LECTURES ON COMMUTATIVE ALGEBRA II

Mel Hochster

Math 615: Lecture of January 4, 2012

In these lectures, all rings are assumed to be commutative, associative, with multiplicative identity denoted 1, which may be subscripted with the letter denoting the ring if precision is needed. Ring homomorphisms $R \to S$ are assumed to map $1_R \in R$ to $1_S \in S$. Modules M over a ring R are assumed to be *unital*, i.e., $1 \cdot u = u$ for all $u \in M$. A *local* ring is a Noetherian ring with a unique maximal ideal. The statement that (R, m) is local means that R is a local ring with maximal ideal m. The statement that (R, m, K) is local means that R is local with maximal ideal m and residue class field $K = R/m$. We use $\mathbb{N} \subseteq \mathbb{Z} \subseteq \mathbb{Q} \subseteq \mathbb{R} \subseteq \mathbb{C}$ for the nonnegative integers, the integers, the rational numbers, the real numbers, and the complex numbers, respectively.

We give an overview of some the material that will be covered near the beginning of this set of lectures.

One theme will be the study of complete local rings. Localization at a prime followed by completion at the resulting maximal ideal is a way of life. Many problems, even some that seem "global," can be attacked by first reducing to the local case and then to the complete case. Complete local rings turn out to have extremely good behavior in many respects. A key ingredient in this type of reduction is that when R is local, $\widehat{R}$ is local and faithfully flat over R.

We shall study the structure of complete local rings. A complete local ring that contains a field always contains a field that maps onto its residue class field: thus, if (R, m, K) contains a field, it contains a field K_0 such that the composite map $K_0 \subseteq R \twoheadrightarrow R/m = K$ is an isomorphism. Then $R = K_0 \oplus_{K_0} m$, and we may identify K with K_0. Such a field K_0 is called a *coefficient field* for R.

The choice of a coefficient field K_0 is *not unique* in general, although in positive prime characteristic p it is unique if K is perfect, which is a bit surprising. The existence of a coefficient field is a rather hard theorem. Once it is known, one can show that every complete local ring that contains a field is a homomorphic image of a formal power series ring over a field. It is also a module-finite extension of a formal power series ring over a field. This situation is analogous to what is true for finitely generated algebras over a field, where one can make the same statements using polynomial rings instead of formal power series rings. The statement about being a module-finite extension of a power series ring is an analogue of the Noether normalization theorem. A local ring (R, m, K) that contains a field is called *equicharacteristic*, because R contains a field if and only if R and K have the same characteristic. (It is clear that if $K \subseteq R$ they must have the same characteristic. If K has characteristic 0, it is clear that R does, and contains a copy of $\mathbb{Z}$. Since no nonzero integer vanishes in R/m, every nonzero integer is a unit in R, which gives a unique map of

$\mathbb{Q} = (\mathbb{Z} - \{0\})^{-1}\mathbb{Z}$ into R by the universal mapping property of localization. On the other hand, if R has positive prime characteristic $p > 0$, it clearly contains a copy of $\mathbb{Z}/p\mathbb{Z}$.)

Local rings that are not equicharacteristic are called *mixed characteristic*. The characteristic of the residue class field of such a ring is always a positive prime integer p. The characteristic of the ring is either 0, which is what it will be in the domain case, or else a power of p, p^k, with $k > 1$.

Throughout these lectures, the term *discrete valuation ring*, abbreviated DVR, will be used for a local domain V, not a field, whose maximal ideal is principal, say tV, $t \neq 0$. It is then the case that every nonzero element of V is uniquely expressible in the form ut^n, where u is a unit, and every ideal is consequently principal. (Technically, these rings should be called *rank one* discrete valuation rings or Noetherian discrete valuation rings.)

A local domain of mixed characteristic will have characteristic 0, while its residue class field has positive prime characteristic p. An example is the ring of p-adic integers, which is the completion of the localization of the integers at the prime ideal generated by the positive prime integer p. A formal power series ring over the p-adic integers also has mixed characteristic.

The structure of complete local rings in mixed characteristic is more complicated, but the theory has been fully worked out: if (R, m) has mixed characteristic, it is a homomorphic image of a formal power series ring over a complete discrete valuation ring (V, pV) whose maximal ideal is generated by a positive prime integer p. If a mixed characteristic local ring is a domain, it is module-finite over a formal power series ring over such a ring $V \subseteq R$ such that the induced map of residue class fields $V/pV \to R/m$ is an isomorphism. V is called a *coefficient ring for* R. When R is not a domain the statements are more complicated, but the situation is completely understood.

We shall study *regular* local rings: these constitute an important class of local rings. (R, m, K) is *regular* precisely if the Krull dimension $\dim(R)$ of R is equal to the least number of generators of the maximal ideal m: by Nakayama's lemma, the latter is the same as $\dim_K(m/m^2)$. The local ring of a complex algebraic variety at a closed point (corresponding to localizing at a maximal ideal) is regular if and only if the variety is smooth (or nonsingular) at that point. Such points are also called *simple* points. In the case of dimension one, a regular local ring is the same thing as a DVR. Although it is not obvious from the definition, a regular local ring is an integral domain. In fact, a regular local ring is a UFD. This was an open question for many years: it was not solved until the introduction of homological methods into commutative algebra by M. Auslander, D. Buchsbaum. We shall eventually give a proof of this fact, following M. P. Murthy, based on recovering the divisor class group of a normal domain R from the Grothendieck group of finitely generated R-modules.

A local ring is regular if and only if its completion is regular. Complete regular local rings can be classified. A complete regular local ring that contains a field is simply the formal power series ring in finitely many variables over a field. The situation in mixed characteristic is more complicated, but also well understood. If V is a coefficient ring, the complete regular ring R of Krull dimension d is either a formal power series ring

$V[[x_1, \ldots, x_{d-1}]]$, or it will have the form $T/(p-f)$, where $T = V[[x_1, \ldots, x_d]]$ has maximal ideal $m_T = (p, x_1, \ldots, x_d)T$, and $f \in m_T^2$.

An important property of complete local rings is that they satisfy Hensel's lemma. Let (R, m, K) be complete local and let f be a monic polynomial over R. If $u \in R[x]$, we write $\overline{u}$ for the polynomial in $K[x]$ obtained by taking residue classes of coefficients of u modulo m. Suppose that $\overline{f}$ factors $\overline{f} = GH$ in $K[x]$, where G and H are relatively prime monic polynomials. Hensel's lemma asserts that this factorization lifts uniquely to $R[x]$. That is, there are monic polynomials $g, h \in R[x]$ such that $f = gh$ and $\overline{g} = G$ while $\overline{h} = H$.

This is a very powerful result. For example, consider the formal power series ring $\mathbb{C}[[z]]$ in one variable over the complex numbers, and consider the polynomial equation $x^2-(1+z)$. Mod the maximal ideal $zC[[z]]$, this equation becomes $x^2 - 1 = (x-1)(x+1)$. Hensel's lemma now implies that $x^2-(1+z)$ factors as $\big(x-\alpha(z)\big)\big(x-\beta(z)\big)$ where $\alpha(z), \beta(z) \in \mathbb{C}[[z]]$. Of course, these must be square roots of $1+z$, so that $\beta = -\alpha$. Hensel's lemma also implies that their constant terms must be 1 and -1. Lifting the factorization yields the existence of power series square roots for $1 + z$. Of course, we know this from Newton's binomial theorem, which gives an explicit formula for $(1 + z)^{1/2}$. But Hensel's lemma provides solutions to much more complicated problems for which no formula is readily available. This result is closely related to the implicit function theorem: we shall make this more explicit when we study *étale* ring extensions.

Algebraists are not satisfied with having Hensel's lemma available over the completion of a local ring R. It turns out that in between the local ring R and its completion is a ring R^{h}, the *Henselization* of R, for which Hensel's lemma holds, but which is algebraic over R. (In many good cases it is the same as the algebraic closure of R in its completion, but it is not defined that way.) The Henselization is constructed using the theory of étale ring extensions. R^{h} is Noetherian, and faithfully flat over R. Heuristically, it may be viewed as an "algebraic version" of the completion of R. When R is regular, R^{h} is also regular. The maximal ideal of R expands to the maximal ideal of R^{h}, and the induced map of residue class fields between a local ring and its Henselization is an isomorphism.

Here is a result due to Artin and Rotthaus which may also be deduced from the Néron-Popescu desingularization theorem. There is a version for formal power series over a complete discrete valuation ring, but in this introduction we only state the result for fields. Let $T = K[[x_1, \ldots, x_n]]$ be a formal power series ring over a field. Let R be any finitely generated K-subalgebra of T. The Artin-Rotthaus theorem asserts that the inclusion $R \subseteq T$ factors $R \to S \to T$ where S is obtained from algebraically independent elements $x_1, \ldots, x_n, y_1, \ldots, y_m$ by localizing $K[x_1, \ldots, x_n, y_1, \ldots, y_m]$ at the maximal ideal $(x_1, \ldots, x_n, y_1, \ldots, y_m)$ and then taking the Henselization: briefly, $S = (K[x, y]_{(x,y)})^{\mathrm{h}}$. $x_i \in S$ maps to $x_i \in T$ for all i, and the y_j map into the maximal ideal of T. Thus, S is a regular local ring, algebraic over $K[x_1, \ldots, x_n, y_1, \ldots, y_m]$, in which the elements $x_1, \ldots, x_n$ are part of a minimal set of generators of the maximal ideal.

It is necessary to allow for the possibility of the extra indeterminates $y_1, \ldots, y_m$, since T has infinite transcendence degree over K. Note that the theorem does *not* assert that the map $S \to T$ has to be injective.

This theorem frequently allows one to reduce problems about complete local rings to the study of algebras finitely generated over a field! The complete local ring is module-finite over a formal power series ring. One can frequently translate the problem into a statement over the formal power series ring T that involves only finitely many elements from the formal power series ring. These elements generate a K-subalgebra R that can be used in the hypothesis of the Artin-Rotthaus theorem. The trouble with working with R is that good properties of T may have been lost. However, these are restored when we map to S and work in S. Moreover, one does not need to use all of S, and one can frequently replace S by a finitely generated K-algebra. In the mixed characteristic case there is an entirely similar result.

In consequence, many problems can be reduced to the case of a finitely generated algebra either over a field or over a complete DVR.

This means that the study of finitely generated algebras over a field and over a DVR is utterly central to the subject of commutative Noetherian rings!

In a different direction, we will also study Hilbert functions associated with local rings and numerical invariants, such as multiplicities. Consider a local ring (R, m, K) of Krull dimension d and an m-primary ideal I. The condition on I simply means that for some N, $m^N \subseteq I \subseteq m$. The function $\ell(R/I^n)$, where ℓ is length, is called the *Hilbert function* of I, and agrees with a polynomial in n of degree d for all $n \gg 0$. The polynomial is called the *Hilbert polynomial*. Its leading term will have the form $\frac{e}{d!}n^d$ where e is a positive integer. The integer e is called the *multiplicity* of I. Note that e can be obtained as a limit:

$$e = d! \lim_{n\to\infty} \frac{\ell(R/I^n)}{n^d}.$$

The multiplicity of m is called the *multiplicity* of R. Under mild assumptions, a local ring of multiplicity 1 is regular. (One can also study $\ell(M/I^nM)$ for any finitely generated R-module M. This is gives the Hilbert function and Hilbert polynomial of M: one difference is that in the module case, the degree of the Hilbert polynomial is the dimension of M.)

Multiplicities can be obtained in other ways. Given a sequence of elements $\underline{x} = x_1, \ldots, x_d$ of ring R, and an R-module M, we shall define a homology theory called *Koszul homology*: the Koszul homology modules are denoted $H_i(\underline{x}; M)$. (They vanish if $i < 0$ or if $i > d$.) We won't give the definition at this point. Koszul homology has many uses, including the proofs of the fundamental facts about behavior of cohomology of coherent sheaves on projective space. The connection with the multiplicities defined in the preceding paragraph is this. If $x_1, \ldots, x_d$ is a system of parameters for the local ring R, which simply means that $d = \dim(R)$ and $I = (x_1, \ldots, x_d)R$ is m-primary, then the multiplicity of the ideal I is the same as $\sum_{i=0}^{d}(-1)^i\ell\big(H_i(\underline{x}; R)\big)$, the alternating sum of the lengths of the Koszul homology modules, which do turn out to have finite length in this situation.

In developing the theory of regular rings and the material on multiplicities we shall introduce and use a number of homological techniques, including derived functors such as Tor and Ext, and the theory of spectral sequences. We shall give a spectral sequence proof

of the equivalence of the two characterizations of the multiplicity associated to an ideal generated by a system of parameters. Eventually we shall also give a proof that does not depend on the theory of spectral sequences, but the spectral sequence argument, which is due to J.-P. Serre, was found first. Spectral sequences take some getting used to, but often provide the right way to look at a problem.

Math 615: Lecture of January 6, 2012

Here is a simple example of a local ring that contains a field but does not have a coefficient field. Let V be the localization of the polynomial ring $\mathbb{R}[t]$ in one variable over the real numbers $\mathbb{R}$ at the prime ideal $P = (t^2+1)$, and let $m = PV$. Then V/PV is the fraction field of $\mathbb{R}[t]/(t^2+1) \cong \mathbb{C}$, which is $\mathbb{C}$. But $S \subseteq \mathbb{R}(t)$ does not contain any element whose square is -1: the square of a non-constant rational function is non-constant, and the square of a real scalar cannot be -1. Note that V is a DVR.

The completion of $\widehat{V}$ of V is also a DVR with residue class field $\mathbb{C}$, and so it must contain a square root of -1. Can you see what it is?

We begin our analysis of the structure of complete local rings by proving Hensel's lemma.

Theorem (Hensel's lemma). *Let (R, m, K) be a complete local ring and let f be a monic polynomial of degree d in $R[x]$. Suppose that $\overline{u}$ denotes the image of $u \in R[x]$ under the ring homomorphism $R[x] \twoheadrightarrow K[x]$ induced by $R \twoheadrightarrow K$. If $\overline{f} = GH$ where G, $H \in K[x]$ are monic of degrees s and t, respectively, and G and H are relatively prime in $K[x]$, then there are unique monic polynomials g, $h \in R[x]$ such that $f = gh$ and $\overline{g} = g$ while $\overline{h} = h$.*

Proof. Let F_n denote the image of f in $(R/m^n)[x]$. We recursively construct monic polynomials $G_n \in (R/m^n)[x]$, $H_n \in (R/m^n)[x]$ such that $F_n = G_n H_n$ for all $n \geq 1$, where G_n and H_n reduce to G and H, respectively, mod m, and show that F_n and G_n are unique. Note that it will follow that for all n, G_n has the same degree as G, namely s, and H_n has the same degree as H, namely t, where $s+t = d$. The uniqueness implies that mod m^{n-1}, G_n, H_n become G_{n-1}, H_{n-1}, respectively. This yields that the sequence of coefficients of x^i in the G_n is an element of $\varprojlim_n (R/m^n) = R$, since R is complete. Using the coefficients determined in this way, we get a polynomial g in $R[x]$, monic of degree s. Similarly, we get a polynomial $h \in R[x]$, monic of degree t. It is clear that $\overline{g} = G$ and $\overline{h} = H$, and that $f = gh$, since this holds mod m^n for all n: thus, every coefficient of $f - gh$ is in $\bigcap_n m^n = (0)$.

It remains to carry through the recursion, and we have $G_1 = G$ and $H_1 = H$ from the hypothesis of the theorem. Now assume that G_n and H_n have been constructed and shown unique for a certain $n \geq 1$. We must construct G_{n+1} and H_{n+1} and show that they are unique as well. It will be convenient to work mod m^{n+1} in the rest of the argument: replace R by R/m^{n+1}. Construct G^*, H^* in $R[x]$ by lifting each coefficient of G_n and H_n respectively, but such that the two leading coefficients occur in degrees s and t respectively and are both 1. Then, mod m^n, $F \equiv G^*H^*$, i.e., $\Delta = F - G^*H^* \in m^n R[x]$. We want to show that there are unique choices of $\delta \in m^n R[x]$ of degree at most $s-1$ and $\epsilon \in m^n R[x]$ of

degree at most $t-1$ such that $F-(G^*+\delta)(H^*+\epsilon)=0$, i.e., such that $\Delta=\epsilon G^*+\delta H^*+\delta\epsilon$. Since $\delta,\epsilon\in m^nR[x]$, $n\geq 1$, their product is in $m^{2n}R[x]=0$, since $2n\geq n+1$. Thus, our problem is to find such ϵ and δ with $\Delta=\epsilon G^*+\delta H^*$. Now, G and H generate the unit ideal in $K[x]$, and $R[x]_{\rm red}=K[x]$. It follows that G^* and H^* generate the unit ideal in $R[x]$, and so we can write $1=\alpha G^*+\beta H^*$. Multiplying by Δ, we get $\Delta=\Delta\alpha G^*+\Delta\beta H^*$. Then $\Delta\alpha$ and $\Delta\beta$ are in $m^nR[x]$, but do not yet satisfy our degree requirements. Since H^* is monic, we can divide $\Delta\alpha$ by H^* to get a quotient γ and remainder ϵ, i.e., $\Delta\alpha=\gamma H^*+\epsilon$, where the degree of ϵ is $\leq t-1$. If we consider this mod m^n, we have $0\equiv\gamma H_n+\epsilon$, from which it follows that γ, $\epsilon\in m^nR[x]$. Then $\Delta=\epsilon G^*+\delta H^*$ where $\delta=\gamma G^*+\Delta\beta$. Since Δ and ϵG^* both have degree $<n$, so does δH^*, which implies that the degree of δ is $\leq s-1$.

Finally, suppose that we also have $\Delta=\epsilon' G^*+\delta' H^*$ where ϵ' has degree $\leq t-1$ and δ' has degree $\leq s-1$. Subtracting, we get an equation $0=\mu G^*+\nu H^*$ where the degree of $\mu=\epsilon-\epsilon'$ is $\leq t-1$ and the degree of $\nu=\delta-\delta'$ is $\leq s-1$. Since G^* is a unit considered mod H^*, it follows that $\mu\in(H^*)$, i.e., that H^* divides μ. But H^* is monic, and so this cannot happen unless $\mu=0$: the degree of μ is too small. Similarly, $\nu=0$. $\square$

Remark. This result does not need that R be Noetherian. The same proof, verbatim, shows that if $(R,\,m)$ is a quasilocal ring that is m-adically separated and complete (so that $R\cong\varprojlim_n R/m^n$), the same result holds.

