Lecture 5-6: Commutative Noetherian rings and algebraic geometry

May 6, 2024

The remainder of the course will be spent on commutative algebra and elementary algebraic geometry, following Chapters 15 and 16 in DF. We will define Noetherian rings and show that any finitely generated algebra A over a field k is such a ring. Such algebras A are the main algebraic objects studied in algebraic geometry.

Definition; DF p. 656

A commutative ring R is called *Noetherian* if it satisfies the ascending chain condition on ideals; that is, given any chain of ideals $I_1 \subseteq I_2 \subseteq \cdots$ of R there is m such that $I_n = I_m$ for $n \geq m$.

It is not difficult to see that R is Noetherian if and only if every nonempty set of ideals in R has a maximal element under inclusion. Also R is Noetherian if and only if every ideal is finitely generated. Indeed, if R is Noetherian and I is an ideal, then we choose $x_1 \in I$; if this element fails to generate I, then choose $x_2 \in I, x_2 \notin (x_1)$; if x_1, x_2 fail to generate I, then choose $x_3 \in I, x_3 \notin (x_1, x_2)$,and so on, so that we have a strictly increasing chain $(x_1) \subset (x_1, x_2) \subset \cdots$. Since this last chain cannot be infinite, there must be $x_1, \ldots, x_n \in I$ generating I.

Conversely, if every ideal is finitely generated and $I_1 \subseteq I_2 \subseteq \cdots$ is an increasing chain of ideals, then the union I of the I_i is also an ideal; if this is generated by $x_1, \ldots, x_n$ with $x_j \in I_{r_j}$, then the maximum m of the r_j has $I_m = I = I_n$ for $n \geq m$, as desired. In particular, every PID is Noetherian. Next we have

Hilbert's Basis Theorem; see DF, p. 316

If R is Noetherian then so is the ring $R[x]$ of polynomials in one variable over R.

Proof.

Let $I \in R[x]$ be an ideal. Let $L = \{a_n \in R : \sum_{i=0}^{n} a_i x^i \in I\}$ consist of the set of leading coefficients of the polynomials in I. Given ℓ and m in L, say corresponding to polynomials of degrees r and s, respectively, then by multiplying one of these polynomials by a suitable power of x and adding it to the other one we get a polynomial in I with leading coefficient $\ell + m$, whence L is closed under addition; clearly it is also closed under multiplication by R, so it is an ideal and as such is finitely generated, say by $\ell_1, \ldots, \ell_n$, corresponding to polynomials $p_1, \ldots, p_n \in I$ of degrees $d_1, \ldots, d_n$. Letting N be the maximum of the d_i, we see that given any polynomial $p \in I$ of degree at least N, say with leading term $a_m x^m$ with $m \geq N$, we can subtract off a suitable combination of p_i times multiples of appropriate powers of x to get a polynomial q of lesser degree in I. Iterating this, we see that I is the sum of the ideal generated by the p_i and the intersection I_N of I with the set of polynomials of degree at most $N - 1$ in $R[x]$. □

Proof.

Identifying any polynomial $q = \sum_{i=0}^{N-1} r_i x^i \in I_N$ with the N-tuple $(r_0, \ldots, r_{N-1})$ (and allowing any r_i to be 0), we see that I_N may be regarded as an R-submodule S of R^N. Arguing by induction on N and peeling off the coordinates of R^N one at a time, we see that S is finitely generated over R, whence both I_N and I are as well. □

Let k be a field. As an immediate corollary, we deduce by induction on n that the polynomial ring $P_n = k[x_1, \ldots, x_n]$ in any number n of variables over k is Noetherian (DF, Corollary 4, p. 659), as is any quotient of P_n, that is, any finitely generated k-algebra.

