Commutative Algebra

lecture 5: Primary decomposition

Misha Verbitsky

IMPA, sala 2

January 12, 2022

Radical ideals

DEFINITION: Let $\mathfrak{u} \subset R$ be an ideal. A **radical** of $\mathfrak{u}$ is the ideal

$$\sqrt{\mathfrak{u}} := \{x \in R \mid x^n \in \mathfrak{u} \text{ for some } n \in \mathbb{Z}^{>0}.\}$$

An ideal $\mathfrak{u} \subset R$ is called **radical** if $\mathfrak{u} = \sqrt{\mathfrak{u}}$

REMARK: An ideal $\mathfrak{u} \subset R$ is radical if and only if $R/\mathfrak{u}$ **has no non-zero nilpotents**.

REMARK: Radical ideals in a finitely-generated ring $R = \mathcal{O}_A$ **are in bijective correspondence with algebraic subsets of A** (this is one of the forms of strong Hilbert Nullstellensatz).

CLAIM: An ideal $\mathfrak{u} \subset R$ is radical **if and only if it is an intersection of prime ideals.**

Proof. Step1: Prime ideals containing $\mathfrak{u}$ are the same as prime ideals in $R/\mathfrak{u}$. Therefore, it suffices to prove that **0 is a radical ideal if and only if it is an intersection of prime ideals.**

Step 2: The quotient $R/\mathfrak{u}$ **has no nilpotents if and only if** 0 **is intersection of all prime ideals in $R/\mathfrak{u}$** (Lecture 3). ■

Irreducible varieties (reminder)

DEFINITION: An affine variety A is called **reducible** if it can be expressed as a union $A = A_1 \cup A_2$ of affine varieties, such that $A_1 \not\subset A_2$ and $A_2 \not\subset A_1$. If such a decomposition is impossible, A is called **irreducible**.

CLAIM: An affine variety A is **irreducible** if and only if its ring of polynomial functions $\mathcal{O}_A$ **has no zero divizors.**

Proof: If $A = A_1 \cup A_2$ is a decomposition of A into a non-trivial union of subvarieties, choose a non-zero function $f \in \mathcal{O}_A$ vanishing at A_1 and g vanishing at A_2. The product of these non-zero functions vanishes in $A = A_1 \cup A_2$, **hence $fg = 0$ in $\mathcal{O}_A$.** Conversely, **if $fg = 0$, we decompose $A = V_f \cup V_g$.** ■

Primary ideals

DEFINITION: An ideal $\mathfrak{u}$ is called **primary** if $\sqrt{\mathfrak{u}}$ is a prime ideal.

PROPOSITION: Let $\mathfrak{u} \subset R = \mathcal{O}_A$ be an ideal, and $V_\mathfrak{u} \subset A$ its zero set. Then **$\mathfrak{u}$ is primary if and only if the algebraic variety $V_\mathfrak{u}$ is irreducible.**

Proof. Step1: By Hilbert Nullstellensatz, the annihilator ideal $\operatorname{Ann}_{V_\mathfrak{u}}$ coincides with $\sqrt{\mathfrak{u}}$. Indeed, $V_\mathfrak{u} = V_{\sqrt{\mathfrak{u}}}$, hence, by Hilbert Nullstellensatz, $\operatorname{Ann}_{V_{\sqrt{\mathfrak{u}}}} = \sqrt{\mathfrak{u}}$. However, $V_{\sqrt{\mathfrak{u}}} = V_\mathfrak{u}$, because $f(x) = 0 \Leftrightarrow f^n(f) = 0$. This gives

$$\operatorname{Ann}_{V_\mathfrak{u}} = \operatorname{Ann}_{V_{\sqrt{\mathfrak{u}}}} = \sqrt{\mathfrak{u}}.$$

Step 2: The variety $A = V_{\sqrt{\mathfrak{u}}}$ is irreducible if and only if $\mathcal{O}_A = \frac{\mathbb{C}[t_1, ..., t_n]}{\operatorname{Ann}_A}$ has no zero divisors, which is equivalent to $\operatorname{Ann}_A = \sqrt{\mathfrak{u}}$ being a prime ideal. ■

Irreducible ideals

DEFINITION: Suppose that J, and J_i are ideals in R, and J is represented as $J = \bigcap_i J_i$. The decomposition $J = \bigcap_i J_i$ is called **non-trivial** if $J_i \neq J$ and $J_i \not\subset J_j$ for all i, j. An ideal $J \subset R$ is called **irreducible** if it does not admit a non-trivial decomposition $J = \bigcap_i J_i$. **An irreducible decomposition** of J is a non-trivial decomposition $J = \bigcap_i J_i$, where all J_i are irreducible.