We can now deduce:

Theorem. *Let $(R,\,m,\,K)$ be a complete local ring that contains a field of characteristic 0. Then R has a coefficient field. In fact, R will contain a maximal subfield, and any such subfield is a coefficient field.*

Proof. Let $\mathcal{S}$ be the set of all subrings of R that happen to be fields. By hypothesis, this set is nonempty. Given a chain of elements of $\mathcal{S}$, the union is again a subring of R that is a field. By Zorn's lemma, $\mathcal{S}$ will have a maximal element K_0. To complete the proof of the theorem, we shall show that K_0 maps isomorphically onto K. Obviously, we have a map $K_0\subseteq R\twoheadrightarrow R/m=K$, and so we have a map $K_0\to K$. This map is automatically injective: call the image K_0'. To complete the proof, it suffices to show that it is surjective.

If not, let θ be an element of K not in the image of K_0. We consider two cases: the first is that θ is transcendental over K_0'. Let t denote an element of R that maps to θ. Then $K_0[t]$ is a polynomial subring of R, and every nonzero element is a unit: if some element were in m, then working mod m we would get an equation of algebraic dependence for θ over K_0' in K. By the universal mapping property of localization, the inclusion $K_0[t]\subseteq R$ extends to a map $K_0(t)\subseteq R$, which is necessarily an inclusion. This yields a subfield of R larger than K_0, a contradiction.

We now consider the case where θ is algebraic over the image of K_0. Consider the minimal polynomial of θ over K_0', and let f be the corresponding polynomial with coefficients in $K_0[x]\subseteq R[x]$. Modulo m, this polynomial factors as $(x-\theta)H(x)$, where these are relatively prime because θ is separable over K_0': this is the only place in the argument where we use that the field has characteristic 0. The factorization lifts uniquely: we have $f=(x-t)h(x)$ where $t\in R$ is such that $t\equiv\theta \bmod m$. That is, $f(t)=0$. We claim that

the map $K_0[t] \subseteq R \twoheadrightarrow R/m$, whose image is $K_0'[\theta]$, gives an isomorphism of $K_0[t]$ with $K_0'[\theta]$: we only need to show injectivity. But if $P(x) \in K_0[x]$ is a polynomial such that $P(t)$ maps to 0, then f divides $P(x)$, which implies that $P(t) = 0$. Since $K_0[t] \cong K_0'[\theta]$ (both are $\cong K_0[t]/\big(f(t)\big)$), $K_0[t]$ is a field contained in R that is strictly larger than K_0, a contradiction. $\square$

Remark. If R is a complete local domain of positive prime characteristic $p > 0$, the same argument shows that R contains a maximal subfield K_0, and that K is purely inseparable and algebraic over the image of K_0.

We can get a similar result easily in characteristic p if K is perfect, although the proof is completely different.

Theorem. *Let (R, m, K) be a complete local ring of positive prime characteristic p. Suppose that K is perfect. Let $R^{p^n} = \{r^{p^n} : r \in R\}$ for every $n \in \mathbb{N}$. Then $K_0 = \bigcap_{n=0}^{\infty} R^{p^n}$ is a coefficient field for R, and it is the only coefficient field for R.*

Math 615: Lecture of January 9, 2012

Theorem. *Let (R, m, K) be a complete local ring of positive prime characteristic p. Suppose that K is perfect. Let $R^{p^n} = \{r^{p^n} : r \in R\}$ for every $n \in \mathbb{N}$. Then $K_0 = \bigcap_{n=0}^{\infty} R^{p^n}$ is a coefficient field for R, and it is the only coefficient field for R.*

Proof. Consider any coefficient field L for R, assuming for the moment that one exists. Then $L \cong K$, and so L is perfect. Then

$$L = L^p = \cdots = L^{p^n} = \cdots,$$

and so for all n,

$$L \subseteq L^{p^n} \subseteq R^{p^n}.$$

Therefore, $L \subseteq K_0$. If we know that K_0 is a field, it follows that $L = K_0$, proving uniqueness.

It therefore suffices to show that K_0 is a coefficient field for K. We first observe that K_0 meets m only in 0. For if $u \in K_0 \cap m$, then u is a p^n th power for all n. But if $u = v^{p^n}$ then $v \in m$, so $u \in \cap_n m^{p^n} = (0)$.

Thus, every element of $K_0 - \{0\}$ is a unit of R. Now if $u = v^{p^n}$, then $1/u = (1/v)^{p^n}$. Therefore, the inverse of every nonzero element of K_0 is in K_0. Since K_0 is clearly a ring, it is a subfield of R.

Finally, we want to show that given $\theta \in K$ some element of K_0 maps to θ. Let r_n denote an element of R that maps to $\theta^{1/p^n} \in K$. Then $r_n^{p^n}$ maps to θ. We claim that $\{r_n^{p^n}\}_n$ is a Cauchy sequence in R, and so has a limit r. To see this, note that r_n and r_{n+1}^p both map to θ^{1/p^n} in K, and so $r_n - r_{n+1}^p$ is in m. Taking p^n powers, we find that

$$r_n^{p^n} - r_{n+1}^{p^{n+1}} \in m^{p^n}.$$

Therefore, the sequence is Cauchy, and has a limit $r \in R$. It is clear that r maps to θ. Therefore, it suffices to show that $r \in R^{p^k}$ for every k. But

$$r_k, r_{k+1}^p, \ldots, r_{k+h}^{p^h} \cdots$$

is a sequence of the same sort for the element θ^{1/p^k}, and so is Cauchy and has a limit s_k in R. But $s_k^{p^k} = r$ and so $r \in R^{p^k}$ for all k. $\square$

Before pursuing the issue of the existence of coefficient fields and coefficient rings further, we show that the existence of a coefficient field implies that the ring is a homomorphic image of a power series ring in finitely many variables over a field, and is also a module-finite extension of such a ring.

We begin as follows:

Proposition. *Let R be separated and complete in the I-adic topology, where I is a finitely generated ideal of R, and let M be an I-adically separated R-module. Let $u_1, \ldots, u_h \in M$ have images that span M/IM over R/I. Then $u_1, \ldots, u_h$ span M over R.*

Proof. Since $M = Ru_1 + \cdots + Ru_h + IM$, we find that for all n,

$$(*) \qquad I^n M = I^n u_1 + \cdots + I^n u_n + I^{n+1} M.$$

Let $u \in M$ be given. Then u can be written in the form $r_{01}u_1 + \cdots + r_{0h}u_h + v_1$ where $v_1 \in IM$. Therefore $v_1 = r_{11}u_1 + \cdots r_{1h}u_h + v_2$ where the $r_{1j} \in IM$ and $v_2 \in I^2M$. Then

$$u = (r_{01} + r_{11})u_1 + \cdots + (r_{0n} + r_{1h})u_h + v_2,$$

where $v_2 \in I^2M$. By a straightforward induction on n we obtain, for every n, that

$$u = (r_{01} + r_{11} + \cdots + r_{n1})u_1 + \cdots + (r_{0h} + r_{1h} + \cdots + r_{nh})u_h + v_{n+1}$$

where every $r_{jk} \in I^j$ and $v_{n+1} \in I^{n+1}M$. In the recursive step, the formula $(*)$ is applied to the element $v_{n+1} \in I^{n+1}M$. For every k, $\sum_{j=0}^{\infty} r_{jk}$ represents an element s_k of the complete ring R. We claim that

$$u = s_1u_1 + \cdots + s_hu_h.$$

The point is that if we subtract

$$(r_{01} + r_{11} + \cdots + r_{n1})u_1 + \cdots + (r_{0h} + r_{1h} + \cdots + r_{nh})u_n$$

from u we get $v_{n+1} \in I^{n+1}M$, and if we subtract it from

$$s_1u_1 + \cdots + s_hu_h$$

we also get an element of $I^{n+1}M$. Therefore,

$$u - (s_1u_1 + \cdots + s_hu_h) \in \bigcap_n I^{n+1}M = 0,$$

since M is I-adically separated. $\square$

Remark. We tacitly used in the argument above that if $r_{jk} \in I^j$ for $j \geq n+1$ then

$$r_{n+1,k} + r_{n+2,k} + \cdots + r_{n+t,k} + \cdots \in I^{n+1}.$$

This actually requires an argument. If I is finitely generated, then I^{n+1} is finitely generated by the monomials of degree $n+1$ in the generators of I, say, $g_1, \ldots, g_d$. Then

$$r_{n+1+t,k} = \sum_{\nu=1}^{d} q_{t\nu}g_\nu,$$

with every $q_{t\nu} \in I^t$, and

$$\sum_{t=0}^{\infty} r_{n+1+t,k} = \sum_{\nu=1}^{d}(\sum_{t=0}^{\infty} q_{t\nu})g_\nu.$$

We also note:

Proposition. *Let $f : R \to S$ be a ring homomorphism, and supposed that S is J-adically complete and separated for an ideal $J \subseteq S$ and that $I \subseteq R$ maps into J. Then there is a unique induced homomorphism $\widehat{R}^I \to S$ that is continuous (i.e., preserves limits of Cauchy sequences in the appropriate ideal-adic topology).*

Proof. $\widehat{R}^I$ is the ring of I-adic Cauchy sequences mod the ideal of sequences that converge to 0. The continuity condition forces the element represented by $\{r_n\}_n$ to map to

$$\lim_{n\to\infty} f(r_n)$$

(Cauchy sequences map to Cauchy sequences: if $r_m - r_n \in I^N$, then $f(r_m) - f(r_n) \in J^N$, since $f(I) \subseteq J$). It is trivial to check that this is a ring homomorphism that kills the ideal of Cauchy sequences that converge to 0, which gives the required map $\widehat{R}^I \to S$. $\square$

A homomorphism of quasilocal rings $h : (A, \mu, \kappa) \to (R, m, K)$ is called a *local homomorphism* if $h(\mu) \subseteq m$. If A is a local domain, not a field, the inclusion of A in its fraction field is not local. If A is a local domain, any quotient map arising from killing a proper ideal is local. A local homomorphism induces a homomorphism of residue class fields $\kappa = A/\mu \to R/m = K$.

Proposition. *Let (A, μ, κ) and (R, m, K) be complete local rings, and $h : A \to R$ a local homomorphism. Suppose that $f_1, \ldots, f_n \in m$ together with μR generate an m-primary ideal. Then:*

(a) *There is a unique continuous homomorphism $h : A[[X_1, \ldots, X_n]] \to R$ extending the A-algebra map $A[X_1, \ldots, X_n]$ taking X_i to f_i for all i.*

(b) *If K is a finite algebraic extension of κ, then R is module-finite over the image of $A[[X_1, \ldots, X_n]]$.*

(c) *If $\kappa \to K$ is an isomorphism, and $\mu R + (f_1, \ldots, f_n)R = m$, then the map h described in (a) is surjective.*

Proof. (a) This is immediate from the preceding Proposition, since $(X_1, \ldots, X_n)$ maps into m.

(b) The expansion of the maximal ideal $\mathcal{M} = (\mu, X_1, \ldots, X_n)$ of $A[[X_1, \ldots, X_n]]$ to R is $\mu R + (f_1, \ldots, f_n)R$, which contains a power of m, say m^N. Thus, $R/\mathcal{M}R$ is a quotient of R/m^N and has finite length: the latter has a filtration whose factors are the finite-dimensional K-vector spaces m^i/m^{i+1}, $0 \leq i \leq N-1$. Since K is finite-dimensional over κ, it follows that $R/\mathcal{M}R$ is finite-dimensional over $A[[X_1, \ldots, X_n]]/\mathcal{M} = \kappa$. Choose elements of R whose images in $R/\mathcal{M}R$ span it over κ. By the earlier Theorem, these elements span R as an $A[[X_1, \ldots, X_n]]$-module. We are using that R is $\mathcal{M}$-adically separated, but this follows because $\mathcal{M}R \subseteq m$, and R is m-adically separated.

(c) We repeat the argument of the proof of part (b), noting that now $R/\mathcal{M}R \cong K \cong \kappa$, so that $1 \in R$ generates R as an $A[[X_1, \ldots, X_n]]$ module. But this says that R is a cyclic $A[[X_1, \ldots, X_n]]$-module spanned by 1, which is equivalent to the assertion that $A[[X_1, \ldots, X_n]] \to R$ is surjective. $\square$

We have now done all the real work needed to prove the following:

Theorem. *Let (R, m, K) be a complete local ring with coefficient field $K_0 \subseteq K$, so that $K_0 \subseteq R \twoheadrightarrow R/m = K$ is an isomorphism. Let $f_1, \ldots, f_n$ be elements of m generating an ideal primary to m. Let $K_0[[X_1, \ldots, X_n]] \to R$ be constructed as in the preceding Proposition, with X_i mapping to f_i and with $A = K_0$. Then:*

(a) *R is module-finite over $K_0[[X_1, \ldots, X_n]]$.*

(b) *Suppose that $f_1, \ldots, f_n$ generate m. Then the homomorphism $K_0[[x_1, \ldots, x_n]] \to R$ is surjective. (By Nakayama's lemma, the least value of n that may be used is the dimension as a K-vector space of m/m^2.)*

(c) *If $d = \dim(R)$ and $f_1, \ldots, f_d$ is a system of parameters for R, the homomorphism*

$$K_0[[x_1, \ldots, x_d]] \to R$$

is injective, and so R is a module-finite extension of a formal power series subring.

Proof. (a) and (b) are immediate from the preceding Proposition. For part (c), let $\mathfrak{A}$ denote the kernel of the map $K_0[[x_1, \ldots, x_d]] \to R$. Since R is a module-finite extension of the ring $K_0[[x_1, \ldots, x_d]]/\mathfrak{A}$, $d = \dim(R) = \dim(K_0[[x_1, \ldots, x_d]]/\mathfrak{A})$. But we know that $\dim(K_0[[x_1, \ldots, x_d]]) = d$. Killing a nonzero prime in a local domain must lower the dimension. Therefore, we must have that $\mathfrak{A} = (0)$. $\square$

Thus, when R has a coefficient field K_0 and $f_1, \ldots, f_d$ are a system of parameters, we may consider a formal power series

$$\sum_{\nu \in \mathbb{N}^d} c_\nu f^\nu,$$

where $\nu = (\nu_1, \ldots, \nu_d)$ is a multi-index, the $c_\nu \in K_0$, and f^ν denotes $f_1^{\nu_1} \cdots f_d^{\nu_d}$. Because R is complete, this expression represents an element of R. Part (c) of the preceding Theorem implies that this element is not 0 unless all of the coefficients c_ν vanish. This fact is sometimes referred to as the *analytic independence of a system of parameters*. The elements of a system of parameters behave like formal indeterminates over a coefficient field. Formal indeterminates are also referred to as *analytic indeterminates*.

Math 615: Lecture of January 11, 2012

A quasilocal ring (R, m, K) is defined to be *Henselian* if whenever $f \in R[x]$ is monic and $f \equiv GH \bmod mR[x]$, where $G, H \in K[x]$ are monic and relatively prime, there exist monic polynomials $g, h \in R[x]$ such that $g \equiv G \bmod mR[x]$, $h \equiv H \bmod mR[x]$, and $f = gh$. More briefly, R is Henselian precisely when all factorizations into relatively prime monic polynomials mod $mR[x]$ over $K[x]$ lift to $R[x]$. With this terminology, Hensel's lemma implies that complete and separated quasilocal rings are Henselian. Notice that if R is Henselian and m-adically separated, then the g and h are unique. The reason is that the proof of Hensel's Lemma shows that the factorizations are unique over R/m^n for all n, so that each coefficient is determined mod m^n for all n. We shall eventually see that Henselian rings can be much smaller than complete rings, and exist in abundance.

We next want to prove that a local ring is regular if and only if its completion is regular, and that a complete regular local ring containing a coefficient field is a formal power series ring over a field. We first observe the following:

Lemma. *Let $R \to S$ be a map of rings such that S is flat over R. Then:*

(a) *For every prime Q of S, if Q lies over P in R then $R_P \to S_Q$ is faithfully flat.*

(b) *If S is faithfully flat over R, then for every prime P of R there exists a prime Q of S lying over P.*

(c) *If S is faithfully flat over R and $P_n \supset \cdots \supset P_0$ is a strictly decreasing chain of primes of R then there exists Q_n lying over P_n in S; moreover, for every choice of Q_n there is a (strictly decreasing) chain $Q_n \supset \cdots \supset Q_0$ such that Q_i lies over P_i for every i.*

(d) *If S is faithfully flat over R then* $\dim(R) \leq \dim(S)$.

Proof. (a) We first show that S_Q is flat over R_P. Recall that if W, M are R_P modules, $W \otimes_R M \to W \otimes_{R_P} M$ is an isomorphism (see the bottom of the second page and top of the third page of the Math 614 Lecture Notes of October 31: briefly, $(1/s)w \otimes u = (1/s)w \otimes s(1/s)u = (1/s)sw \otimes (1/s)u = w \otimes (1/s)u$). Thus, to show that if $N \hookrightarrow M$ is an injection of R_P-modules then $S_Q \otimes_{R_P} M \to S_Q \otimes_{R_P} M$ is injective, it suffices to show that $S_Q \otimes_R N \to S_Q \otimes_R M$ is injective. But since S_Q is flat over S and S is flat over R, we have that S_Q is flat over R, and the needed injectivity follows.

Thus S_Q is flat over R_P. Since the maximal ideal PR_P maps into S_Q, faithful flatness is then clear.

(b) When S is faithfully flat over R, R injects into S and the contraction of IS to R is I for every ideal I of R: see Math 614 Problem Set #6, problem **5.** and its solution. Hence, for every prime P, the contraction of PS is disjoint from $R - P$, and so PS is disjoint from the image of $R - P$ in S. Thus, there is a prime ideal Q of S that contains PS and is disjoint from the image of $R - P$, and this means that Q lies over P in R.

