Lecture 5-29: Review, part 2

May 29, 2024

We continue with review, now summarizing the material on group cohomology and starting on algebraic geometry.

We start with the notion of projective module. Given a ring R (not necessarily commutative) and a left R-module M, we say that M is projective if given any surjection $g : N \to N'$ of left R-modules and an R-module map $f : M \to N'$ there is an R-module map $h : M \to N$ with $gh = f$ (so that h lifts f to N). It is easy to show that M is projective if and only if M is a direct summand of a free R-module. Thus, in particular, if R is a PID and M is finitely generated (or even in general), M is projective if and only if M is free.

In particular, every free R-module is projective; since any R-module A is a homomorphic image of a free module (for example, the one with any set of generators of A as a free basis) one sees that any such module A admits a projective resolution $\cdots P_n \to \cdots \to \cdots \to P_1 \to P_0 \to A \to 0$, so that the P_i are projective and the sequence is exact. Taking homomorphisms into an R-module D, we get a cochain complex $0 \to \hom_R(A, D) \to \hom_R(P_0, D) \to \cdots$, where $d_n : \hom_R(P_{n-1}, D) \to \hom_R(P_n, D)$. The the nth cohomology group of this complex, or the quotient $\ker d_{n+1} / \operatorname{im} d_n$, is defined to be the nth Ext group $\operatorname{Ext}^n_R(A, D)$ of A (with coefficients in D). It is independent of the choice of projective resolution $\{P_i\}$. In particular $\operatorname{Ext}^0_R(A, D) = \hom_R(A, D)$. The Ext groups are $\mathbb{Z}$-modules, but not R-modules, unless R is commutative.

The cohomology groups $H^n(G, A)$ of a (finite) group G with coefficients in a G-module A are a special case of Ext groups. More precisely, let $R = \mathbb{Z}G$ be the integral group ring consisting of all combinations $\sum_{g \in G} z_g g$ with $z_g \in \mathbb{Z}$ and addition and multiplication defined in the obvious way. A G-module A is then just a (left) R–module; in particular, one has the trivial G-module $\mathbb{Z}$, on which G acts trivially. Then the cohomology group $H^n(G, A)$ is defined to be $\mathrm{Ext}^n_R(\mathbb{Z}, A)$. In particular $H^0(G, A)$ identifies with A^G, the subgroup of G-fixed elements in A.

If $G = \mathbb{Z}_m$ is cyclic of order m, say with generator σ, then one has a simple explicit resolution of $\mathbb{Z}$ in which every term apart from $\mathbb{Z}$ is $R = \mathbb{Z}G$; the maps toggle between multiplication by $N = 1 + \sigma + \cdots + \sigma^{m-1}$ and multiplication by $\sigma - 1$, except for the last one, which sends $\sum z_g g$ to $\sum z_g$. It follows easily that $H^0(G, A) \cong A^G$, $H^n(G, A) \cong A^G/NA$ if n is even and $n \geq 2$, while $H^n(G, A) \cong {}_NA/(\sigma - 1)A$ if n is odd, where ${}_NA = \{a \in A : Na = 0\}$. For general groups G, there is a standard resolution called the bar resolution to compute $H^n(G, A)$; but don't worry about the details of this resolution.

An easy consequence of the definition of $H^n(G, A)$ is that if A is torsion, so that there is a nonzero integer m with $mA = 0$, then we also have $mH^n(G, A) = 0$ for all n. A deeper fact, relying on maps called the restriction and corestriction maps, is that $|G|H^n(G, A) = 0$ for all $n > 0$ if G has order $|G|$. Putting these two constraints together, we deduce that $H^n(G, A) = 0$ for all $n > 0$ if A and G are finite with relatively prime orders. As a consequence of this vanishing result together with the interpretation of $H^2(G, A)$ by group extensions, we obtain Schur's Theorem that any finite group E admitting a normal subgroup A (not necessarily abelian) whose index is relatively prime to its order necessarily has a subgroup G isomorphic to E/A, so that E is the semidirect product of A and G. Moreover, any two complements of A in E are conjugate under A if A is abelian.

Turning now to algebraic geometry, we start with an algebraically closed field k and recall that in the Zariski topology the closed, or algebraic, subsets of k^n (now denoted $\mathbb{A}^n$ and called affine space) are precisely the zero loci $\mathcal{Z}(I)$ of ideals I in the polynomial ring $P_n = k[x_1, \ldots, x_n]$. The Nullstellensatz then asserts the existence of inclusion-reversing inverse bijections between radical ideals in P_n and closed subsets of $\mathbf{A}^n$, mapping an ideal I to its zero locus $\mathcal{Z}(I)$ and a closed set Z to the ideal $I(Z)$ of polynomials vanishing on Z.

A closed subset V is called irreducible if it is not the union of two (nonempty) proper closed subsets. Any closed set is then uniquely the union of finitely many irreducible closed subsets, none contained in another; these can overlap, unlike the connected components of a topological space. We call V a variety if it is irreducible. Subvarieties of $\mathbf{A}^n$ then correspond to prime ideals in P_n via the Nullstellensatz bijection.

The Nullstellensatz was proved via the Noether normalization lemma, which asserts for any field k that any finitely generated k-algebra is a finitely generated integral extension of some polynomial ring P_d over k. Using this we showed that the only finitely generated k-algebras that are field are the finite extensions of k, from which one can deduce a version of the Nullstellensatz that holds over any field k. Also Noether normalization gives a very convenient alternate characterization of the dimension of a variety V (that is, an irreducible closed subset of $\mathbf{A}^n$). The dimension of V was initially defined as the transcendence degree of the quotient field $k(V)$ of its coordinate ring $k[V] = P_n/I(v), I$ the ideal of V; but it can also be defined as the integer d such that $k[V]$ is integral over P_d (this integer being unique).

Morphisms π (that is, roughly speaking, polynomial maps) from oneclosed set V to another one W, not necessarily of the same affine space $\mathbf{A}^n$, correspond to k-algebra homomorphisms $\tilde{\pi}$ from the coordinate ring $k[W]$ to $k[V]$. If π is surjective then $\tilde{\pi}$ is injective; if π is surjective then $\tilde{\pi}$ is surjective. In particular any proper subvariety W of a variety V is such that $k[W]$ is a quotient of $k[V]$. The dimension $\dim W$ must be strictly less than $\dim V$ in this situation.

More algebraically and generally, we can define the (Krull) dimension of a commutative ring R to be the largest number n such that there is a chain $P_0 \subset \cdots \subset P_n$ of distinct prime ideals in R. The dimension of an algebraic set V is then equal to the Krull dimension of its coordinate ring $k[V]$.

Given an algebraic set $V \subset \mathbf{A}^n$ and a point $v \in V$, the tangent space $T_v V$ of V at v is the subspace of k^n defined by the linear polynomials $\sum_{i=1}^{n} D_i f(v) x_i$, where D_i denotes partial differentiation with respect to the ith variable x_i and the functions f run through the elements of the ideal $I(V)$ of V, or equivalently (thanks to the product rule) just through a set of generators of I. On a nonempty open subset of V, this space has dimension equal to that of V; we call any point v for which this holds nonsingular. The set of singular (i.e., not nonsingular) points forms a proper closed subset of V, of smaller dimension; the tangent space at any of those points has dimension larger than that of V.