Lecture 6.

1) Proof of Hilbert's Basis theorem
   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 every ideal is fin. gen'd, equivalently, AC condition holds: No AC (ascending chain) of ideals in $A$ terminates.

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

Proof: Notation: $I \subseteq A[x]$, ideals, need to show it's fin. gen'd.

For $k \in \mathbb{Z} \geq 0 \Rightarrow A[x]_{\leq k} = \{ \sum_{i=0}^{k} a_i x^i \in A[x] \}$ is an $A$-submodule of $A[x]$, $A[x]_{\leq k} \subseteq A^{\oplus k+1}$ (as $A$-module).

$I_{\leq k} = I \cap A[x]_{\leq k}$, an $A$-submodule in $A[x]_{\leq k}.$

$I_k = \{ a \in A \mid \text{s.t. } \exists \ a x^k \text{ + lower deg. terms } \in I \}$

Step 1: Claim: $I_k \subseteq A$ is an ideal. Indeed, $0 \in I_k$; $a \in I_k, b \in A \Rightarrow b a \in I_k$ by $a x^k \text{ + lower deg. terms } \in I \Rightarrow b (a x^k \ldots) \in I$.

$a, a' \in I_k \Rightarrow a + a' \in I_k$ (exercise).

Step 2: $I_k \subseteq I_{k+1}$: $a \in I_k \Rightarrow a x^{k+\ldots} \in I \Rightarrow x (a x^k \ldots) \in I \Rightarrow a x^{k+\ldots} \in I_{k+1}$.

Conclusion: $(I_k)_{k\geq 0}$ form an NC of ideals, must terminate: $\exists m > 0 \text{ s.t. } I_k = I_m \ \forall k > m.$ Let $a_1, \ldots, a_l$ be generators of $I_m$.

$\frac{f_i}{a_i} = a_i x^m \ldots$ be elements of $I_{\leq m}$ (only care about top coeff's).
Step 3: Look at \( I_{m-1} \subseteq A[x] \subseteq A^m \) finitely generated

\[ \Rightarrow [A \text{ is Noetherian}] \ A^m \text{ is Noetherian (Cor. from Lec S)} \Rightarrow \]

\( I_{m-1} \) is fin. gen'd. Pick generators \( g_1, \ldots, g_e \in I_{m-1} \) (as \( A \)-module)

Final claim: \( I = (f_1, \ldots, f_d, g_1, \ldots, g_e) \)

Step 4: (proof of this claim) assume the contrary: \( \exists f \notin \]

\( I \setminus (f_1, \ldots, f_d, g_1, \ldots, g_e) \). Assume that \( f \) has minimal degree among

all such elements, let this deg be \( p \). Note \( p \geq m \), otherwise

\( f \in \text{Span}_A (g_1, \ldots, g_e) \). So \( f = a_0 + \text{low deg terms}, a \in I_p = I_m \\
= \text{Span}_A (a_1, \ldots, a_d) \Rightarrow a = \sum b_i a_i \)

\[ f(x) = x^{p-m} \sum_{i=1}^d b_i f_i(x) = \left( a - \sum_{i=1}^d b_i a_i \right) x^p + \text{low deg. terms} \]

\[ \in I, \text{ has deg } < p \Rightarrow \text{it lies in } (f_1, \ldots, f_d, g_1, \ldots, g_e) \text{ by choice of } p \]

\[ f(x) = (f(x) - x^{p-m} \sum b_i f_i(x)) + x^{p-m} \sum b_i f_i(x) \]

\( \in (f_1, \ldots, f_d, g_1, \ldots, g_e) \) So \( f(x) \in (f_1, \ldots, f_d, g_1, \ldots, g_e) \)

Contr'n w. choice of \( f \), finishes the proof \( \Box \)

2.1) Artinian module.

Noetherian \( \iff \) satisfies AC condition

Definition: let \( M \) be \( A \)-module. A descending chain (DC) of submodules is \((N_i)_{i \geq 0}\) s.t. \( N_i \supseteq N_{i+1} \forall k \geq 0 \)
Definition: $M$ is an Artinian $A$-module if $\mathcal{H}$ DC of submodules terminates (DC condition).

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

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

$\Rightarrow$ let $\dim M = \infty \iff M$ has basis, $e_i, i \in I$, where $I$ is infinite. Since $I$ is infinite, $\exists$ subsets $I_1 \supseteq I_2 \supseteq I_3 \supseteq \ldots$ (infinite chain of subsets). Define $M_j = \text{Span}_A(e_i | i \in I_j)$ - a DC of subspaces that don't terminate.