(c) The existence of Q_n follows from part (b). By a straightforward induction on n, it suffices to show the existence of $Q_{n-1} \subseteq Q_n$ and lying over P_{n-1}. Then, once we have found $Q_i, \ldots, Q_n$, the problem of finding Q_{i-1} is of exactly the same sort. Consider the map $R_{P_n} \to R_{Q_n}$, which is faithfully flat by part (a). Thus, there exists a prime $\mathcal{Q}_{n-1}$ of R_{Q_n} lying over $P_{n-1}R_{P_n}$. Let Q_{n-1} be the contraction of $\mathcal{Q}_{n-1}$ to R. Since $\mathcal{Q}_{n-1} \subseteq Q_n R_{Q_n}$, we have that $Q_{n-1} \subseteq Q_n$. Since $\mathcal{Q}_{n-1}$ contracts to $P_{n-1}R_{P_n}$, it contracts to P_{n-1} in R, and so Q_{n-1} contracts to P_{n-1} as well.

(d) Given a finite strictly decreasing chain in R, there is a chain in S that lies over it, by part (c), and the inclusions are strict for the chain in S since they are strict upon contraction to R. It follows that $\dim(S) \geq \dim(R)$. $\square$

All of the completions referred to in the next result are m-adic completions.

Proposition. *Let (R, m, K) be a local ring and let $\widehat{R}$ be its completion.*

(a) *The maximal $m_{\widehat{R}}$ ideal of $\widehat{R}$ is the expansion of m to $\widehat{R}$. Hence, $m^n\widehat{R} = m_{\widehat{R}}^n$ for all n.*

(b) *The completion $\widehat{I}$ of any ideal I of R may be identified with $I\widehat{R}$. In particular, $m_{\widehat{R}}$ may be identified with $\widehat{m}$.*

(c) *Expansion and contraction gives a bijection between m-primary ideals of R and $\widehat{m}$-primary ideals of $\widehat{R}$. If $\mathfrak{A}$ is an m-primary ideal of R, $R/\mathfrak{A} \cong \widehat{R}/\widehat{\mathfrak{A}}$.*

(d) *$\dim(R) = \dim(\widehat{R})$, and every system of parameters for R is a system of parameters for $\widehat{R}$.*

(e) *The embedding dimension of R, which is $\dim_K(m/m^2)$, is the same as the embedding dimension of $\widehat{R}$.*

Proof. Part (b) is a consequence of the fact that completion is an exact functor on finitely generated R-modules that agrees with $\widehat{R} \otimes_R \_$: since we have an injection $I \to R$, we get injections $\widehat{I} \hookrightarrow \widehat{R}$ and $I \otimes_R \widehat{R} \hookrightarrow R \otimes_R \widehat{R} \cong \widehat{R}$. The image of $I \otimes_R \widehat{R}$ is $I\widehat{R}$, so that $I \otimes_R \widehat{R} \cong I\widehat{R} \cong \widehat{I} \hookrightarrow \widehat{R}$, as claimed. When $I = m$, the short exact sequence $0 \to m \to R \to K \to 0$ remains exact upon completion, and $\widehat{K} \cong K$, which shows that $m_{\widehat{R}} = m\widehat{R}$, proving (a). When $I = \mathfrak{A}$ is m-primary, we have that $0 \to \mathfrak{A} \to R \to R/\mathfrak{A}$ is exact, and so we get an exact sequence of completions

$$0 \to \widehat{\mathfrak{A}} \to \widehat{R} \to \widehat{R/\mathfrak{A}} \to 0.$$

Because there is a power of m contained in $\mathfrak{A}$, there is a power of m that kills $R/\mathfrak{A}$, and it follows that the natural map $R/\mathfrak{A} \hookrightarrow \widehat{R/\mathfrak{A}}$ is an isomorphism. The bijection between

m-primary ideals of R and $\widehat{m}$-primary ideals of $\widehat{R}$ may be seen as follows: the ideals of R containing m^n correspond bijectively to the ideals of R/m^n, while the ideals of $\widehat{R}$ containing $\widehat{m}^n = m^n\widehat{R}$ correspond bijectively to the ideals of $\widehat{R}$ containing $\widehat{m}^n$. But $R/m^n \cong \widehat{R}/\widehat{m}^n$.

We have that $\dim(\widehat{R}) \geq \dim(R)$ since $\widehat{R}$ is faithfully flat over R. But if $x_1, \ldots, x_n$ is a system of parameters in R, so that $m^N \subseteq (x_1, \ldots, x_n)R$, then $\widehat{m}^n \subseteq (x_1, \ldots, x_n)\widehat{R}$. It follows that $\dim(\widehat{R}) \leq n = \dim(R)$, and so $\dim(\widehat{R}) = \dim(R) = n$, and it is now clear that the images of $x_1, \ldots, x_n$ in $\widehat{R}$ form a system of parameters.

Now, $\widehat{m}/\widehat{m}^2 \cong m\widehat{R}/m^2\widehat{R} \subseteq \widehat{R}/m^2\widehat{R} \cong R/m^2$, and it follows that $\widehat{m}/\widehat{m}^2 \cong m/m^2$, as required. $\square$

Remark. Let K be, for simplicity, an algebraically closed field, and let R be a finitely generated K-algebra, so that the maximal spectrum of R can be thought of as an closed algebraic set X in some $\mathbb{A}_k^N$. To get an embedding, one maps a polynomial ring over K onto R: the least integer N such that $K[x_1, \ldots, x_N]$ can be mapped onto on R as a K-algebra is the smallest integer such that X can be embedded as a closed algebraic set in $\mathbb{A}_K^N$. In this context it is natural to refer to N as the embedding dimension of X, and by extension, of the ring R. We now let K be any field. It is natural to extend this terminology to complete rings containing a field: the integer $\dim_K(m/m^2)$ gives the least N such that $K[[x_1, \ldots, x_n]]$ can be mapped onto the complete local ring (R, m, K) when R contains a field (in which case, as we shall soon see, it has a coefficient field). The term *embedding dimension*, which is reasonably natural for complete equicharacteristic local rings, has been extended to all local rings.

Corollary. *A local ring R is regular if and only if $\widehat{R}$ is regular.*

Proof. By definition, R is regular if and only if it dimension and embedding dimension are equal. The result is therefore clear from parts (d) and (e) of the preceding Proposition. $\square$

We now prove the following characterization of equicharacteristic regular local rings, modulo the final step of proving the existence of coefficient fields in general in characteristic $p > 0$.

Corollary. *Suppose that (R, m, K) be an equicharacteristic local ring. Then R is regular of Krull dimension n if and only if $\widehat{R}$ is isomorphic to a formal power series ring $K[[X_1, \ldots, X_n]]$.*

Proof. We assume the existence of coefficient fields in general for equicharacteristic complete local rings: we give the proof of the remaining case immediately following. By the preceding Corollary, we may assume that R is complete. It is clear that a formal power series ring is regular: we want to prove the converse. We have a field $K_0 \subseteq R$ such that $K_0 \subseteq R \twoheadrightarrow R/m = K$ is an isomorphism. Let $x_1, \ldots, x_n$ be a minimal set of generators of m. By the final Theorem of the preceding lecture, we have a map $K_0[[X_1, \ldots, X_n]] \to R$ sending X_i to x_i. By part (b) of the theorem, since the X_i generate m the map is surjective. By part (c) of the theorem, since $x_1, \ldots, x_n$ is a system of parameters the map is injective. Thus, the map is an isomorphism. $\square$

We now discuss the construction of coefficient fields in local rings $(R,\, m,\, K)$ of prime characteristic $p > 0$ that contain a field when K need not be perfect, which is needed to complete the proof of the result given just above.

Let K be a field of characteristic $p > 0$. Finitely many elements $\theta_1, \ldots, \theta_n$ in $K - K^p$ are called *p-independent* if $[K^p[\theta_1, \ldots, \theta_n] : K^p] = p^n$. This is equivalent to the assertion that

$$K^p \subseteq K[\theta_1] \subseteq K^p[\theta_1,\, \theta_2] \subseteq \cdots \subseteq K^p[\theta_1,\, \theta_2,\, \ldots, \theta_n]$$

is a strictly increasing tower of fields. At each stage there are two possibilities: either θ_{i+1} is already in $K^p[\theta_1, \ldots, \theta_i]$, or it has degree p over it, since θ_{i+1} is purely inseparable of degree p over K^p. Every subset of a p-independent set is p-independent. An infinite subset of $K - K^p$ is called *p-independent* if every finite subset is p-independent.

A maximal p-independent subset of $K - K^p$ is called a *p-base* for K. Zorn's Lemma guarantees the existence of a p-base, since the union of a chain of p-independent sets is p-independent. If Θ is a p-base, then $K = K^p[\Theta]$, for an element of $K - K^p[\Theta]$ could be used to enlarge the p-base. The empty set is a p-base for K if and only if K is perfect.

It is easy to see that Θ is a p-base for K if and only if every element of K is uniquely expressible as a polynomial in the elements of Θ with coefficients in K^p such that the exponent on every θ is at most $p-1$, i.e., the monomials in the elements of Θ of degree at most $p-1$ in each element are a basis for K over K^p.

Now for $q = p^n$, the elements of $\Theta^q = \{\theta^q : \theta \in \Theta\}$ are a p-base for K^q over K^{pq}: in fact we have a commutative diagram:

$$\begin{array}{ccc} K & \xrightarrow{F^q} & K^q \\ \uparrow & & \uparrow \\ K^p & \xrightarrow[F^{pq}]{} & K^{pq} \end{array}$$

where the vertical arrows are inclusions and the horizontal arrows are isomorphisms: here, $F^q(c) = c^q$. In particular, Θ^p is a p-base for K^p, and it follows by multiplying the two bases together that the monomials in the elements of Θ of degree at most $p^2 - 1$ are a basis for K over K^{p^2}. By a straightforward induction, the monomials in the elements of Θ of degree at most $p^n - 1$ in each element are a basis for K over K^{p^n} for every $n \in \mathbb{N}$.

Theorem. *Let $(R,\, m,\, K)$ be a complete local ring of positive prime characteristic p, and let Θ be a p-base for K. Let T be a subset of R that maps bijectively onto Θ, i.e., a lifting of the p-base to R. Then there is a unique coefficient field for R that contains T, namely, $K_0 = \bigcap_n R_n$, where $R_n = R^{p^n}[T]$. Thus, there is a bijection between liftings of the p-base Θ and the coefficient fields of R.*

Proof. Note that any coefficient field must contain some lifting of Θ. Observe also that K_0 is clearly a subring of R that contains T. It will suffice to show that K_0 is a coefficient field and that any coefficient field L containing T is contained in K_0. The latter is easy:

the isomorphism $L \to K$ takes T to Θ, and so T is a p-base for L. Every element of L is therefore in $L^{p^n}[T] \subseteq R^{p^n}[T]$. Notice also that every element of $R^{p^n}[T]$ can be written as a polynomial in the elements of T of degree at most $p^n - 1$ in each element, with coefficients in R^{p^n}. The reason is that any $N \in \mathbb{N}$ can be written as $ap^n + b$ with $a, b \in \mathbb{N}$ and $b \leq p^n - 1$. So t^N can be rewritten as $(t^a)^{p^n} t^b$, and thus if t^N occurs in a term we can rewrite that term so that it only involves t^b by absorbing $(t^a)^{p^n}$ into the coefficient from R^{p^n}. Let us call a polynomial in the elements of T with coefficients in R^{p^n} *special* if the exponents are all at most $p^n - 1$. Thus, every element of $R^{p^n}[T]$ is represented by a special polynomial. We shall also say that a polynomial in elements of Θ with coefficients in K^{p^n} is *special* if all exponents on elements of T are at most $p^n - 1$. Note that special polynomials in elements of T with coefficients in R^{p^n} map mod m onto special polynomials in elements of Θ with coefficients in K^{p^n}.

We next observe that

$$R^{p^n}[T] \cap m \subseteq m^{p^n}.$$

Write the element of $u \in R^{p^n}[T] \cap m$ as a special polynomial in elements of T with coefficients in R^{p^n}. Then its image in K, which is 0, is a special polynomial in the elements of Θ with coefficients in K^{p^n}, and so cannot vanish unless every coefficient is 0. This means that each coefficient of the special polynomial representing u must have been in $m \cap R^{p^n} \subseteq m^{p^n}$. Thus,

$$K_0 \cap m = \bigcap_n (R^{p^n}[T] \cap m) \subseteq \bigcap_n m^{p^n} = (0).$$

We can therefore conclude that K_0 injects into K. It will suffice to show that $K_0 \to K$ is surjective to complete the proof.

Let $\lambda \in K$ be given. Since $K = K^{p^n}[\Theta]$, for every n we can choose an element of $R^{p^n}[T]$ that maps to λ: call it r_n. Then $r_{n+1} \in R^{p^{n+1}}[T] \subseteq R^{p^n}[T]$, and so $r_n - r_{n+1} \in R^{p^n} \cap m \subseteq m^{p^n}$ (the difference $r_n - r_{n+1}$ is in m because both r_n and r_{n+1} map to λ in K). This shows that $\{r_n\}_n$ is Cauchy, and has a limit r_λ. It is clear that $r_\lambda \equiv \lambda \bmod m$, since that is true for every r_n. Moreover, r_λ is independent of the choices of the r_n: given another sequence r'_n with the same property, $r_n - r'_n \in R^{p^n}[T] \cap m \subseteq m^{p^n}$, and so $\{r_n\}_n$ and $\{r'_n\}_n$ have the same limit. It remains only to show that for every n, $r_\lambda \in R^{p^n}[T]$. To see this, write λ as a polynomial in the elements of Θ with coefficients of the form c^{p^n}. Explicitly,

$$\lambda = \sum_{\mu \in \mathcal{F}} c_\mu^{p^n} \mu$$

where $\mathcal{F}$ is some finite set of monomials in the elements of θ. If $\mu = \theta_1^{k_1} \cdots \theta_s^{k_s}$, let $\mu' = t_1^{k_1} \cdots t_s^{k_s}$, where t_j is the element of T that maps to θ_j. For every $\mu \in \mathcal{F}$ and every $n \in \mathbb{N}$, choose $c_{\mu,n} \in R_n$ such that $c_{\mu,n}$ maps to c_μ mod m. Thus, $\{c_{\mu,n}\}_n$ is a Cauchy sequence converging to r_{c_μ}. Let

$$w_n = \sum_{\mu \in \mathcal{F}} c_{\mu,n}^{p^n} \mu'$$

for every $n \in \mathbb{N}$. Then $w_n \in R_n$ and $w_n \equiv \lambda \bmod m$. It follows that

$$\lim_{n\to\infty} w_n = r_\lambda,$$

but this limit is also

$$\sum_{\mu\in\mathcal{F}} r_{c_\mu}^{p^n}\mu' \in R_n.$$

□

Remark. This result shows that if (R, m, K) is a complete local ring that is not a field and K is not perfect, then the choice of a coefficient field is *never* unique. Given a lifting of a p-base T, where $T \neq \emptyset$ because K is not perfect, we can always change it by adding a nonzero element of m to one or more of the elements in the p-base.

Math 615: Lecture of January 13, 2012

Before proceeding further with the investigation of coefficient rings in mixed characteristic, we explore several consequences of the theory that we already have, and then discuss enough homological algebra to use it as a tool in investigating regular rings.

Theorem (Weierstrass preparation theorem). *Let (A, m, K) be a complete local ring and let x be a formal indeterminate over A. Let $f = \sum_{n=0}^{\infty} a_n x^n \in A[[x]]$, where $a_h \in A - m$ is a unit and $a_n \in m$ for $n < h$. (Such an element f is said to be regular in x of order h.) Then the images of $1, x, \ldots, x^{h-1}$ are a free basis over A for the ring $A[[x]]/fA[[x]]$, and every element $g \in A[[x]]$ can be written uniquely in the form $qf + r$ where $q \in A[[x]]$, and $r \in A[x]$ is a polynomial of degree $\leq h - 1$.*

Proof. Let $M = A[[x]]/(f)$, which is a finitely generated $A[[x]]$-module, and so will be separated in the $\mathcal{M}$-adic topology, where $\mathcal{M} = (m, x)A[[x]]$. Hence, it is certainly separated in the m-adic topology. Then $M/mM \cong K[[x]]/(\overline{f})$, where $\overline{f}$ is the image of f under the map $A[[x]] \twoheadrightarrow K[[x]]$ induced by $A \twoheadrightarrow K$: it is the result of reducing coefficients of f mod m. It follows that the lowest nonzero term of $\overline{f}$ has the form cx^h, where $c \in K$, and so $\overline{f} = x^h\gamma$ where γ is a unit in $K[[x]]$. Thus,

$$M/mM \cong K[[x]]/(\overline{f}) = K[[x]]/(x^h),$$

which is a K-vector space for which the images of $1, x, \ldots, x^{h-1}$ form a K-basis. By the first Theorem of the Lecture Notes from January 9, the elements $1, x, \ldots, x^{h-1}$ span $A[[x]]/(f)$ as an A-module. This means precisely that every $g \in A[[x]]$ can be written $g = qf + r$ where $r \in A[x]$ has degree at most $h - 1$.

Suppose that $g'f + r'$ is another such representation. Then $r' - r = (q - q')f$. Thus, it will suffice to show if $r = qf$ is a polynomial in x of degree at most $h - 1$, then $q = 0$ (and $r = 0$ follows). Suppose otherwise. Since some coefficient of q is not 0, we can choose t

such that q is not 0 when considered mod $m^t A[[x]]$. Choose such a t as small as possible, and let d be the least degree such that the coefficient of x^d is not in m^t. Pass to R/m^t. Then q has lowest degree term ax^d, and both a and all higher coefficients are in m^{t-1}, or we could have chosen a smaller value of t. When we multiply by f (still thinking mod m^t), note that all terms of f of degree smaller than h kill q, because their coefficients are in m. There is at most one nonzero term of degree $h+d$, and its coefficient is not zero, because the coefficient of x^h in f is a unit. Thus, qf has a nonzero term of degree $\geq h+d > h-1$, a contradiction. This completes the proof of the existence and uniqueness of q and r. $\square$

Corollary. *Let $A[[x]]$ and f be as in the statement of the Weierstrass Preparation Theorem, with f regular of order h in x. Then f has a unique multiple fq which is a monic polynomial in $A[x]$ of degree h. The multiplier q is a unit, and qf has all non-leading coefficients in m. The polynomial qf called the unique monic associate of f.*

Proof. Apply the Weierstrass Preparation Theorem to $g = x^h$. Then $x^h = qf + r$, which says that $x^h - r = qf$. By the uniqueness part of the theorem, these are the only choices of q, r that satisfy the equation, and so the uniqueness statement follows. It remains only to see that q is a unit, and that r has coefficients in m. To this end, we may work mod $mA[[x]]$. We use $\overline{u}$ for the class of $u \in A[[x]]$ mod $mA[[x]]$, and think of $\overline{u}$ as an element of $K[[x]]$.