Now assume that k is infinite. Polynomials are functions on k^n and two polynomials coincide if and only if they agree as functions on k^n. This last domain is usually denoted $\mathbf{A}^n$ in this context and called affine n-space. Given a subset S of P_n we can therefore form the (affine) algebraic set $\mathcal{Z}(S)$ of common zeros in $\mathbf{A}^n$ of the polynomials in S. Note that $\mathcal{Z}(S)$ coincides with $\mathcal{Z}(I)$, where I is the ideal generated by S; letting $f_1, \ldots, f_m$ be a finite generating set for I, we see that we are ultimately reduced to the case where $S = \{f_1, \ldots, f_m\}$ is finite. Given two finite subsets $S = \{f_1, \ldots, f_m\}, T = \{g_1, \ldots, g_r\}$, we observe that $\mathcal{Z}(S) \cup \mathcal{Z}(T) = \mathcal{Z}(\{f_i g_j : 1 \leq i \leq m, 1 \leq j \leq r\})$. Also if $S_1, S_2, \ldots$ are any subsets of P_n, then the intersection of the $\mathcal{Z}(S_i)$ is just $\mathcal{Z}(S)$, where S is the union of the S_i.

Finally, we note that $\mathbf{A}^n$ itself is $\mathcal{Z}\{0\}$, while the empty set is $\mathcal{Z}\{1\}$. Putting these properties together, we deduce that there is a topology on $\mathbf{A}^n$ for which the closed sets are exactly the algebraic sets: any finite union or arbitrary intersection of closed sets is closed. This topology is called the Zariski topology (see DF, p. 676); of course the Zariski open sets are just the complements of the closed ones. Any Zariski open subset of $\mathbb{R}^n$ or $\mathbb{C}^n$ is Euclidean open, since polynomials are continuous functions. Compared to the usual Euclidean topology on $\mathbb{R}^n$ or $\mathbb{C}^n$, it turns out that there are many fewer open sets in the Zariski topology and the nonempty open sets are much fatter.

For example, the only Zariski closed subsets of $\mathbb{R}$ or $\mathbb{C}$ apart from $\mathbb{R}$ or $\mathbb{C}$ itself are the finite ones. In general, a nonempty Zariski open set must be dense in the Euclidean topology, since a nonzero polynomial in $\mathbb{C}[x_1, \ldots, x_n]$ cannot vanish identically on a nonempty Euclidean open subset.

Conversely, given any subset V of $\mathbb{A}^n$, one can form the ideal $\mathcal{I}(V)$ of P_n consisting of all polynomials vanishing on V. If V is algebraic, then the quotient $P_n/I(V)$ is called the coordinate ring of V and denoted $k[V]$ (DF, p. 661). In particular, we have the alternative notation $k[\mathbf{A}^n]$ for $P_n = k[x_1, \ldots, x_n]$. Now let $V \subset \mathbf{A}^n, W \subset \mathbf{A}^m$ be algebraic.

Definition; DF, p. 662

A map $\phi : V \to W$ is called a morphism if it is the restriction to V of a polynomial map $p = (p_1, \ldots, p_m) : \mathbf{A}^n \to \mathbf{A}^m$ (so that the coordinates p_i of p are polynomial functions of n variables), whose image $\phi(V)$ lies in W. Two morphisms are identified if they are equal as functions on V. An isomorphism is a bijective morphism whose inverse (as a function) is also a morphism.

Given a morphism $\phi = (\phi_1, \ldots, \phi_m) : V \to W$, the map $\tilde{\phi}$ sending x_i to ϕ_i extends uniquely to a k-algebra homomorphism from P_m to the coordinate ring $k[V]$; the range is $k[V]$ rather than P_n since ϕ is well-defined only up to an element of I_V, the ideal of V. Moreover we must have $p(\phi_1(v), \ldots, \phi_m(v)) = 0$ for all $v \in V$ and p in the ideal I_W of W, so $\tilde{\phi}$ descends to a k-algebra homomorphism from $k[W]$ to $k[V]$. Conversely, it is easy to see that any k-algebra homomorphism $\tilde{\phi} : k[W] \to k[V]$ arises in this way from a morphism $\phi : V \to W$. We deduce

Theorem 6, DF, p. 663

Given algebraic sets $V \subset \mathbf{A}^n$, $W \subset \mathbf{A}^m$, there is a bijection $\phi \leftrightarrow \tilde{\phi}$ defined as above between morphisms from V to W and k-algebra homomorphisms $k[W] \to k[V]$, with isomorphisms of algebraic sets corresponding to k-algebra isomorphisms.

Thus the notion of morphism is intrinsic, not depending on the affine spaces containing algebraic sets.