Basic properties (compare to Propositions 1,2 from Lecture 5). Proposition 1: For $A$-module $M$ TFAE:

1) $M$ is Artinian

2) If nonempty set of submodule of $M$ has a minimal elt (w.r.t. $\subseteq$)

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

TFAE: 1) $M$ is Artinian.

2) Both $N$ & $M/N$ are Artinian.

Proofs: repeat those in Noetherian case (exercise)

2.2) Artinian rings.

Definition: A ring $A$ is Artinian 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 (bc $A$-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 \( \implies A \) is a field. Indeed, let \( a \in A \) be noninvertible:

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

\( \because a \) is not divisible by \( a^2 \): \( a = a^2 b \implies 1 = ab \)

Thm: Every Artinian ring is Noetherian
For proof, see [AM], Prop 8.1-Thm 8.5 (comments: nilradical = \( \sqrt{0} = \cap \) all prime ideals by Prop 1.8, Jacobson radical = \( \cap \) all max ideals)

3) Finite length module
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'rn.

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 submodule) 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 \( \{0\} = M_0 \neq M_1 \neq M_2 \neq \ldots \neq M_k = M \) s.t. \( M_i/M_{i-1} \) is simple \( \forall i \).

(\( \because \) 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 $\Rightarrow$ IH filtr'n
$\{0\} = M_0 \triangleright M_1 \triangleright M_2 \triangleright \ldots \triangleright M_k = M$. We prove by induction on $i$ that $M_i$ is Artinian & Noetherian

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

Step: $i-1 \sim i$: $M_{i-1}$ is Art'n & Noeth'n, so is $M_i/M_{i-1}$

b/c it's simple. $\Rightarrow$ by Prop'n 2 from this lecture & Lec 5 $\Rightarrow M_i$ is Artinian & Noetherian. Use this for $i=k \sim M_k = M$.

So 2) $\Rightarrow$ 1).

1$\Rightarrow$2): $M$ is Artinian & Noetherian. Want to produce a IH 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 $\neq M$. Consider the set of all nonzero 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 $M \rightarrow M/M_i$.

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

We've got an AC $M_0 \triangleright M_1 \triangleright M_2 \triangleright \ldots$, it must terminate

b/c $M$ is Noeth'n. So we've got a IH filtr'n \hfill \Box

**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 a finite-dimensional $k$-vector space $V$ by linear transformations, $(gv) = gx\).

We want to understand when two vectors $v, v_0 \in V$ lie in the same orbit.

**Definition:** A function $f : V \rightarrow C$ is invariant if $f$ is constant on orbits: $f(gv) = f(v) \iff g \in G, v \in V.$

**Exercise:** $v, v_0 \in V$ lie in the same orbit $\iff f(v) = f(v_0) \iff$ 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 $k$-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 $\mathbb{C}[x_1, \ldots , x_n].$ 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 $V = C^n$, $G = S_n$, the symmetric group, acting on $V$ by permuting coordinates. Then $\mathbb{C}[V]^G$ consists precisely of symmetric polynomials.

**Example 2:** Let $V = C^n$ & $G = C^* (= C \setminus \{0\}$ w.r.t. multiplication)

Let $G$ act on $V$ by rescaling the coordinates: $t_i(x_1, \ldots , x_n) = \frac{x_i}{x_1}$
\((x_{i_1}, \ldots, x_{i_n})\). We have \(f(x_{i_1}, \ldots, x_{i_n}) \in \mathbb{C}[V]^G \iff f(tx_{i_1}, \ldots, tx_{i_n}) = f(x_{i_1}, \ldots, x_{i_n})\)

\(\forall t \in \mathbb{C}, x_{i_1}, \ldots, x_{i_n} \in \mathbb{C}\). 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 \(G\)'s orbits.

Now suppose we want to understand when, for \(u, v \in V\), we have \(f(u) = f(v)\) \(\forall f \in \mathbb{C}[V]^G\). 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 non-degenerate 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 18th problem).

Basis theorem is an essential ingredient in Hilbert’s proof of finite generation. For more details on this see [E], 19.1 & 15; 13 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 filtrations

$$0 \subseteq M_0 \triangleleft M_1 \triangleleft \cdots \triangleleft M_k = M \quad \text{and} \quad 0 \subseteq M'_0 \triangleleft M'_1 \triangleleft \cdots \triangleleft M'_k = M$$

have $k = l$ & 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 *indecomposable* 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

$$M \cong N_1 \oplus \cdots \oplus N_k = N'_1 \oplus \cdots \oplus N'_l$$

be two decompositions into indecomposables. Then $k = l$ & the collection $\{N'_i\}_{i=1}^l$ is obtained from $\{N_i\}_{i=1}^k$ by a permutation (not as submodules of $M$ but as modules—up to isomorphism).