Then $x^h - \overline{r} = \overline{q}\overline{f}$. Since $\overline{f}$ is a unit γ times x^h, we must have $\overline{r} = 0$. It follows that $x^h = x^h \overline{q}\gamma$. We may cancel x^h, and so $\overline{q}$ is a unit of of $K[[x]]$. It follows that q is a unit of $A[[x]]$, as asserted. $\square$

Discussion. This result is often applied to the formal power series ring in n-variables, $K[[x_1, \ldots, x_n]]$: one may take $A = K[[x_1, \ldots, x_{n-1}]]$ and $x = x_n$, for example, though, obviously, one might make any of the variable play the role of x. In this case, a power series f is regular in x_n if it involves a term of the form cx_n^h with $c \in K - \{0\}$, and if one takes h as small as possible, f is regular of order h in x_n. The regularity of f of order h in x_n is equivalent to the assertion that under the unique continuous $K[[x_n]]$-algebra map $K[[x_1, \ldots, x_n]] \to K[[x_n]]$ that kills $x_1, \ldots, x_{n-1}$, the image of f is a unit times x_n^h. A logical notation for the image of f is $f(0, \ldots, 0, x_n)$. The Weierstrass preparation theorem asserts that for any g, we can write $f = qg + r$ uniquely, where $q \in K[[x_1, \ldots, x_n]]$, and $r \in K[[x_1, \ldots, x_{n-1}]][x_n]$. In this context, the unique monic associate of f is sometimes call the *distinguished pseudo-polynomial* associated with f. If $K = \mathbb{R}$ or $\mathbb{C}$ one can consider instead the ring of convergent (on a neighborhood of 0) power series. One can carry through the proof of the Weierstrass preparation theorem completely constructively, and show that when g and f are convergent, so are q and r. See, for example, [O. Zariski and P. Samuel, *Commutative Algebra*, Vol. II, D. Van Nostrand Co., Inc., Princeton, 1960], pp. 139–146.

Any nonzero element of the power series ring (convergent or formal) can be made regular in x_n by a change of variables. The same applies to finitely many elements $f_1, \ldots, f_s$, since it suffices to make the product $f_1 \cdots f_s$ regular in x_n, (if the image of $f_1 \cdots f_s$ in $K[[x_n]]$ is nonzero, so is the image of every factor). If the field is infinite one may make use of a K-automorphism that maps $x_1, \ldots, x_n$ to a different basis for $Kx_1 + \cdots + Kx_n$. One can think of f as $f_0 + f_1 + f_2 + \cdots$ where every f_j is a homogeneous polynomial of degree j in

$x_1, \ldots, x_n$. Any given form occurring in $f_j \neq 0$ can be made into a monic polynomial by a suitable linear change of variables, by problem **3.** of Problem Set #3 for Math 614 and its solution.

If K is finite one can still get the image of f under an automorphism to be regular in x_n by mapping $x_1, \ldots, x_n$ to $x_1 + x_n^{N_1}, \ldots, x_{n-1} + x_n^{N_{n-1}}, x_n$, respectively, as in the proof of the Noether normalization theorem, although the details are somewhat more difficult. Consider the monomials that occur in f (there is at least one, since f is not 0), and totally order the monomials so that $x_1^{j_1} \cdots x_n^{j_n} < x_1^{k_1} \cdots x_n^{k_n}$ means that for some i, $1 \leq i \leq n$, $j_1 = k_1$, $j_2 = k_2$, ..., $j_{i-1} = k_{i-1}$, while $j_i < k_i$. Let $x_1^{d_1} \cdots x_n^{d_n}$ be the smallest monomial that occurs with nonzero coefficient in f with respect to this ordering, and let $d = \max\{d_1, \ldots, d_n\}$. Let $N_i = (nd)^{n-i}$, and let θ denote the continuous K-automorphism of $K[[x_1, \ldots, x_n]]$ that sends $x_i \mapsto x_i + {x_n}^{N_i}$ for $1 \leq i \leq n-1$, and $x_n \mapsto x_n$. We claim that $\theta(f)$ is regular in x_n. The point is that the value of $\theta(f)$ after killing $x_1, \ldots, x_{n-1}$ is

$$f(x_n^{N_1}, x_n^{N_2}, \ldots, x_n^{N_{n-1}}, x_n),$$

and the term $c' x_1^{e_1} \cdots x_n^{e_n}$ where $c' \in K - \{0\}$ maps to

$$c' x_n^{e_1 N_1 + e_2 N_2 + \cdots + e_{n-1} N_{n-1} + e_n}.$$

In particular, there is a term in the image of $\theta(f)$ coming from the $x_1^{d_1} \cdots x_n^{d_n}$ term in f, and that term is a nonzero scalar multiple of

$$x_n^{d_1 N_1 + d_2 N_2 + \cdots + d_{n-1} N_{n-1} + d_n}.$$

It suffices to show that no other term cancels it, and so it suffices to show that if for some i with $1 \leq i \leq n$, we have that $e_j = d_j$ for $j < i$ and $e_i > d_i$, then

$$e_1 N_1 + e_2 N_2 + \cdots + e_{n-1} N_{n-1} + e_n > d_1 N_1 + d_2 N_2 + \cdots + d_{n-1} N_{n-1} + d_n.$$

The left hand side minus the right hand side gives

$$(e_i - d_i) N_i + \sum_{j>i} (e_j - d_j) N_j,$$

since $d_j = e_j$ for $j < i$. It will be enough to show that this difference is positive. Since $e_i > d_i$, the leftmost term is at least N_i. Some of the remaining terms are nonnegative, and we omit these. The terms for those j such $e_j < d_j$ are negative, but what is being subtracted is bounded by $d_j N_j \leq d N_j$. Since at most $n-1$ terms are being subtracted, the sum of the quantities being subtracted is strictly bounded by $nd \max_{j>i}\{dN_j\}$. The largest of the N_j is N_{i+1}, which is $(dn)^{n-(i+1)}$. Thus, the total quantity being subtracted is strictly bounded by $(dn)(dn)^{n-i-1} = (dn)^{n-i} = N_i$. This completes the proof that

$$e_1 N_1 + e_2 N_2 + \cdots + e_{n-1} N_{n-1} + e_n > d_1 N_1 + d_2 N_2 + \cdots + d_{n-1} N_{n-1} + d_n,$$

and we see that $\theta(f)$ is regular in x_n, as required.

If the Weierstrass Preparation Theorem is proved directly for a formal or convergent power series ring R over a field K (the constructive proofs do not use *a priori* knowledge that the power series ring is Noetherian), the theorem can be used to prove that the ring R is Noetherian by induction on n. The cases where $n = 0$ or $n = 1$ are obvious: the ring is a field or a discrete valuation ring. Suppose the result is known for the power series ring A in $n-1$ variables, and let R be the power series ring in one variable x_n over A. Let I be an ideal of R. We must show that I is finitely generated over R. If $I = (0)$ this is clear. If $I \neq 0$ choose $f \in I$ with $f \neq 0$. Make a change of variables such that f is regular in x_n over A. Then $I/fR \subseteq R/fR$, which is a finitely generated module over A. By the induction hypothesis, A is Noetherian, and so R/fR is Noetherian over A, and hence I/fR is a Noetherian A-module, and is finitely generated as an A-module. Lift these generators to I. The resulting elements, together with f, give a finite set of generators for I.

Math 615: Lecture of January 18, 2012

Although we shall later give a quite different proof valid for all regular local rings, we want to show how the Weierstrass preparation theorem can be used to prove unique factorization in a formal power series ring.

Theorem. *Let K be a field and let $R = K[[x_1, \ldots, x_n]]$ be the formal power series ring in n variables over K. Then R is a unique factorization domain.*

Proof. We use induction on n. If $n = 0$ then R is a field, and if $n = 1$, R is a discrete valuation ring. In particular, R is a principal ideal domain and, hence, a unique factorization domain.

Suppose that $n > 1$. It suffices to prove that if $f \in m$ is irreducible then f is prime. Suppose that f divides gh, where it may be assumed without loss of generality that g, $h \in m$. Then we have an equation $fw = gh$, and since f is irreducible, we must have that $w \in m$ as well. We may make a change of variables so that all of f, w, g and h are regular in x_n. Moreover, we can replace f, g, and h by monic polynomials in x_n over

$$A = K[[x_1, \ldots, x_{n-1}]]$$

whose non-leading coefficients are in $Q = (x_1, \ldots, x_{n-1})R$: we multiply each by a suitable unit. The equation will hold after we multiply w by a unit as well, although we do not know *a priori* that w is a polynomial in x_n. We can divide $gh \in A[x_n]$ by f which is monic in x_n to get a unique quotient and remainder, say $gh = qf + r$, where the degree of r is less the degree d of f. The Weierstrass preparation theorem guarantees a unique such representation in $A[[x_n]]$, and in the larger ring we know that $r = 0$. Therefore, the equation $gh = qf$ holds in $A[x_n]$, and this means that $q = w$ is a monic polynomial in x_n as well.

By the induction hypothesis, A is a UFD, and so $A[x_n]$ is a UFD. If f is irreducible in $A[x_n]$, we immediately obtain that $f \mid g$ or $f \mid h$. But if f factors non-trivially $f = f_1 f_2$ in

$A[x_n]$, the factors f_1, f_2 must be polynomials in x_n of lower degree which can be taken to be monic. Mod Q, f_1, f_2 give a factorization of x^d, and this must be into two powers of x of lower degree. Therefore, f_1 and f_2 both have all non-leading coefficients in Q, and, in particular their constant terms are in Q. This implies that neither f_1 nor f_2 is a unit of R, and this contradicts the irreducibility of f in R. Thus, f must be irreducible in $A[x_n]$ as well. $\square$

We are next going to treat the theory of regular local rings and develop part of the theory of multiplicities: in the course of that treatment, we will introduce powerful techniques from homological algebra (derived functors, including Tor and Ext, and spectral sequences). One of the auxiliary notions we will utilize is that of an *associated graded* ring or module. We first recall some material about graded rings and modules.

Let H be an additive semigroup with identity 0. A ring R is *graded* by H if it has a direct sum decomposition

$$R = \bigoplus_{h \in H} R_h$$

such that $1 \in R_0$ and for all $h, k \in H$, $R_h R_k \subseteq R_{h+k}$, where

$$R_h R_k = \{rs : r \in R_h,\, s \in R_k\}.$$

It follows that R_0 is a subring of R, and every R_h is an R_0-module. A *grading* of an R-module M is a direct sum decomposition $M = \bigoplus_{h \in H} M_h$ such that for all h, $k \in H$,

$$R_h M_k \subseteq M_{h+k},$$

where

$$R_h M_k = \{ru : r \in R_h,\, u \in M_k\}.$$

An element of R_h for any h is called *homogeneous* or a *form*. If it is nonzero, it is said to have *degree* h. The element 0 is homogeneous, but does not have a degree. In dealing with $\mathbb{N}$-gradings, some authors assign 0 the degree -1 or $-\infty$, but this is not so natural when H is an arbitary semigroup. We leave the degree of 0 undefined. In dealing with $\mathbb{N}$-gradings, the degree of a possibly inhomogeneous element is defined to be the largest degree of a nonzero homogeneous component of the element. If $n \in \mathbb{N}$, the phrase "elements of degree $\leq n$" is then understood to include the 0 element.

When an element $u \in M$ (or R) is written in the form

$$u_{h_1} \oplus \cdots \oplus u_{h_n},$$

with the h_i distinct elements of H, the u_{h_i} are called the *homogeneous components* of u. Those not shown explicitly are 0. Every nonzero element of M or R has a unique (except for the order of the terms) expression as a sum of nonzero homogeneous components of distinct degrees.

We are mainly interested in the case where $H = \mathbb{N}$, but the cases where $H = \mathbb{Z}$, $\mathbb{N}^d$ and $\mathbb{Z}^d$ arise with reasonable frequency. When $H = \mathbb{N}^d$ or $\mathbb{Z}^d$ the term *multidegree* is sometimes used instead of degree. When $n = 2$, the term *bidegree* is sometimes used.

A submodule N of a graded module M is called *homogeneous* or *graded* if whenever $u \in N$, all homogeneous components of u are in N. An equivalent condition is that N be generated by forms. A third equivalent condition is that

$$N = \bigoplus_{h \in H} N \cap M_h,$$

and so a graded submodule inherits a grading from M. In particular, we may refer to *homogeneous* ideals of R. Arbitrary sums and intersections of graded submodules are graded, and the operations may be performed componentwise. If M is a graded module and N a graded submodule there is an obvious way of grading the quotient:

$$M/N = \bigoplus_{h \in H} M_h/N_h.$$

Theorem. *Let M be a Noetherian graded module over a Noetherian graded ring R, where the grading is by $\mathbb{N}$ or $\mathbb{Z}$. Then every associated prime P of M is a homogeneous ideal.*

Proof. If P is an associated prime of M it is the annihilator of a nonzero element

$$u = u_{j_1} + \cdots + u_{j_t} \in M,$$

where the u_{j_ν} are nonzero homogeneous elements of degrees $j_1 < \cdots < j_t$. Choose u such that t is as small as possible. Suppose that

$$r = r_{i_1} + \cdots + r_{i_s}$$

kills u, where for every ν, r_{i_ν} has degree i_ν, and $i_1 < \cdots < i_t$. We shall show that every r_{i_ν} kills u, which proves that P is homogeneous. If not, we may subtract off all the r_{i_ν} that do kill u: the resulting element still kills u. Therefore, to get a contradiction, it suffices to show that r_{i_1} kills u. Since $ru = 0$, the unique least degree term $r_{i_1}u_{j_1} = 0$. Therefore

$$u' = r_{i_1}u = r_{i_1}u_{j_2} + \cdots + r_{i_1}u_{j_t}.$$

If this element is nonzero, its annihilator is still P, since $Ru \cong R/P$ and every nonzero element has annihilator P. Since $r_{i_1}u_{j_\nu}$ is homogeneous of degree $i_1 + j_\nu$, or else is 0, u' has fewer nonzero homogeneous components than u does, contradicting our choice of u. $\square$

Corollary. *If I is a homogeneous ideal of a Noetherian ring R graded by $\mathbb{N}$ or $\mathbb{Z}$, every minimal prime of I is homogeneous.*

Proof. This is immediate, since the minimal primes of I are among the associated primes of R/I. $\square$

Without any finiteness assumptions we have:

Proposition. *If R is graded by $\mathbb{N}$ or $\mathbb{Z}$ and I is a homogeneous ideal, then* $\mathrm{Rad}\,(I)$ *is homogeneous.*

Proof. Let

$$f_{i_1} + \cdots + f_{i_k} \in \mathrm{Rad}\,(I)$$

with $i_1 < \cdots < i_k$ and each f_{i_j} nonzero of degree i_j. We need to show that every $f_{i_j} \in \mathrm{Rad}\,(I)$. If any of the components are in $\mathrm{Rad}\,(I)$, we may subtract them off, giving a similar sum whose terms are the homogeneous components not in $\mathrm{Rad}\,(I)$. Therefore, it will suffice to show that $f_{i_1} \in \mathrm{Rad}\,(I)$. But

$$(f_{i_1} + \cdots + f_{i_k})^N \in I$$

for some $N > 0$. When we expand, there is a unique term formally of least degree, namely $f_{i_1}^N$, and therefore this term is in I, since I is homogeneous. But this means that $f_{i_1} \in \mathrm{Rad}\,(I)$, as required. $\square$

Sometimes we shall use the notation $[M]_n$ for the n th graded component of the graded module M, particularly in contexts where there is also a filtration, for in that case $\{M_n\}_n$ will frequently be used to denote an infinite descending sequence of submodules of M.

Let M be an R-module and $I \subseteq R$ an ideal. The *I-adic filtration* on R is the infinite descending sequence of ideals $\{I^n\}_n$, i.e.,

$$R \supset I \supset I^2 \supset \cdots \supset I^n \supset \cdots .$$

Similarly, the *I-adic filtration* on the R-module M is the sequence $\{I^n M\}_n$. An infinite descending filtration

$$(*) \qquad M = M_0 \supseteq M_1 \supseteq M_2 \supseteq \cdots \supseteq M_n \supseteq \cdots$$

is called *I-stable* if $IM_n \subseteq M_{n+1}$ for all n and $IM_n = M_{n+1}$ for all sufficiently large integers n. The terminology *I-good* (*I-bon* by French authors) is also used. Note that this implies that there is a constant positive integer c such that $M_{n+c} = I^n M_c$ for all $n \in \mathbb{N}$.

Given a filtration $(*)$ of M and a submodule N, N acquires a filtration using the submodules $M_n \cap N = N_n$, called the *inherited filtration*.

The Artin-Rees Lemma asserts precisely that if M is a finitely generated module over a Noetherian ring R and $N \subseteq M$ is a submodule, the filtration on N inherited from the I-adic filtration on M is I-stable. One can generalize this slightly as follows:

Theorem (Artin-Rees Lemma). *Let $N \subseteq M$ be finitely generated modules over the Noetherian ring R, let I be an ideal of R, let $\{M_n\}_n$ be an I-stable filtration of M, and let $\{N_n\}_n$ be the inherited filtration on N. Then $\{N_n\}_n$ is also I-stable.*

Proof. First, $IN_n \subseteq IM_n \cap N \subseteq M_{n+1} \cap N = N_{n+1}$. Choose c such that $M_{n+c} = I^n M_c$ for all c. Then

$$N_{n+c} = I^n M_c \cap N = I^n M_c \cap N_c,$$

since $N_c \supseteq N_{n+c}$, and, by the usual Artin-Rees Lemma applied to $N_c \subseteq M_c$, this is

$$I(I^{n-1}M_c \cap N_c) = IN_{n+c-1}$$

for all sufficiently large n. $\square$

Math 615: Lecture of January 20, 2012

We recall that an $\mathbb{N}$-graded ring R is Noetherian iff R_0 is Noetherian and R is finitely generated over R_0: cf. problem **4.** of Problem Set #5 from Math 614 last semester, and its solution. The generators may be taken to be homogeneous. This means that we may write R as the homomorphic image of $R_0[x_1, \ldots, x_n]$ for some n, where the polynomial ring is graded so that x_i has degree $d_i > 0$. In this situation R_t is the R_0-free module on the monomials $x_1^{a_1} \cdots x_n^{a_n}$ such that $\sum_{i=1}^n a_i d_i = t$. Since all the a_i are at most t, there are only finitely many such monomials, so that every R_t is a finitely generated R_0-module. Thus, since a Noetherian $\mathbb{N}$-graded ring R is a homomorphic of such a graded polynomial ring, all homogeneous components R_t of such a ring R are finitely generated R_0-modules. Moreover, given a finitely generated graded module M over R with homogeneous generators $u_1, \ldots, u_s$ of degrees $d_1, \ldots, d_s$,

$$M_n = \sum_{j=1}^{s} R_{n-d_j} u_j,$$

and since every R_{n-d_j} is a finitely generated R_0-module, every M_n is a finitely generated R_0-module.

