\simeq N_1'\oplus\ldots\oplus N_\ell'$ be two decompositions into indecomposables. Then $k=\ell$ & the collection $(N_i')_{i=1}^k$ is obtained from $(N_i)_{i=1}^k$ by a permutation (not as submodules of M but as modules - up to isomorphism).