LEMMA: In a Noetherian ring R, **every ideal admits an irreducible decomposition**.

Proof: Let $\mathfrak{R}$ be the set of all ideals not admitting an irreducible decomposition, and J a maximal element in this set; it exists, because R is Noetherian, unless $\mathfrak{R}$ is empty. Since J is not irreducible, we can decompose J as $\bigcap_i J_i$, where all J_i are strictly bigger than J, hence admit an irreducible decomposition $J_i = \bigcap_j J_{ij}$. Then $J = \bigcap_{i,j} J_{ij}$ gives an irreducible decomposition for J. ■

Primary decomposition

LEMMA: An irreducible ideal $J \subset R$ in a Noetherian ring is primary.

Proof. Step1: Replacing R by R/J, we find that it suffices to show that 0 is primary when it is irreducible. Let $xy = 0$ be some non-trivial zero divisors in R, and $\mathfrak{A}(x^k) := \{z \in R \ \ |zx^k = 0\}$. Since the chain $\mathfrak{A}(x) \subset \mathfrak{A}(x^2) \subset ...$ stabilizes, we have $\mathfrak{A}(x^n) = \mathfrak{A}(x^{n+1})$ for some $n > 0$.

Step 2: The ideals (x^n) and (y) generated by x^n and y satisfy $(x^n) \cap (y) = 0$. Indeed, each $a \in (x^n) \cap (y)$ satisfies $a \in \mathfrak{A}(x) \cap (x^n)$, hence $a = bx^n$ and $bx^{n+1} = 0$, giving $b \in \mathfrak{A}(x^{n+1})$. Since $\mathfrak{A}(x^n) = \mathfrak{A}(x^{n+1})$, this implies $a = bx^n = 0$. Since 0 is irreducible, this implies $x^n = 0$, hence 0 is primary (all zero divisors are nilpotents). ∎

DEFINITION: We say that an ideal $J \subset R$ **admits a primary decomposition** if R is represented as an intersection of primary ideals.

THEOREM: (Noether-Lasker theorem)
Let R be a Noetherian ring. **Then every ideal $J \subset R$ admits a primary decomposition.**

Proof: Indeed, every ideal admits an irreducible decomposition, and irreducible ideals are primary. ∎

Emmy Noether

Amalie Emmy Noether (1882-1935).

Emanuel Lasker

Emanuel Lasker (1868-1941).

Group representations

DEFINITION: Representation of a group G is a homomorphism $G \longrightarrow GL(V)$. In this case, V is called **representation space**, and **a representation**.

DEFINITION: Irreducible representation is a representation having no G-invariant subspaces. **Semisimple representation** is a direct sum of irreducible ones.

Let V be a vector space over a field k. **The space of bilinear maps $V \times V \longrightarrow k$ is denoted $V^* \otimes V^*$.**

REMARK: If the group G acts on a vector space V, it G **acts on** $V^* \otimes V^*$ **as** $g(h)(x,y) = h(g^{-1}(x), g^{-1}(y))$, for any $g \in G$, $h \in V^* \otimes V^*$ and $x, y \in V$.

DEFINITION: A metric h (Euclidean or Hermitian) on a vector space V is called **G-invariant** if the corresponding tensor $h \in V^* \otimes V^*$ is G-invariant.

G-invariant metrics

CLAIM:
A sum of two Hermitian (Euclidean) metrics is Hermitian (Euclidean).
■

COROLLARY: Let V be a representation of a finite group (over $\mathbb{R}$ or $\mathbb{C}$). **Then V admits a G-invariant metric** (Hermitian or Euclidean).