The polynomial ring $R_0[x_1, \ldots, x_n]$ also has an $\mathbb{N}^n$-grading: if we let $h = (h_1, \ldots, h_n) \in \mathbb{N}^h$, then

$$[R]_h = R_0 x_1^{a_1} \cdots x_n^{a_n}$$

where $a_i d_i = h_i$, $1 \leq i \leq n$, or 0 if for some i, d_i does not divide h_i. The usual $\mathbb{N}$-grading on a polynomial ring is obtained when all the d_i are specified to be 1.

An $\mathbb{N}$-graded Noetherian A-algebra R is called *standard* if $A = R_0$ and it is generated over R_0 by R_1, in which case it is a homomorphic image of some $A[x_1, \ldots, x_n]$ with the usual grading. The kernel of the surjection $A[x_1, \ldots, x_n] \twoheadrightarrow R$ is a homogeneous ideal.

The *associated graded ring* of R with respect to I, denoted $\mathrm{gr}_I R$, is the $\mathbb{N}$-graded ring such that

$$[\mathrm{gr}_I(R)]_n = I^n/I^{n+1},$$

with multiplication defined by the rule $[i_h][i_k] = [i_h i_k]$, where $i_h \in I^h$, $i_k \in I^k$, and $[i_h]$, $[i_k]$, and $[i_h i_k]$ represent elements of I^h/I^{h+1}, I^k/I^{k+1}, and I^{h+k}/I^{h+k+1}, respectively. It is easy to see that if one alters i_h by adding an element of I^{h+1}, the class of $i_h i_k$ mod I^{h+k+1} does not change since $i_h i_k$ is altered by adding an element of I^{h+k+1}. The same remark applies if one changes i_k by adding an element of I_{k+1}. It follows that multiplication on

these classes is well-defined, and it extends to the whole ring by forcing the distributive law. This ring is generated over R/I by the classes $[i] \in I/I^2$, $i \in I$, and if $i_1, \ldots, i_s$ generate I then $[i_1], \ldots, [i_s]$, thought of in I/I^2, generate $\mathrm{gr}_I R$ over R/I. Thus, $\mathrm{gr}_I R$ is a standard graded R/I-algebra, finitely generated as an R/I-algebra whenever I is finitely generated as an ideal of R. In particular, if R is a Noetherian ring, $\mathrm{gr}_I R$ is a standard Noetherian (R/I)-algebra for every ideal I.

The associated graded ring can also be obtained from the *second Rees ring*, which is defined as $R[It,\, 1/t] \subseteq R[t,\, 1/t]$. More explicitly,

$$R[It,\, 1/t] = \cdots + R\frac{1}{t^2} + R\frac{1}{t} + R + It + I^2t^2 + \cdots .$$

This ring is a $\mathbb{Z}$-graded R-algebra. Let $v = 1/t$. Notice that v is not a unit in $S = R[It, 1/t]$ (unless $I = R$). In fact S/vS is $\mathbb{Z}$-graded: the negative graded components vanish, and the n th nonnegative graded component is $I^n t^n / I^{n+1} t^n \cong I^n/I^{n+1}$, since $I^{n+1}t^{n+1}v = I^{n+1}t^n$. Thus, S/vS may also be thought of as $\mathbb{N}$-graded, and, in fact, $R[It,\, v]/(v) \cong \mathrm{gr}_I R$.

Suppose that R contains a field of K. One may think of $R[It,\, v]$ as giving rise to a family of rings parametrized by K, obtained by killing $v - \lambda$ as λ varies in K. For values of $\lambda \neq 0$, the quotient ring is R, while for $\lambda = 0$, the quotient is $\mathrm{gr}_I R$.

If $\{M_n\}_n$ is an I-stable filtration of an R-module M, then there is an *associated graded module* $\bigoplus_n M_n/M_{n+1}$, which is easily checked to be a $\mathrm{gr}_I R$-module with multiplication determined by the rule $[i_h][m_k] = [i_h m_k]$ for $i_h \in I^h R$ and $m_k \in M_k$, where $[i_h]$, $[m_k]$, and $[i_h m_k]$ are interpreted in I^h/I^{h+1}, M_k/M_{k+1}, and M_{h+k}/M_{h+k+1}, respectively. If $M_{n+c} = I^n M_c$ for $n \in \mathbb{N}$, then this associated graded module is generated by its graded components with indices $\leq c$, namely M/M_1, M_1/M_2, $\ldots$, M_c/M_{c+1}. Thus, if R and M are Noetherian it is a finitely generated $\mathbb{N}$-graded $\mathrm{gr}_I(R)$-module, and is Noetherian. If the filtration is the I-adic filtration, one writes $\mathrm{gr}_I M$ for the associated graded module.

When we refer to a *graded ring* without specifying H, it is understood that $H = \mathbb{N}$. However, when we refer to a graded module M over a graded ring R, our convention is that M is $\mathbb{Z}$-graded. If M is finitely generated, it will have finitely many homogeneous generators: if the least degree among these is $a \in \mathbb{Z}$, then all homogeneous elements of M have degree $\geq a$, so that the n th graded component M_n of M will be nonzero for only finitely many negative values of n. When M is $\mathbb{Z}$-graded it is convenient to have a notation for the same module with its grading shifted. We write $M(t)$ for M graded so that $M(t)_n = M_{t+n}$. For example, $R(t)$ is a free R-module with a homogeneous free generator in degree $-t$: note that $R(t)_{-t} = R_0$ and so contains $1 \in R$.

Let M be a finitely generated graded module over a graded algebra R over $R_0 = A$ where A is an Artin local ring. We define the *Hilbert function* $\mathrm{Hilb}_M(n)$ of M by the rule $\mathrm{Hilb}_M(n) = \ell_A(M_n)$ for all $n \in \mathbb{Z}$, and we define the *Poincaré series* $P_M(t)$ of M by the formula $P_M(t) = \sum_{n=-\infty}^{\infty} \mathrm{Hilb}_M(n) t^n \in \mathbb{Z}[[t]]$. Note that $\ell(M_n)$ is finite for all $n \in \mathbb{Z}$, because each M_n is finitely generated as an A-module, by the discussion of the first paragraph. If A has a coefficient field, lengths over A are the same as vector space dimensions over its coefficient field. Technically, it is necessary to specify A in describing

length. For example, $\ell_{\mathbb{C}}(\mathbb{C}) = 1$, while $\ell_{\mathbb{R}}(\mathbb{C}) = 2$. However, it is usually clear from context over which ring lengths are being taken, and then the ring is omitted from the notation.

Note that $Z[t] \subseteq Z[[t]]$, and that elements of the set of polynomials W with constant ± 1 are invertible. We view $W^{-1}Z[t] \subseteq Z[[t]]$, and so it makes sense to say that a power series in $\mathbb{Z}[[t]]$ is in $W^{-1}\mathbb{Z}[t]$.

Example. Suppose that $R = K[x_1, \ldots, x_d]$ the standard graded polynomial ring. Here, $A = K$ and length over K is the same as vector space dimension. The length of the vector space R_n is the same as the number of monomials $x_1^{k_1} \cdots x_d^{k_d}$ of degree n in the variables $x_1, \ldots, x_d$, since these form a K-vector space basis for R_n. This is the same as the number of d-tuples of nonnegative integers whose sum is n. We can count these as follows: form a string of k_1 dots, then a slash, then a string of k_2 dots, then another slash, and so forth, finishing with a string of k_d dots. For example, $x_1^3 x_2^2 x_4^5$ would correspond to

$$\cdots / \cdot\cdot // \cdot\cdot\cdot\cdot.$$

The result is a string of dots and slashes in which the total number of dots is $k_1 + \cdots + k_d = n$ and the number of slashes is $d - 1$. There is a bijection between such strings and the monomials that we want to count. The string has total length $k + d - 1$, and is determined by the choice of the $d - 1$ spots where the slashes go. Therefore, the number of monomials is $\binom{n+d-1}{d-1}$. The Hilbert function of the polynomial ring is given by the rule $\mathrm{Hilb}_R(n) = 0$ if $n < 0$ and

$$\mathrm{Hilb}_R(n) = \binom{n+d-1}{d-1}$$

if $n \geq 0$. Note that, in this case, the Hilbert function agrees with a polynomial in n of degree $d - 1 = \dim(R) - 1$ for all $n \gg 0$. This gives one formula for the Poincaré series, namely

$$\sum_{n=0}^{\infty} \binom{n+d-1}{d-1} t^n.$$

We give a different way of obtaining the Poincaré series. Consider the formal power series in $Z[[x_1, \ldots, x_d]]$ which is the sum of all monomials in the x_i:

$$1 + x_1 + \cdots + x_d + x_1^2 + x_1 x_2 + \cdots + x_d^2 + \cdots$$

This makes sense because there are only finitely many monomials of any given degree. It is easy to check that this power series is the product of the series

$$1 + x_j + x_j^2 + \cdots + x_j^n + \cdots$$

as j varies from 1 to d: in distributing terms of the product in all possible ways, one gets every monomial in the x_j exactly once. This leads to the formula

$$1 + x_1 + \cdots + x_d + x_1^2 + x_1 x_2 + \cdots + x_d^2 + \cdots = \prod_{j=1}^{d} \frac{1}{1 - x_j}.$$

There is a unique continuous homomorphism $\mathbb{Z}[[x_1, \ldots, x_d]] \to \mathbb{Z}[[t]]$ that sends $x_j \to t$ for all j. Each monomial of degree n in the x_j maps to t^n. It follows that the formal power series

$$1 + x_1 + \cdots + x_d + x_1^2 + x_1x_2 + \cdots + x_d^2 + \cdots$$

maps to $P_R(t)$, but evidently it also maps to $1/(1-t)^d$. This calculation of the Poincaré series yields the identity:

$$\frac{1}{(1-t)^d} = \sum_{n=0}^{\infty} \binom{n+d-1}{d-1} t^n.$$

Theorem. *Let R be a finitely generated graded A-algebra with $R_0 = A$, an Artin ring, and suppose that the generators $f_1, \ldots, f_d$ have positive degrees $k_1, \ldots, k_d$, respectively. Let M be a finitely generated $\mathbb{N}$-graded R-module. Then $P_M(t)$ can be written as the ratio of polynomials in $\mathbb{Z}[t]$ with denominator*

$$(1-t^{k_1}) \cdots (1-t^{k_d}).$$

If M is finitely generated and $\mathbb{Z}$-graded, one has the same result, but the numerator is a Laurent polynomial in $\mathbb{Z}[t, t^{-1}]$.

Proof. If the set of generators is empty, M is a finitely generated A-module and has only finitely many nonzero components. The Poincaré series is clearly a polynomial (respectively, a Laurent polynomial) in t. We use induction on d. We have an exact sequence of graded modules:

$$0 \to \operatorname{Ann}_M f_d \to M \xrightarrow{f_d} M \to M/f_dM \to 0.$$

In each degree, the alternating sum of the lengths is 0. This proves that

$$P_M(t) - t^{d_k} P_M(t) = P_{M/f_dM}(t) - P_{\operatorname{Ann}_M f_d}(t).$$

Since multiplication by f_d is 0 on both modules on the right, each may be thought of as a finitely generated $\mathbb{N}$- (respectively, $\mathbb{Z}$-) graded module over $A[f_1, \ldots, f_{d-1}]$, which shows, using the induction hypothesis, that $(1-t^{k_d})P_M(t)$ can be written as a polynomial (respectively, Laurent polynomial) in t divided by

$$(1-t^{k_1}) \cdots (1-t^{k_{d-1}}).$$

Dividing both sides by $1-t^{k_d}$ yields the required result. □

Math 615: Lecture of January 23, 2012

Remark. Base change over a field K to a field L does not change the Krull dimension of a finitely generated K-algebra, nor of a finitely generated module over such an algebra. A finitely generated K-algebra R is a module-finite extension of a polynomial ring

$K[x_1, \ldots, x_d] \hookrightarrow R$, where $d = \dim(R)$. Then $L[x_1, \ldots, x_d] \cong L \otimes_K K[x_1, \ldots, x_d] \hookrightarrow L \otimes_K R$, ($L$ is free and therefore flat over K), and if $r_1, \ldots, r_s$ span R over $K[x_1, \ldots, x_d]$, then $1 \otimes r_1, \ldots, 1 \otimes r_s$ span $L \otimes R$ over $L[x_1, \ldots, x_d]$.

Evidently, for graded K-algebras R with $R_0 = K$ and graded K-modules M,

$$L \otimes R = \bigoplus_n L \otimes_K R_n$$

and

$$L \otimes_K M = \bigoplus_n L \otimes_K M_n$$

are graded, and their Hilbert functions do not change.

Proposition. *If R is finitely generated and graded over $R_0 = A$, Artin local, and $f \in R$ is homogeneous of degree $k > 0$, then if f is a not a zerodivisor on M, a finitely generated graded R-module, then $P_M(t) = \frac{1}{1-t^k} P_{M/fM}$.*

Proof. This is immediate from the exact sequence

$$0 \to M(-k) \xrightarrow{f} M \to M/fM \to 0$$

of graded modules and degree preserving maps: one has

$$P_M(t) - t^k P_M(t) = P_{M/fM}(t).$$

□

By induction on the number of indeterminates, this gives at once:

Proposition. *Let A be Artin local and $x_1, \ldots, x_d$ indeterminates over A whose respective degrees are $k_1, \ldots, k_d$. Let $R = A[[x_1, \ldots, x_d]]$. Then*

$$P_R(t) = \frac{\ell(A)}{\prod_{i=1}^{d}(1 - t^{k_i})}.$$

□

We note the following facts about integer valued functions on $\mathbb{Z}$ that are eventually polynomial. It will be convenient to assume that functions are defined for all integers even though we are only interested in their values for large integers. We write $f \sim g$ to mean that $f(n) = g(n)$ for all $n \gg 0$.

If f is a function on $\mathbb{Z}$ we define $\Delta(f)$ by the rule

$$\Delta(f)(n) = f(n) - f(n-1)$$

for all n. We define $\Sigma(f)$ by the rule $\Sigma(f)(n) = 0$ if $n < 0$ and

$$\Sigma(f)(n) = \sum_{j=0}^{n} f(j)$$

if $n \geq 0$. Suppose that $d \in \mathbb{N}$. We shall assume that $\binom{n}{d}$, is 0 if n is negative or if $d > n$. It is a polynomial in n of degree d if $n \geq 0$, namely

$$\frac{1}{d!} n(n-1)\cdots(n-d+1).$$

It is obvious that if $f \sim g$ then $\Delta(f) \sim \Delta(g)$, that $\Sigma(f) - \Sigma(g)$ is eventually constant, that $\Delta\Sigma(f) \sim f$, and that $\Sigma\Delta(f) - f$ is equivalent to a constant function. When $f \sim g$ is a nonzero polynomial we refer to the *degree* and *leading coefficient* of f, meaning the degree and leading coefficient of g.

Lemma. *A function f from $\mathbb{Z}$ to $\mathbb{Z}$ that agrees with a polynomial in n for all sufficiently large n is equivalent to a $\mathbb{Z}$-linear combination of the functions $\binom{n}{d}$, and any such $\mathbb{Z}$-linear function has this property. Hence, a polynomial g that agrees with f has, at worst, coefficients in $\mathbb{Q}$, and the leading coefficient has the form $e/d!$, where $e \in \mathbb{Z}$ and $d = \deg(g)$.*

If $f : \mathbb{Z} \to \mathbb{Z}$ then $\Delta(f)$ agrees with a polynomial of degree $d-1$, $d \geq 1$, if and only if f agrees with a polynomial of degree d, and the leading coefficient of $\Delta(f)$ is d times the leading coefficient of f. $\Delta(f) \sim 0$ iff $f \sim c$, where c is a constant integer. For $d \geq 0$, $\Sigma(f)$ $\sim$ a polynomial of degree $d+1$ iff $f \sim$ a polynomial of degree d (nonzero if $d = 0$), and the leading coefficient of $\Sigma(f)$ is the leading coefficient of f divided by $d+1$.

Proof. Every polynomial in n is uniquely a linear combination of the functions $\binom{n}{d}$, since there is exactly one of the latter for every degree $d = 0, 1, 2, \ldots$. Note that $\Delta\binom{n}{d} = \binom{n}{d} - \binom{n-1}{d} = \binom{n}{d-1}$ for all $n \gg 0$, from which the statement about that $\Delta(f)$ is polynomial when f is follows, as well as the statement relating the leading coefficients. Also, if f is eventually polynomial of degree d, then we may apply the Δ operator d times to obtain a nonzero constant function $\Delta^d f$, whose leading coefficient is $d!a$, where a is the leading coefficient of the polynomial that agrees with f, and this is an integer for large n, whence it is an integer. It follows that the leading coefficient of f has the form $e/d!$ for some $e \in \mathbb{Z} - \{0\}$. We may therefore subtract $e\binom{n}{d}$ from f to obtain a $\mathbb{Z}$-valued function that is polynomial of smaller degree than f for large n. We may continue in this way. Thus, the polynomial that agrees with f is a $\mathbb{Z}$-linear combination of the polynomials that agree with the $\binom{n}{d}$. Note also that $\Sigma\binom{n}{d} = \binom{0}{d} + \cdots + \binom{n}{d} = \binom{d}{d} + \cdots + \binom{n}{d}$ for $n \geq d$ and 0 otherwise. The value of the sum shown, when $n \geq d$, is $\binom{n+1}{d+1}$, by a straightforward induction on n. Finally, f is equivalent to a polynomial when Δf is, since $\Sigma\Delta(f) - f$ is equivalent to a constant. $\square$

Theorem. *Let R be a standard graded A-algebra, where (A, μ, K) is Artin local, and let M be a finitely generated graded R-module. Then the Hilbert function $\mathrm{Hilb}_M(n)$ of the finitely generated graded module M is eventually a polynomial in n of degree $\dim(M) - 1$ with a positive leading coefficient, except when M has dimension 0, in which case the Hilbert function is eventually identically 0.*

Proof. The Poincaré series can be written in the form $t^k Q(1-t)/(1-t)^d$ for some $k \leq 0$: we can write a polynomial in t as a polynomial in $1-t$ instead. This is a sum of finitely many terms of the form $mt^k/(1-t)^s$. We have already seen that the coefficient on t^n in $1/(1-t)^s$ is eventually given by a polynomial in n of degree $s-1$, and multiplying by t^k

has the effect of substituting $n-k$ for n in the Hilbert function. A linear combination of polynomials is still a polynomial. It remains to prove the assertion about dimensions.

