Lecture 6-4: Review, part 2

June 4, 2025

Today I will pick up on some topics in commutative algebra omitted last time.

I begin with localization, a fundamental tool for simplifying (and thereby better understanding) the ideal structure of rings. Given a ring R and a multiplicatively closed subset S (so that $1 \in S, 0 \notin S$, and S is closed under multiplication), the localized ring $S^{-1}R$ consists by definition of all equivalence classes of pairs $(r, s) \in R \times S$, the relation $\sim$ being defined by $(r_1, s_1) \sim (r_2, s_2)$ if there is $s \in S$ with $s(r_1 s_2 - r_2 s_1) = 0$. A particularly important example is the case where $S = R - P$ is the complement of a prime ideal P of R. Every ideal I in $R' = S^{-1}R$ is the extension JR' of some ideal J of R, the extension being proper (not all of R') if and only if J does not intersect S.

There is an order-preserving bijection between prime ideals of R contained in P and prime ideals of $R' = R_P$, a prime ideal Q of R corresponding to its extension QR' in R' and a prime ideal Q' of R' corresponding to its contraction $Q' \cap R$ in R. (More generally, there is an order-preserving bijection between prime ideals of any localization $S^{-1}R$ and prime ideals of R not intersecting S.) In particular, R_P is always local, its maximal ideal being PR_P. The passage from R to R_P thus cuts out all ideals (and in particular all prime ideals) except those contained in P, just as the passage from R to its quotient R/P cuts out all ideals except those containing P. In particular the quotient R_P/PR_P is a field and may be identified with the quotient field of R/P.

Modules can also be localized: given an R-module M and a multiplicatively closed subset S of R, one has the localized module $S^{-1}M$, defined in the same way as $S^{-1}R$, replacing R by M. Localization of modules is then an exact functor. This construction actually appeared already in the fall, though rather inconspicuously; there I showed that for any module M over an integral domain R, the tensor product $M \otimes_R K$ may be identified with $S^{-1}M$, where S consists of the nonzero elements in R and K is its quotient field.

Using localization I was able to show that if S is a finitely generated integral extension of R and P is a prime ideal of R then there is always at least one but only finitely many prime ideals Q of S contracting to P; also there are no inclusion relations between any two of the ideals Q. I used this to show that the Krull dimension of a finitely generated integral extension of a ring R is the same as the Krull dimension of R itself.

Another construction this quarter changes the structure of R more drastically, enabling us to solve many equations in a larger ring that have no solutions in R. This is completion of R with respect to an ideal I. One starts by putting a topology on R, namely the I-adic topology, such that a nonempty open subset of R is exactly one that contains $r + I^n$ for some n whenever it contains $r \in R$. One then completes R in this topology, looking at the set $\hat{R}$ of coherent (or Cauchy) sequences $(r_1, r_2, \ldots)$ such that $r_i \in R/I^i$ and r_j maps to r_i under the canonical surjection $R/I^j \Rightarrow R/I^i$ whenever $j \geq i$. There is a natural map $R \to \hat{R}$ sending r to the constant sequence $(r, r, \ldots)$; its kernel is the intersection $\cap_n I^n$ of all the powers of I. If R is Noetherian, this intersection coincides with the set of $s \in R$ such that $(1 - i)s = 0$ for some $i \in I$.

The usual geometric series $\sum_{n=0}^{\infty} i^n$ then converges in $\hat{R}$ for any $i \in I$, thus guaranteeing that $1 - i$ is invertible in $\hat{R}$ for any $i \in I$. If I is maximal, then any r$\in R$ not lying in I thereby acquires a multiplicative inverse in $\hat{R}$, so that (if R is Noetherian) $\hat{R}$ contains a copy of the localization R_I. In addition, though, and as promised above, many polynomial equations with coefficients in R have solutions in $\hat{R}$. More precisely, we have Hensel's lemma: given an ideal I and a polynomial $F \in \hat{R}[x]$ reducing to $f \in R/I[x]$, suppose that $f = g_1 g_2$ with $g_1, g_2 \in R/I[x]$ generating the unit ideal of $R/I[x]$ and g_1 is monic; then the factorization of f lifts to a factorization $G_1 G_2$ of F in $\hat{R}[x]$ such G_1 is monic and G_i reduces to g_i for $i = 1, 2$. In particular, given a polynomial $q \in K[x]$ over a field $K = \mathbb{Z}/p\mathbb{Z}$ of prime order with distinct roots in its splitting field, this polynomial has a full complement of distinct roots in the completion $\mathbb{Z}_p$ of $\mathbb{Z}$ with respect to (p).

As large as a completion $\hat{R}$ of R has to be (to contain roots for a wide family of polynomials), it is still not too large: the completion $\hat{R}$ of a Noetherian ring R with respect to an ideal I is Noetherian. Also the completion $\hat{R}$ of R with respect to a maximal principal ideal (x) is a discrete valuation ring, so that (as you saw last quarter) the only nonzero ideals of $\hat{R}$ are the powers of (x). A fundamental example to keep in mind is $R = \mathbb{Z}, I = (p)$ for p prime, where elements of the completion $\mathbb{Z}_p$ can be thought of as Laurent series $\sum_{n=-m}^{\infty} a_n p^n$ with the coefficients a_i lie in $\{0, \ldots, p-1\}$, where addition, subtraction, and multiplication take place with carrying. Another simpler example is the power series ring $k[[x_1, \ldots, x_n]]$, which can be identified with the completion of the polynomial ring $k[x_1, \ldots, x_n]$ with respect to the maximal ideal $(x_1, \ldots, x_n)$.