Proof: Let h be an arbitrary metric, and $\frac{1}{|G|}\sum_{g\in G} g(h)$ its average over the G action. The previous claim implies that it is a metric. Since G acts on itself bijectively, interchanging all terms in the sum, **it is G-invariant.** ■

COROLLARY: Let $E \subset V$ be a subrepresentation in a finite group representation over $\mathbb{R}$ or $\mathbb{C}$. Then **V can be decomposed onto a direct sum of two G-representations $V = W \oplus W'$.**

Proof: Choose a G-invariant metric on V, and let $W^\perp$ be the orthogonal complement to W. Then $W^\perp$ is also G-invariant **(check this)**. This gives a decomposition $V = W \oplus W^\perp$. ■

COROLLARY: Any finite-dimensional representation of a finite group is semisimple. ■

Exact functors

DEFINITION: An **exact sequence** is a sequence of vector spaces and maps $... \longrightarrow A_1 \longrightarrow A_2 \longrightarrow A_3 \longrightarrow ...$ such the kernel of each map is the image of the previous one. A **short exact sequence** is exact sequence of form $0 \longrightarrow A \stackrel{i}{\longrightarrow} B \stackrel{j}{\longrightarrow} C \longrightarrow 0$. **Here "exact" means that i is injective, j surjective, and the image of i is the kernel of j.**

DEFINITION: A functor $A \longrightarrow FA$ on the category of R-modules or vector spaces is called **left exact** if any exact sequence $0 \longrightarrow A \longrightarrow B \longrightarrow C \longrightarrow 0$ is mapped to an exact sequence

$$0 \longrightarrow FA \longrightarrow FB \longrightarrow FC,$$

right exact if it is mapped to an exact sequence

$$FA \longrightarrow FB \longrightarrow FC \longrightarrow 0,$$

and **exact** if the sequence

$$0 \longrightarrow FA \longrightarrow FB \longrightarrow FC \longrightarrow 0$$

is exact.

Invariants and coinvariants

DEFINITION: Let G be a finite group, and V its representation. Define **the space of G-invariants** V^G as the space of all G-invariant vectors, and **the space of coinvariants** as the quotient of V by its subspace generated by vectors $v - g(v)$, where $g \in G, v \in V$.

CLAIM: Let V be an irreducible representation of G. **Then its invariants and co-ivariants are equal 0 if it is non-trivial, and equal V if it is trivial.**

COROLLARY: Let V be a semisimple representation of G. **Then $V_G = V^G$.**

EXERCISE: Prove that **the functor $V \longrightarrow V^G$ is left exact, and $V \longrightarrow V_G$ is right exact**.

COROLLARY: For any finite group G, the functor of G-invariants $V \longrightarrow V^G$ on the category of complex representations of G is exact.

REMARK: The averaging map

$$m \longrightarrow \frac{1}{|G|} \sum_{g \in G} g(m)$$

gives a projection of V to V^G, and the kernel of this map is the kernel of the natural projection $V \longrightarrow V_G$

Ring of invariants and quotient space

DEFINITION: Action of a group G on an affine manifold A is the action of G on the ring $\mathcal{O}_A$ of polynomial functions on A.

REMARK: By Strong Nullstellensatz, **this is the same as action of G on A by automorphisms.**

REMARK: We want to define the quotient space A/G as the algebraic variety associated with the invariant ring $\mathcal{O}_A^G$.

Problem # 1: We need to show that the ring $\mathcal{O}_A^G$ is finitely generated (Noether theorem).

Problem # 2: We need to identify the maximal ideals in $\mathcal{O}_A^G$ with the elements of the quotient set A/G.

Noether theorem (scheme of the proof)

THEOREM: Let R be a finitely generated ring over $\mathbb{C}$, and G a finite group acting on R by automorphisms. Then **the ring R^G of G-invariants is finitely generated**.

Scheme of the proof:

1. Noetheriannes of R is used to prove that R^G is Noetherian.

2. Prove that R^G is finitely generated for the ring of polynomials $R = \mathbb{C}[z_1, ..., z_n]$, where G acts on polynomials of degree 1 by linear automorphisms.

3. Deduce the general case from (2) and exactness of the functor $V \longrightarrow V^G$