Since A is Artin, we know that $\mu^s = 0$ for some positive integer s. Then M has a filtration

$$M \supseteq \mu M \supseteq \mu^2 M \supseteq \cdots \supseteq \mu^{s-1} M \supseteq \mu^S M = 0,$$

and each of the $\mu^j M$ is a graded submodule. It follows that the Hilbert function of M is the sum of the Hilbert functions of the modules $\mu^j M/\mu^{j+1}M$. Since the dimension of M is the supremum of the dimensions of the factors, it suffices to prove the result for each $\mu^j M/\mu^{j+1}M$, which is a module over the standard graded K-algebra $R/\mu R$. We have therefore reduced to the case where $A = K$ is a field.

We may apply $L \otimes_K \_$ for some infinite field L, and so we may assume without loss of generality that K is infinite. We use induction on $d = \dim(M)$. Let m be the homogeneous maximal ideal of R, which is generated by 1-forms. If M is 0-dimensional, this is the only associated prime of M, and M has a finite filtration with factors $\cong K$ and is killed by a power of m. Thus, M is a finite-dimensional K-vector space, and M_n is 0 for all $n \gg 0$. Now assume that M has positive dimension. Let

$$N = \bigcup_t \operatorname{Ann}_M m^t.$$

The modules $\operatorname{Ann}_M m^t$ form an ascending chain, so this is the same as $\operatorname{Ann}_M m^t$ for any $t \gg 0$ and is a graded submodule of M of finite length. The Hilbert function of M is the sum of the Hilbert functions of M/N and N, and the latter is eventually 0. Therefore we may study M/N instead of N. In M/N no nonzero element is killed by a power of m (or else its representative in M is multiplied into N by a power of m — but then it would be killed by a power of m, and so it would be in N). Replace M by M/N. Then no element of $M - \{0\}$ is killed by m, and so $m \notin \operatorname{Ass} M$. This means that the associated primes of M cannot cover R_1, which generates m, for then one of them would contain R_1. Thus, we can choose a degree one element f in R_1 that is not a zerodivisor on M. Then $\dim(M/fM) = \dim(M) - 1$, and so $P(n) = \operatorname{Hilb}_{M/fM}(m)$ is eventually a polynomial in n of degree $d-2$ if $d \geq 2$; if $d = 1$, it is constantly 0 for $n \gg 0$. Let $Q(n) = \operatorname{Hilb}_M(n)$. Since $Q(n) - Q(n-1) = P(n)$, Q is a polynomial of degree $d-1$, (if $d = 1$, we can conclude that Q is constant). Since $Q(n)$ is positive for $n \gg 0$, the leading coefficient is positive for all $d \geq 1$. $\square$

Remark. The trick of enlarging the field avoids the need to prove a lemma on homogeneous prime avoidance.

Let (R, m, K) be a local ring, and let M be a finitely generated R-module with m-stable filtration $\mathcal{M} = \{M_n\}_n$. We write $\operatorname{gr}_{\mathcal{M}}(M)$ for the associated graded module $\bigoplus_{n=0}^{\infty} M_n/M_{n+1}$, which is a finitely generated $\operatorname{gr}_I R$-module, and we write $\operatorname{gr}_I M$ in case $\mathcal{M}$ is the I-adic filtration. In this situation we define $H_R(n) = \ell(R/m^{n+1})$, and call this the *Hilbert function of* R, and we write $H_{\mathcal{M}}(n) = \ell(M/M_{n+1})$, the *Hilbert function* of M with respect to the m-stable filtration $\mathcal{M}$. In case $\mathcal{M}$ is the m-adic filtration on M, we write $H_M(n)$ for $\ell(M/m^{n+1}M)$.

Our next objective is the following result:

Theorem. *Let (R, m, K) be local and let M be a nonzero R-module of Krull dimension d. Then for any m-stable filtration $\mathcal{M}$ of M, $H_{\mathcal{M}}(n)$ is eventually a polynomial in n of degree d.*

First note that $\mathrm{gr}_c MM = \bigoplus_n M_n/M_{n+1}$, then for all n, $H_{\mathcal{M}}(n) = \ell(M/M_{n+1}) = \sum_{i=0}^{n} \ell(M_i/M_{i+1})$ since M/M_{n+1} has a filtration with the M_i/M_{i+1} as factors, $0 \leq i \leq n$. This says that $\Sigma\,\mathrm{Hilb}_{\mathrm{gr}\mathcal{M}} = H_{\mathcal{M}}$. This shows that $H_{\mathcal{M}}(n)$ is eventually polynomial in n of degree $\dim\left(\mathrm{gr}_{\mathcal{M}}(M)\right)$. Once we complete the proof of the theorem above, it will follow that $\dim\left(\mathrm{gr}_{\mathcal{M}}(M)\right) = \dim(M)$, and, in particular, $\dim\left(\mathrm{gr}_m(R)\right) = \dim(R)$ for any local ring R. Before proving the theorem we need the following observation.

Proposition. *Let (R, m, K) be local, and let $0 \to N \to M \to \overline{M} \to 0$ be an exact sequence of finitely generated R-modules. Let $\mathcal{M}$ be an M-stable filtration on M, let $\overline{\mathcal{M}}$ be the induced filtration on $\overline{M}$ whose n th term in the image of M_n, and let $\mathcal{N}$ be the inherited filtration on N, whose n th term is $M_n \cap N$. Then the sequence*

$$0 \to \mathrm{gr}_{\mathcal{N}}(N) \to \mathrm{gr}_{\mathcal{M}}(M) \to \mathrm{gr}_{\overline{\mathcal{M}}}(\overline{M}) \to 0$$

is an exact sequence of graded modules with degree-preserving maps, and so

$$H_{\mathcal{M}}(n) = H_{\mathcal{N}}(n) + H_{\overline{\mathcal{M}}}(n)$$

for all n.

Proof. For every n, the sequence

$$(*_n) \qquad 0 \to N_n \to M_n \to (M/N)_n \to 0$$

is exact by construction: $(M/N)_n$ is the image of M_n by definition, and the kernel of $M_n \to (M/N)_n$ is the same as the kernel of $M_n \to M/N$, which is $N \cap M_n = N_n$ by definition. The exactness of $(*_n)$ and $(*_{n+1})$ implies the exactness of the sequence of quotients

$$0 \to \frac{N_n}{N_{n+1}} \to \frac{M_n}{M_{n+1}} \to \frac{(M/N)_n}{(M/N)_{n+1}} \to 0$$

for all n. $\square$

In order to prove the Theorem, we may again consider $N = \bigcup_t \mathrm{Ann}_N m^t$, which will be the same as $\mathrm{Ann}_M m^t$ for any $t \gg 0$. Any m-stable filtration on N is eventually 0, and so $H_{\mathcal{N}}(n) = \ell(N)$ for all sufficiently large n. If M is 0-dimensional we are done. If not, by the Proposition it suffices to consider M/N instead of M.

Math 615: Lecture of January 25, 2012

We have reduced the problem of proving that the degree of the Hilbert function of $M \neq 0$ is the Krull dimension of M to the case where $m \notin \mathrm{Ass}(M)$. Here M is a finitely generated module over the local ring (R, m, K).

Before proceeding further, we generalize the notion of Hilbert functions to a larger context. Let M be a finitely generated module over the local ring (R, m, K) and let $\mathfrak{A}$ be any ideal of R that is primary to m modulo the annihilator I of M. That is, $\mathfrak{A} + I$ is m-primary, or, equivalently, $\mathfrak{A}(R/I)$ is primary to $m/I \subseteq R/I$. Note that $\dim(M) = \dim(R/I)$, by definition. Then for any $\mathfrak{A}$-stable filtration $\mathcal{M} = \{M_n\}_n$, we define $H_{\mathcal{M}}(n) = \ell(M/M_{n+1})$. We may always use the $\mathfrak{A}$-adic filtration, in which case we write $H_{\mathfrak{A},M}(n) = \ell(M/\mathfrak{A}^n M)$. The calculation of the values of this function is unaffected if we replace R by R/I: all of the modules involved are killed by I, and multiplying any of these modules by $\mathfrak{A}$ is the same as multiplying it by the expansion of $\mathfrak{A}$ to R/I. Thus, without loss of generality, we may readily assume that M is faithful and that $\mathfrak{A}$ is m-primary, by passing to R/I as indicated.

The following result will complete the proof of the Theorem from the previous lecture:

Theorem. *Let M be a finitely generated nonzero module over a local ring (R, m, K). For any $\mathfrak{A}$-stable filtration $\mathcal{M}$ on M, $H_{\mathcal{M}}(n)$ is eventually a polynomial that agrees with $\Sigma\,\mathrm{Hilb}_{\mathrm{gr}_{\mathcal{M}}}(M)$. The degree and leading coefficient of this polynomial are independent of the choice of the $\mathfrak{A}$-stable filtration $\mathcal{M}$. The degree is the same as $\dim(M)$, and also the same as $\dim\big(\mathrm{gr}_{\mathcal{M}}(M)\big)$.*

Proof. We kill $\mathrm{Ann}_R M$, and so assume that M is faithful over R, that $\mathfrak{A}$ is m-primary, and that $\dim(M) = \dim(R)$. Since $\mathrm{gr}_{\mathcal{M}}(M)$ is a finitely generated module over $\mathrm{gr}_{\mathfrak{A}} R$, which is a standard graded algebra over the Artin local ring $R/\mathfrak{A}$, we have that $\mathrm{Hilb}_{\mathrm{gr}_{\mathcal{M}}(M)}(n)$ is a polynomial of degree $\dim\big(\mathrm{gr}_{\mathcal{M}}(M)\big) - 1$. Since

$$\ell(M_{n+1}) = \ell(M/M_1) + \ell(M_1/M_2) + \cdots + \ell(M_n/M_{n+1}),$$

it follows that $H_{\mathcal{M}}(n)$ is polynomial of degree $\dim\big(\mathrm{gr}_{\mathcal{M}}(M)\big)$.

We know compare the leading term of the polynomial coming from $\mathcal{M} = \{M_n\}_n$ with the polynomial given by the $\mathfrak{A}$-adic filtration. Since $\mathfrak{A}M_n \subseteq M_{n+1}$ for all n, $\mathfrak{A}^n M \subseteq M_n$ for all n, and $\ell(M/M_n) \leq \ell(M/\mathfrak{A}^n M)$. Let c be such that $M_{n+c} = \mathfrak{A}^n M_c$ for all $n \geq c$. Then $M_{n+c} \subseteq \mathfrak{A}^n m$, and so $\ell(M/M_{n+c}) \geq \ell(M/\mathfrak{A}^n M)$ for all n. Thus,

$$H_{\mathcal{M}}(n+c) \geq H_{\mathfrak{A},M}(n) \geq H_{\mathcal{M}}(n)$$

for all n, and so $H_{\mathfrak{A},M}$ is trapped between two polynomials with the same degree and leading coefficient. Therefore all three have the same degree and leading coefficient. This shows that the leading term of the polynomial in independent of the choice of $\mathcal{M}$.

We next show that the degree is independent of the choice of $\mathfrak{A}$. We can choose c such that $m^b \subseteq \mathfrak{A} \subseteq m$, and then $m^{nb} \subseteq \mathfrak{A}^n \subseteq m^n$ for all n, and so

$$\ell(M/m^{nb}) \geq \ell(M/\mathfrak{A}^n M) \geq \ell(M/m^n M)$$

which shows that $H_{\mathfrak{A},M}$ is eventually a polynomial trapped between $H_M(n)$ and $H_M(bn)$. The latter two are eventually polynomials of the same degree, and so $H_{\mathcal{M}}(n)$ must be as well, since we know that it is eventually polynomial.

It remains to see that the degree is $d = \dim(M) = \dim(R)$. To see that the degree is $\leq \dim(R)$, we choose $\mathfrak{A}$ to be generated by a system of parameters $x_1, \ldots, x_d \in m$. Then $\mathrm{gr}_{\mathfrak{A}}(R)$ is generated over $R/\mathfrak{A}$ by the classes of the elements x_i in $\mathfrak{A}/\mathfrak{A}^2$. Since the algebra is generated by d elements of degree 1, the denominator of the Poincaré series for $\mathrm{gr}_{\mathcal{M}}M$ is $(1-t)^d$, at worst, and this shows that the degree of the Hilbert polynomial of the associated graded module is at most $d-1$, which yields the upper bound d for the degree of $H_{\mathcal{M}}(n)$.

The last step is to show that the degree is at least d. We use induction on $\dim(M)$: the case where $d = 0$ is trivial. Since the degree is independent of both the m-primary ideal $\mathfrak{A}$ chosen and the specific $\mathfrak{A}$-stable filtration used, it suffices to consider the m-adic filtration. Moreover, we have already shown that one need only consider the case when no element of M is killed by m (for we may kill $\bigcup_t \mathrm{Ann}_M m^t$). Thus, we may assume that $m \notin \mathrm{Ass}(M)$, and by prime avoidance we may choose $f \in m$ such that f is not a zerodivisor on M. Consider the short exact sequence

$$0 \to M \xrightarrow{f} M \to M/fM \to 0.$$

Place the m-adic filtration on the central copy of M, the inherited m-adic filtration on the left hand copy of M (using that it is isomorphic with fM to think of it as a submodule of M: specifically, $M_n = m^n M :_M f$), and the image of the m-adic filtration of M on M/fM: this is the same as the m-adic filtration on M/fM. By the Proposition from last time, we find that $H_M(n) - H_{\mathcal{M}}(n) = H_{M/fM}(n)$. By what was proved above, the two polynomials on the left have the same leading term: when we subtract, we get a polynomial of lower degree. By the induction hypothesis, the polynomial on the right has degree $\dim(M/fM) = d-1$. It follows that the degree of $H_M(n)$ is at least d. □

For emphasis, we state the following consequence separately.

Corollary. *If M is a finitely generated module over the local ring (R, m), and $\mathfrak{A}$ is m-primary, M, $\mathrm{gr}_m(M)$, and $\mathrm{gr}_{\mathfrak{A}}(M)$ have the same Krull dimension.* □

Note that if (R, m, K) is local, for any m-primary ideal $\mathfrak{A}$, we have that $R/\mathfrak{A}^n \cong \widehat{R}/\mathfrak{A}^n\widehat{R}$ (recall that $\mathfrak{A}\widehat{R} \cong \widehat{\mathfrak{A}}$), and that for any finitely generated R-module M, $\widehat{M}/\mathfrak{A}^n\widehat{M} \cong M/\mathfrak{A}^n M$ for all n. The completions referred to here are all m-adic. This shows that we may identify $\mathrm{gr}_{\mathfrak{A}}(R) \cong \mathrm{gr}_{\widehat{\mathfrak{A}}}\widehat{R}$, and $\mathrm{gr}_{\mathfrak{A}}(M) \cong \mathrm{gr}_{\widehat{\mathfrak{A}}}\widehat{M}$; in particular, we have these identifications when $\mathfrak{A} = m$.

We also note:

Proposition. *If (R, m, K) is local and $\mathrm{gr}_m(R)$ is a domain then R and $\widehat{R}$ are domains.*

Proof. The result for R implies the result for $\widehat{R}$, since their associated graded rings are the same. Suppose the result is false, so that $f, g \in m - \{0\}$ are such that $fg = 0$. Since $f \neq 0$, we can choose $s \in \mathbb{N}$ such that $f \in m^s - m^{s+1}$, and, similarly, we can choose $t \in \mathbb{N}$ such that $g \in m^t - m^{t+1}$. Let $[f]$ indicate the class of f in m^s/m^{s+1} and $[g]$ the class of $g \in m^t - m^{t+1}$. Then $[f]$ and $[g]$ are nonzero homogeneous elements of $\mathrm{gr}_m(R)$, and their product is $[fg] = [0]$, contradicting that $\mathrm{gr}_m(R)$ is a domain. □

Note that the completion of a local domain need not be a domain in general. The polynomial $f = y^2 - x^2(1+x)$ is irreducible in the polynomial ring $\mathbb{C}[x,y]$, since $1+x$ is not a square (even in the fraction field), and so $x^2(1+x)$ is not a square. Thus, it generates a prime ideal which remains prime if we localize at (x,y). Let $R = \mathbb{C}[x,y]_{(x,y)}/(f)$, which is a local domain. Its completion $\widehat{R}$ is $\mathbb{C}[[x,y]]/(f)$, but now f is reducible: $1+x$ is a perfect square in $\mathbb{C}[[x]]$, by Hensel's lemma (or use Newton's binomial theorem to give an explicit formula for the power series square root of $1+x$). Instead of $\mathbb{C}$, we could have used any field of characteristic different from 2. In characteristic 2, $y^3 - x^3(1+x)$ gives a similar example.

We can use associated graded rings to characterize regular local rings.

Theorem. *A local ring (R, m, K) is regular if and only if $\mathrm{gr}_m(R)$ is a polynomial ring in d variables over K, in which case $d = \dim(R)$.*

Proof. Let $x_1, \ldots, x_s$ be a minimal set of generators for m, and note that m/m^2 is the K-vector space of forms of degree 1 in $\mathrm{gr}_m(R)$. Now $d = \dim(R) = \dim\big(\mathrm{gr}_m(R)\big)$. If $\mathrm{gr}_m(R)$ is polynomial, it must be the polynomial ring in s variables, and since it has dimension both s and d we have that $s = d$, which shows that R is regular. If R is regular, we know that $\mathrm{gr}_m(R)$ is generated over K by d one forms, and has dimension d. Thus, it is a homomorphic image of the polynomial ring in d variables over K, where the variables map to the $[x_i]$. Since the dimension of $\mathrm{gr}_m(R)$ is d, there cannot be any kernel: a proper homomorphic image of a polynomial ring in d variables has Krull dimension $< d$. This shows that $\mathrm{gr}_m(R)$ is a polynomial ring in d variables. $\square$

Since the associated graded ring of a regular local ring is a domain, we have at once:

Corollary. *A regular local ring is a domain.* $\square$

Math 615: Lecture of January 27, 2012

Let (R, m, K) be local, let M be a nonzero finitely generated R-module with annihilator I of Krull dimension d, and let $\mathfrak{A} \subseteq R$ be an ideal such that $\mathfrak{A}(R/I)$ is primary to $m/I \subseteq R/I$. We define the multiplicity of M with respect to $\mathfrak{A}$ to be $d!$ times the leading coefficient of the Hilbert function of M. This function is integer-valued, and the equivalent polynomial has degree d, and is therefore a $\mathbb{Z}$-linear combination of the polynomials $\binom{n}{j}$, $0 \leq j \leq d$, and $\binom{n}{d}$ must occur with positive coefficient. Therefore, the multiplicity is a positive integer. It may also be described as

$$d! \lim_{n\to\infty} \frac{\ell(M/\mathfrak{A}^{n+1}M)}{n^d}.$$

If $\mathfrak{A} = m$, we simply refer to the *multiplicity* of M. In particular we may refer to the *multiplicity* of R itself.

We shall be particularly interested in determining multiplicities of rings with respect to parameter ideals, i.e., ideals generated by a system of parameters. In this case, the

multiplicity can be recovered as an alternating sum of lengths of homology modules for a certain homology theory, Koszul homology, which can be viewed as a special case of Tor. The proof that we shall give of our result in this direction will depend on the theory of spectral sequences.

We shall also use Tor and related homological ideas to prove properties of regular rings. The only known proofs that a localization of a regular local ring at prime is again regular are by these methods, and the proof of unique factorization also depends on these ideas.

Before beginning the development of these homological methods, we want to make a few more comments about associated graded rings and multiplicities.

Note that the multiplicity of any regular local ring is 1. To check this, observe that the associated graded ring is $K[x_1, \ldots, x_d]$ where d is the dimension, and the Hilbert polynomial corresponds to $\binom{n+d-1}{d-1}$. The Hilbert function of the local ring is obtained by summing the values of $\binom{t+d-1}{d-1}$ for $t = 0, \ldots, n$. However, we note that the number of monomials in $x_1, \ldots, x_n$ of degree $\leq n$ is the same as the number of monomials of degree precisely n in $x_0, x_1, \ldots, x_d$: there is a bijection obtained by substituting $x_0 = 1$. Thus, the Hilbert function of the regular ring corresponds to $\binom{n+d}{d}$, which has leading coefficient $1/d!$, and this shows that the multiplicity is 1.

Let $R = K[[x_1, \ldots, x_d]]$ and let $f \in R$ have a lowest degree term of degree $\mu > 0$. The multiplicity of the ring R/f is μ. We shall check this by giving a technique for calculating associated graded rings of quotients.

If (R, m, K) is local and $f \in R - \{0\}$, there is always a unique integer $t \in N$ such that $f \in m^t - m^{t+1}$. Then $[f] \in m^t/m^{t+1} = [\mathrm{gr}_m(R)]_t$ is homogeneous and nonzero: we denote this element $\mathcal{L}(f)$, and call it the *leading form* of f. Note that $\mathcal{L}(f)$ is in $\mathrm{gr}_m(R)$, not in R. If $I \subseteq R$, we write $\mathcal{L}(I)$ for the ideal of $\mathrm{gr}_m(R)$ generated by all leading forms of elements of $I - \{0\}$: this is evidently a homogeneous ideal. In attempting to find generators for $\mathcal{L}(I)$, it is not in general sufficient to take the leading forms of a set of generators of I. See problems **1.** and **5.** of Problem Set #2. However, it is easy to see that this is sufficient for a nonzero principal ideal in a formal power series ring $K[[x_1, \ldots, x_d]]$ over a field K: when one multiplies by another nonzero power series, the leading form of the product is the product of the leading forms.

Proposition. *Let (R, m, K) be local and let I be a nonzero ideal of R. Then*

$$\mathrm{gr}_{m/I}(R/I) \cong \mathrm{gr}_m R/\mathcal{L}(I).$$

Proof. We have that

$$[\mathrm{gr}_{m/I}(R/I)]_n = (m/I)^n/(m/I)^{n+1} \cong (m^n + I)/(m^{n+1} + I) \cong m^n/\big(m^n \cap (m^{n+1} + I)\big).$$

But if $u \in m^{n+1}$, $i \in I$, and $u + i \in m^n$, then $u \in m^n$, and so $u \in m^n \cap I$. This shows that $m^n \cap (m^{n+1} + I) = m^{n+1} + (m^n \cap I)$, and so

$$[\mathrm{gr}_{m/I}(R/I)]_n \cong m^n/(m^{n+1} + m^n \cap I) \cong (m^n/m^{n+1})/W_n,$$

where W_n is the image of $m^n \cap I$ in $m^n/m^{n+1} = [\mathrm{gr}_m(R)]_n$. But if $f \in m^n \cap I$, then if $f \in m^{n+1}$ the image of f in $[\mathrm{gr}_m(R)]_n$ is 0, while if $f \notin m^{n+1}$ then $[f] \in m^n/m^{n+1}$ is precisely a nonzero leading form in degree n of an element of I, and the result now follows. $\square$

We now come back to the problem of calculating the associated graded ring of $R = K[[x_1, \ldots, x_d]]/(f)$ where f has nonzero leading form L of degree $\mu \geq 1$. From the remarks we have made, $\mathrm{gr}_m(R) \cong K[x_1, \ldots, x_d]/(L)$. We have a short exact sequence $0 \to T(-\mu) \xrightarrow{L} T \to T/(L) \to 0$, where $T = K[x_1, \ldots, x_d]$. Since the Hilbert function of T corresponds to $\binom{n+d-1}{d-1}$, the Hilbert function of $T/(L)$ corresponds to $\binom{n+d-1}{d-1} - \binom{n-\mu+d-1}{d-1}$. When we sum, we get $\binom{n+d}{d} - \binom{n-\mu+d}{d}$ up to a constant. It is easy to check that if $P(n)$ has leading coefficient a, then $P(n) - P(n-\mu)$ has leading coefficient μa. Thus, the leading coefficient is $\mu/d!$, and so the multiplicity is μ, as asserted earlier.

We want to make some comments on regular sequences. Recall that x is *not a zerodivisor* on M, or is a *nonzerodivisor* on M if for $u \in M$, $xu = 0$ implies that $u = 0$: in other words, the map on M given by multiplication by u is injective. We define an *improper regular sequence* $x_1, \ldots, x_d$ in R on an R-module M to be a sequence with the property that x_1 is not a zerodivisor on M and for all j, $1 < j \leq d$, x_j is a nonzerodivisor on $M/(x_1, \ldots, x_{j-1})M$. We allow the empty sequence as an improper regular sequence.

An improper regular sequence on the R-module M is called a *regular sequence* if, moreover, $(x_1, \ldots, x_d)M \neq M$. Thus, a regular sequence is an improper regular sequence. One might use the term *possibly improper* instead, but that necessitates many uses of the extra word "possibly." A regular sequence may sometimes be referred to as a *proper* regular sequence to emphasize the condition that $(x_1, \ldots, x_d)M \neq M$: the word "proper" is redundant here. The empty sequence is a regular sequence on M provided that $M \neq 0$.

Regular sequences are also called *Rees sequences* in honor of David Rees, who was one of the first to make use of such sequences. Some authors also refer to *R-sequences* on M, but we avoid this term.

A nonzero element of a domain R always gives an improper regular sequence of length one on R, which will be a regular sequence precisely when the element is not a unit. 2 is a regular sequence in $\mathbb{Z}$, while 2, 1 is an improper regular sequence. A unit α of R followed by any sequence of elements thereafter is an improper regular sequence on M, since the unit is not a zerodivisor even if $M = 0$, while $M/\alpha M = 0$ — every element of R is a nonzerodivisor on the 0 module. This should help explain why one usually wants to restrict to proper regular sequences.

Regular sequences are not permutable in general, although we shall prove theorems in this direction later. The sequence $z - 1$, xz, yz is a regular sequence in the polynomial ring $K[x, y, z]$ in three variables over a field K, while $xz, yz, z - 1$ is not: in the quotient by (xz), yz kills the class $[x]$ of x, which is not 0.

It is a straightforward exercise to show that in a UFD, two elements that generate a proper ideal form a regular sequence of length 2 if and only if they are relatively prime, i.e., if and only if they have no prime factor in common.

In a local ring, any regular sequence is part of a system of parameters: the first element is not a zerodivisor and so not in any associated prime. In particular, it is not in any minimal prime, and killing the first element must drop the dimension of the ring by 1. The rest of the argument is a straightforward induction. We also note:

Proposition. *A local ring (R, m) is regular if and only if m is generated by a regular sequence, in which case any minimal set of generators of m is a regular sequence.*

Proof. If m is generated by a regular sequence, it is generated by a system of parameters, which shows that the dimension of R is equal to the least number of generators of m. Now suppose that R is regular, and that $x = x_1, x_2, \dots, x_d$ is a minimal set of generators of m. We use induction on d: the case $d = 1$ is clear. Suppose $d > 1$. Note that $x \in m - m^2$. Since R is a domain, x is not a zerodivisor. In R/xR, the dimension and the least number of generators of the maximal ideal have both dropped by one, and are therefore still equal, so that R/xR is again regular. Moreover, the images of $x_2, \dots, x_n$ are a minimal set of generators of m/xR. The result now follows from the induction hypothesis. $\square$

A minimal set of generators of the maximal ideal of a regular local ring R is called a *regular* system of parameters. The term is not defined except in regular local rings.

We now want to begin our treatment of Tor, for which we need to talk about projective resolutions. Let R be any ring, and M be any R-module. Then it is possible to map a projective R-module P onto M. In fact one can choose a set of generators $\{u_\lambda\}_{\lambda\in\Lambda}$ for M, and then map the free module $P = \bigoplus_{\lambda\in\Lambda} Rb_\lambda$ on a correspondingly indexed set of generators $\{b_\lambda\}_{\lambda\in\Lambda}$ onto M: there is a unique R-linear map $P \twoheadrightarrow M$ that sends $b_\lambda \to u_\lambda$ for all $\lambda \in \Lambda$. Whenever we have such a surjection, the kernel M' of $P \twoheadrightarrow M$ is referred to as a *first module of syzygies* of M. We define k th modules of syzygies by recursion: a k th module of syzygies of a first module of syzygies is referred to as a $k+1$ st module of syzygies.

There is even a completely canonical way to map a free module onto M. Given M let $\mathcal{F}(M)$ denote the module of all functions from M to R that vanish on all but finitely many elements of M. This module is R-free on a basis $\{b_m\}_{m\in M}$ where b_m is the function that is 1 on m and 0 elsewhere. The map that sends $f \in \mathcal{F}(M)$ to $\sum_{m\in M} f(m)m$ is a canonical surjection: note that it maps b_m to m. The sum makes sense because all but finitely many terms are 0.

By a *projective resolution* of M we mean an infinite sequence of projective modules

$$\cdots \to P_n \to \cdots \to P_1 \to P_0 \to 0$$

which is exact at P_i for $i > 0$, together with an isomorphism $P_0/\mathrm{Im}\,(P_1) \cong M$. Recall the exactness at P_i means that the image of the map into P_i is the kernel of the map from P_i. Note that it is equivalent to give an exact sequence

$$\cdots \to P_n \to \cdots \to P_1 \to P_0 \twoheadrightarrow M \to 0$$

which is exact everywhere. A projective resolution is called *finite* if $P_n = 0$ for all sufficiently large n.

We can always construct a projective resolution of M as follows: map a projective module P_0 onto M. Let Z_1 be the kernel, a first module of syzygies of M. Map a projective module P_1 onto Z_1. It follows that $P_1 \to P_0 \to M \to 0$ is exact, and Z_2, the kernel of $P_1 \to P_0$, is a second module of syzygies of M. Proceed recursively. If $P_n \to \cdots \to P_1 \to P_0 \to M \to 0$ has been constructed so that it is exact (except at P_n), let Z_n be the kernel of $P_n \to P_{n-1}$), which will be an n th module of syzygies of M. Simply map a projective P_{n+1} onto Z_n, and use the composite map

$$P_{n+1} \twoheadrightarrow Z_n \subseteq P_n$$

to extend the resolution.

One can form a completely canonical resolution that is free, not merely projective, by taking $P_0 = \mathcal{F}(M)$ together with the canonical map $\mathcal{F}(M) \twoheadrightarrow M$ to begin, and choosing $P_{n+1} = \mathcal{F}(Z_n)$ along with the canonical map $\mathcal{F}(Z_n) \to Z_n$ at the recursive step. We refer to this as the *canonical* free resolution of M. We shall see that one can compute Tor using any projective resolution, but it is convenient for the purpose of having an unambiguous definition at the start to have a canonical choice of resolution.

If M is an R-module, we define $\mathrm{Tor}_n^R(M, N)$ to be the n th homology module of the complex $\cdots \to P_n \otimes_R N \to \cdots \to P_1 \otimes_R N \to P_0 \otimes_R N \to 0$, i.e., $H_n(P_\bullet \otimes_R N)$, where $P_\bullet$ is the canonical free resolution of M. The n th homology module of a complex $G_\bullet$ is Z_n/B_n where Z_n is the kernel of the map $G_n \to G_{n-1}$ and B_n is the image of the map $G_{n+1} \to G_n$.

Despite the unwieldy definition, the values of $\mathrm{Tor}^R(M, N)$ are highly computable. One might take the view that all of the values of Tor make a small correction for the fact that tensor is not an exact functor. The values of Tor are not always small, but one can often show that Tor vanishes, or has finite length, and the information it can provide is very useful.

Math 615: Lecture of January 2, 2012

We make some conventions that will be useful in dealing with complexes.

By a *sequence* of R-modules (and maps, although they will usually not be mentioned) we mean a family of modules $\{M_n\}_{n\in\mathbb{Z}}$ indexed by the integers, and for every $n \in \mathbb{Z}$ an R-linear map $d_n : M_n \to M_{n-1}$. The sequence is called a *complex* if $d_n \circ d_{n+1} = 0$ for all $n \in \mathbb{Z}$. This is equivalent to the condition that $\mathrm{Im}\,(d_{n+1}) \subseteq \mathrm{Ker}\,(d_n)$ for all n. We often use the notation $M_\bullet$ to denote a complex of modules. We define $H_n(M_\bullet)$ to be $\mathrm{Ker}\,(d_n)/\mathrm{Im}\,(d_{n+1})$, the n th *homology* module of $M_\bullet$. We shall make the homology modules into a new complex, somewhat artificially, by defining all the maps to be 0. Given a complex $M_\bullet$ we make the convention $M^n = M_{-n}$ for all $n \in \mathbb{Z}$. Thus, the same complex may be indicated either as

$$\cdots \to M_{n+1} \to M_n \to M_{n-1} \to \cdots \to M_1 \to M_0 \to M_{-1} \to$$

$$\cdots \to M_{-(n-1)} \to M_{-n} \to M_{-(n+1)} \to \cdots$$

or as

$$\cdots \to M^{-(n+1)} \to M^{-n} \to M^{-(n-1)} \to \cdots \to M^{-1} \to M^0 \to M^1 \to$$

$$\cdots \to M^{n-1} \to M^n \to M^{n+1} \to \cdots$$

for which we write $M^\bullet$. With these conventions, $H^i(M^\bullet) = H_{-i}(M_\bullet)$. Thus, there really isn't any distinction between cohomology ($H^i(M^\bullet)$) and homology. A complex that is exact at every spot is called an *exact* sequence.

By a morphism of sequences $M_\bullet \to M'_\bullet$ we mean a family of R-linear maps $\phi_n : M_n \to M'_n$ such that for every $n \in \mathbb{Z}$ the diagram

$$\begin{array}{ccc} M_n & \xrightarrow{d_n} & M_{n-1} \\ {\scriptstyle \phi_n}\downarrow & & \downarrow{\scriptstyle \phi_{n-1}} \\ M'_n & \xrightarrow[d'_n]{} & M'_{n-1} \end{array}$$

commutes. There is an obvious notion of composition of morphisms of sequences: if $\phi : M_\bullet \to M'_\bullet$ and $\psi : M'_\bullet \to M''_\bullet$, let $\psi \circ \phi : M_\bullet \to M''_\bullet$ be such that $(\psi \circ \phi)_n = \psi_n \circ \phi_n$. Then sequences of R-modules and morphisms is a category (the identity map from $M_\bullet \to M_\bullet$ is, in degree n, the identity map $M_n \to M_n$).

Given a category $\mathcal{C}$, we say that $\mathcal{D}$ is a *full subcategory* of $\mathcal{C}$ if $\mathrm{Ob}\,(\mathcal{D}) \subseteq \mathrm{Ob}\,(\mathcal{C})$ and for all objects X and Y of $\mathcal{D}$, $\mathrm{Mor}_{\mathcal{D}}(X, Y) = \mathrm{Mor}_{\mathcal{C}}(X, Y)$. Composition in $\mathcal{D}$ is the same as composition in $\mathcal{C}$, when it is defined. Note that for every subclass of $\mathrm{Ob}\,(\mathcal{C})$ there is a unique full subcategory of $\mathcal{C}$ with these as its objects. For example, finite sets and functions is a full subcategory of sets and functions, abelian groups and group homomorphisms is a full subcategory of groups and group homomorphisms, and Hausdorff topological spaces and continuous maps is a full subcategory of topological spaces and maps.

The category of complexes of R-modules is defined as the full subcategory of the category of sequences of R-modules whose objects are the complexes of R-modules. We define a *left* complex $M_\bullet$ as a complex such that $M_n = 0$ for all $n < 0$, and a *right complex* as a complex such that $M_n = 0$ for all $n > 0$. Thus, a left complex has the form

$$\cdots \to M_n \to M_{n-1} \to \cdots \to M_1 \to M_0 \to 0 \to 0 \to \cdots$$

and a right complex has the form

$$\cdots \to 0 \to 0 \to M_0 \to M_{-1} \to \cdots \to M_{-(n-1)} \to M_{-n} \to \cdots$$

which we may also write, given our conventions, as

$$\cdots \to 0 \to 0 \to M^0 \to M^1 \to \cdots \to M^{n-1} \to M^n \to \cdots$$

Left complexes and right complexes are also full subcategories of sequences (and of complexes).

A complex is called *projective* (respectively, *free*) if all of the modules occurring are projective (respectively, free).

By a *short exact sequence* we mean an exact sequence of modules $M_\bullet$ such that $M_n = 0$ except possibly when $n \in \{0, 1, 2\}$:

$$0 \to M_2 \to M_1 \to M_0 \to 0.$$

These also forms a full subcategory of complexes. The numbering is not very important here. We shall also refer to M_2 as the *leftmost* module, M_1 as the *middle* module, and M_0 as the *rightmost* module in such a sequence.

The homology modules of a complex may be regarded as a complex by taking all the maps to be 0. The homology operator is then in fact a covariant functor from complexes to complexes: given a map $\{\phi_n\}_n$ of complexes $M_\bullet \to M'_\bullet$, with maps $\{d_n\}_n$ and $\{d'_n\}_n$ respectively, note that if $d_n(u) = 0$, then

$$d'_n\big(\phi_n(u)\big) = \phi_{n-1}\big(d_n(u)\big) = \phi_{n-1}(0) = 0,$$

so that ϕ maps $\mathrm{Ker}\,(d_n)$ into $\mathrm{Ker}\,(d'_n)$. If $u = d_{n+1}(v)$, then

$$\phi_n(u) = \phi_n\big(d_{n+1}(v)\big) = d'_{n+1}\big(\phi_{n+1}(v)\big),$$

which shows that ϕ_n maps $\mathrm{Im}\,(d_{n+1})$ into $\mathrm{Im}\,(d'_{n+1})$. This implies that ϕ_n induces a map of homology

$$H_n(M_\bullet) = \mathrm{Ker}\,(d_n)/\mathrm{Im}\,(d_{n+1}) \to \mathrm{Ker}\,(d'_n)/\mathrm{Im}\,(d'_{n+1}) = H_n(M'_\bullet).$$

This is easily checked to be a covariant functor from complexes to complexes.

In this language, we define a *projective resolution* of an R-module M to be a left projective complex $P_\bullet$ such that $H_n(P_\bullet) = 0$ for $n \geq 1$ together with an isomorphism $H_0(P_\bullet) \cong M$. Since $H_0(P_\bullet) \cong P_0/\mathrm{Im}\,(P_1)$, giving an isomorphism $H_0(P_\bullet) \cong M$ is equivalent to giving a surjection $P_0 \twoheadrightarrow M$ whose kernel is $\mathrm{Im}\,(P_1)$. Thus, giving a projective resolution of M in the sense just described is equivalent to giving a complex

$$(*) \qquad \cdots \to P_n \to \cdots \to P_1 \to P_0 \twoheadrightarrow M \to 0$$

that is exact, and such that P_n is projective for $n \geq 0$. In this context it will be convenient to write $P_{-1} = M$, but it must be remembered that P_{-1} need not be projective. The complex $(*)$ will be referred to as an *augmented projective resolution* of M.

We recall that an R-module P is projective if and if, equivalently

(1) When $M \twoheadrightarrow N$ is onto, $\mathrm{Hom}_R(P, M) \to \mathrm{Hom}_R(P, N)$ is onto.

(2) $\mathrm{Hom}_R(P, \_)$ is an exact functor.

(3) P is a direct summand of a free module.

A direct sum of modules (finite or infinite) is projective if and only if all of the summands are. It is easy to verify (1) for free modules: if P is free on the free basis $\{b_\lambda\}_{\lambda\in\Lambda}$ and $M \twoheadrightarrow N$ is onto, given a map $f : P \to N$, we lift to a map $g : P \to M$ as follows: for each free basis element b_λ of P, choose $u_\lambda \in M$ that maps to $f(b_\lambda)$, and let $g(b_\lambda) = u_\lambda$.

We next want to define what it means for two maps of complexes of R-modules to be homotopic. Let $P_\bullet$ and $N_\bullet$ be two complexes. First note that the set of maps of complexes $\mathrm{Mor}\,(P_\bullet,\ N_\bullet)$ is an R-module: we let

$$\{\phi_n\}_n + \{\psi_n\}_n = \{\phi_n + \psi_n\}_n,$$

and

$$r\{\phi_n\}_n = \{r\phi_n\}_n.$$

We define $\{\phi_n\}_n$ to be *null homotopic* or *homotopic* to 0 if there exist maps $h_n : P_n \to N_{n+1}$ (these are *not* assumed to commute with the complex maps) such that for all n,

$$\phi_n = d'_{n+1}h_n + h_{n-1}d_n.$$

The set of null homotopic maps is an R-submodule of the R-module of maps of complexes. Note that the homology functor $H_\bullet$ is R-linear on maps of complexes.

Two maps of complexes are called *homotopic* if their difference is null homotopic.

Lemma. *If two maps of complexes are homotopic, they induce the same map of homology.*

Proof. We have

$$\phi_n - \phi'_n = d'_{n+1}h_n + h_{n-1}d_n$$

for all n. Let $z \in \mathrm{Ker}\,(d_n)$. Then

$$\phi_n(z) - \phi'_n(z) = d'_{n+1}\big(h_n(z)\big) + h_{n-1}\big(d_n(z)\big).$$

The second term is 0, since $d_n(z) = 0$, and the first term is in $\mathrm{Im}\,(d'_{n+1})$. This shows that

$$[\phi_n(z)] - [\phi'_n(z)] = 0,$$

as required. $\square$

The following Theorem is critical in developing the theory of derived functors such as Tor and Ext. In the applications a will typically be 0, but the starting point really does not matter.

Theorem. *Let $P_\bullet$ and $N_\bullet$ be complexes such that $P_n = 0$ for $n < a-1$ and $N_n = 0$ for $n < a-1$. Suppose that $N_\bullet$ is exact, and that P_n is projective for $n \geq a$. Let $M = P_{a-1}$ (which need not be projective) and $N = N_{a-1}$. Let ϕ be a given R-linear map from M to N. Then we can choose $\phi_n : P_n \to N_n$ for all $n \geq a$ such that, with $\phi_{a-1} = \phi$, $\{\phi_n\}_n$ is a map of complexes (of course, $\phi_n = 0$ is forced for $n < a-1$). Briefly, ϕ lifts to a map*

$\{\phi_n\}_n$ of complexes. Moreover, any two different choices $\{\phi_n\}_n$ and $\{\phi'_n\}_n$ for the lifting (but with $\phi_{a-1} = \phi'_{a-1} = \phi$) are homotopic.

Proof of existence. We have a composite map $P_a \to M \to N$ and a surjection $N_a \twoheadrightarrow N$. Therefore, by the universal mapping property of projective modules, we can choose an R-linear map $\phi_a : P_a \to N_a$ such that $\phi \circ d_a = d'_a \circ \phi_a$. We now shorten both complexes: we replace the right end

$$N_{a+1} \to N_a \twoheadrightarrow N \to 0$$

of $N_\bullet$ by

$$N_{a+1} \to N' \to 0,$$

where N' is the image of N_{a+1} in N_a, which is also Ker $(N_a \to N)$. We shorten the complex $P_\bullet$ by replacing the right end

$$P_{a+1} \to P_a \to M \to 0$$

by

$$P_{a+1} \to M' \to 0,$$

where M' is the kernel of $P_a \to M$. The restriction of ϕ_a to M' gives a map ϕ' of M' to N'. We are now in precisely the same situation that we started with, and we construct ϕ_{a+1} in the same manner that we constructed ϕ_a. The existence of all the ϕ_n follows by a straightforward induction. $\square$

Math 615: Lecture of February 1, 2012

Proof of uniqueness up to homotopy. We work with the difference of the two liftings. It therefore suffices to show that a lifting of the 0 map $M \to N$ is null homotopic. Of course, we must define $h_n = 0$ if $n < a - 1$, and we define $h_{a-1} = 0$ as well: the property we need holds because $\phi = 0$. We construct the maps h_n recursively. Suppose that we have constructed h_n for $n < b$ where $b \geq a$ such that

$$\phi_n = d'_{n+1} h_n + h_{n-1} d_n$$

for all $n < b$. It will suffice to construct $h_b : P_b \to N_{b+1}$ such that

$$\phi_b = d'_{b+1} h_b + h_{b-1} d_b.$$

We claim that the image of $\phi_b - h_{b-1} d_b$ is contained in the image of N_{b+1}. By the exactness of $N_\bullet$, it suffices to show that the image of $\phi_b - h_{b-1} d_b$ is contained in the kernel of d'_b, i.e.,

$$d'_b \phi_b - d'_b h_{b-1} d_b = 0.$$

But since

$$\phi_{b-1} = d'_b h_{b-1} + + h_{b-2} d_{b-1},$$

we may substitute

$$d'_b h_{b-1} = \phi_{b-1} - h_{b-2} d_{b-1}$$

to get

$$d'_b \phi_b - (\phi_{b-1} - h_{b-2} d_{b-1}) d_b.$$

since $d_{b-1} d_b = 0$, this is just

$$d'_b \phi_b - \phi_{b-1} d_b = 0$$

since $\{\phi_n\}_n$ is a map of complexes. Since

$$\alpha = \phi_b - h_{b-1} d_b$$

has image in $\mathrm{Im}\,(N_{b+1})$, we may let β be α with its target restricted to $\mathrm{Im}\,(N_{b+1})$. Since P_b is projective and d'_{b+1} maps onto the target of β, we may lift β to a map $h_b : P_b \to N_{b+1}$, so that $d'_{b+1} h_b = \beta$, which implies that

$$d'_{b+1} h_b = \phi_b - h_{b-1} d_b,$$

as required. □

Remark. Consider the case where $a = 0$. We also have maps of complexes once the augmentations $P_{-1} = M$ and $N_{-1} = N$ are dropped, and because $h_{-1} = 0$, we still have homotopic maps of complexes.

The significance of the result just proved is that we can use *any* projective resolution of M to calculate Tor — up to canonical isomorphism.

Theorem. *Let $P_\bullet$ and $Q_\bullet$ be projective resolutions of the R-module M. Choose a lifting of id_M to a map of resolutions $\phi_\bullet : P_\bullet \to Q_\bullet$ and also to a map of resolutions $\psi_\bullet : Q_\bullet \to P_\bullet$. Then $\phi_\bullet \otimes_R \mathrm{id}_N$ and $\psi_\bullet$ induce mutually inverse isomorphisms between $H_\bullet(P_\bullet \otimes_R N)$ $H_\bullet(Q_\bullet \otimes_R N)$ that are independent of the choices of the ϕ and ψ. In this sense, any projective resolution of M may be used to compute all the modules $\mathrm{Tor}_n^R(M, N)$ up to canonical isomorphism.*

Proof. If we took a different choice of $\phi_\bullet$ it would be homotopic to the original. The homotopy is preserved when we apply $\_ \otimes_R N$. Therefore we get maps of homology that are independent of the choice of $\phi_\bullet$. The same remark applies to $\psi_\bullet$. The composition $\psi_\bullet \circ \phi_\bullet$ gives a map of complexes $P_\bullet \to P_\bullet$ that lifts id_M. The identity map of complexes is also such a lifting. This shows that $\psi \circ \phi$ is homotopic to the identity map on $P_\bullet$. This homotopy is preserved when we apply $\_ \otimes_R N$. This shows that the composition of the induced maps of homology is the identity map. The argument is the same when the composition is taken in the other order. □

Notice that $Tor_n^R(M, N) = 0$ if $n < 0$. If

$$\cdots \to P_1 \to P_0 \twoheadrightarrow M \to 0$$

is a projective resolution of M, then

$$\mathrm{Tor}_0^R(M,\, N) = H_0(\cdots \to P_1 \otimes_R N \to P_0 \otimes_R N \to 0) \cong \frac{P_0 \otimes_R N}{\mathrm{Im}\,(P_1 \otimes_R N)} \cong \frac{P_0}{\mathrm{Im}\,(P_1)} \otimes N$$

using the right exactness of tensor. Since

$$\frac{P_0}{\mathrm{Im}\,(P_1)} \cong M,$$

we have that

$$\mathrm{Tor}_0^R(M,\, N) \cong M \otimes N.$$

We now give an alternative point of view about complexes. Let $R[d] = R[\Delta]/\Delta^2$, and give Δ degree -1. The category of sequences is the same as the category of $\mathbb{Z}$-graded $R[\Delta]$-modules and degree preserving maps. The category of complexes is the same as the full subcategory of $\mathbb{Z}$-graded $R[d]$-modules and degree-preserving maps. It is very easy to see that given $M_\bullet \to M'_\bullet$, one has induced maps $\mathrm{Ann}_{M_\bullet} d \to \mathrm{Ann}_{M'_\bullet} d$ and $dM_\bullet \to dM'_\bullet$. Homology is recovered as $\mathrm{Ann}_{M_\bullet} d/dM_\bullet$, This is an $R[d]$-module on which d acts trivially, and it is now quite obvious that there are induced maps $H_\bullet(M_\bullet) \to H_\bullet(M'_\bullet)$ of homology.

From this point of view, the map h that gives a null homotopy is a degree 1 map of graded R-modules, that is, it increases degrees of homogeneous elements by 1: it need not commute with d. Then $hd + dh$ preserves degree, and does commute with d:

$$d(hd + dh) = dhd = (hd + dh)d.$$

$hd+dh$ gives the zero map on homology because if $dz = 0$, $(hd+dh)(z) = d(h(z)) \in \mathrm{Im}\,(d)$.

We next want to show that Tor is a covariant functor of two variables. Given an R-module map $M \to M'$ it lifts to a map of projective resolutions $P_\bullet$ for M and $P'_\bullet$ for M'. This gives induced maps of homology when we apply $\_ \otimes N$. If we choose a different lifting we get homotopic maps of complexes and the homotopy is preserved when we apply $\_ \otimes_R N$. The check of functoriality in M is straightforward.

Given a map $N \to N'$, we get obvious induced maps $P_\bullet \otimes N \to P_\bullet \otimes N'$ that yield the maps of Tor. Once again, the proof of functoriality is straightforward.

Math 615: Lecture of February 3, 2012

In order to develop the theory of Tor further, we want to consider double complexes. One point of view is that a double complex consists of a family of R-modules $\{M_{ij}\}_{i,j\in\mathbb{Z}}$ together with "horizontal" R-module maps $d_{ij} : M_{ij} \to M_{i,j-1}$ and "vertical" R-module maps $d'_{ij} : M_{ij} \to M_{i-1,j}$ for all $i, j \in \mathbb{Z}$, such that every $d_{ij}d_{i,j+1} = 0$ (the rows are

complexes), every $d'_{i,j}d'_{i+1,j} = 0$ (the columns are complexes) and such that all of the squares

$$\begin{array}{ccc} M_{ij} & \xrightarrow{d_{i,j}} & M_{i,j-1} \\ {\scriptstyle d'_{ij}}\downarrow & & \downarrow{\scriptstyle d'_{i,j-1}} \\ M_{i-1,j} & \xrightarrow[d_{i-1,j}]{} & M_{i-1,j-1} \end{array}$$

commute: omitting subscripts, this means that $d'd = dd'$. An alternative convention that is sometimes made instead is that in a double complex, the vertical and horizontal differentials anticommute: i.e., $d'd = -dd'$. Both conventions have advantages and disadvantages: we shall call the latter type of double complex a *signed double complex*, but this terminology is not standard.

Given a double complex in our sense, one can alway create a signed double complex by altering the signs on some of the maps. To have a standard way of doing this, our convention will be that the associated signed double complex is obtained by replacing d'_{ij} by $(-1)^i d'_{ij}$, while not changing any of the d_{ij}. There are many ways to alter signs to get the squares to anticommute. It does not matter which one is used in the sense that the homology of the total complex (we shall define the total complex momentarily) is unaffected.

An alternative point of view is obtained by working with $\bigoplus_{ij} M_{ij}$, a $(\mathbb{Z} \times \mathbb{Z})$-graded R-module. Let Δ and Δ' be indeterminates over R, and let $R[d, d'] = R[\Delta, \Delta']/(\Delta^2, \Delta'^2)$, where Δ has degree $(0, -1)$, Δ' has degree $(-1, 0)$, and d, d' are their images. The d_{ij} define an action of d on $\bigoplus_{ij} M_{ij}$ that lowers the second index by 1, and the d'_{ij} define an action of d' on $\bigoplus_{ij} M_{ij}$ that lowers the first index by 1. Thus, a double complex is simply a $(\mathbb{Z} \times \mathbb{Z})$-graded $R[d, d']$-module.

A signed double complex may be thought of as a $(\mathbb{Z} \times \mathbb{Z})$-graded module over the noncommutative ring Λ generated over R by elements d and d' of degrees $(0, -1)$ and $(-1, 0)$, respectively, satisfying $d^2 = d'^2 = 0$ and $dd' = -d'd$. Λ may be identified with the exterior algebra over R of the free R-module $Rd \oplus Rd'$.

A *morphism* of double complexes is a bidegree-preserving $\mathbb{Z} \times \mathbb{Z}$-graded $R[d, d']$-module homomorphism, so that the maps commute with the actions of d and of d'. We indicate a double complex, whether signed or not, with the notation $M_{\bullet\bullet}$: the subscript is a reminder that the bidegree has two integer components. The *total complex* of a signed double complex $M_{\bullet\bullet}$, denoted $\mathcal{T}_\bullet(M_{\bullet\bullet})$, is obtained by letting $\mathcal{T}_n(M_{\bullet\bullet}) = \bigoplus_{i+j=n} M_{ij}$, with differential $d+d'$. This is indeed a complex because $(d+d')(d+d') = d^2+d'd+dd'+d'^2 = 0$. The *total complex* of a double complex $M_{\bullet\bullet}$ is simply the total complex of the associated signed double complex. This means that the differential, restricted to M_{ij}, is $d_{ij}+(-1)^i d'_{ij}$.

Example. If $M_\bullet$ and $N_\bullet$ are complexes with differentials $d_\bullet$ and $d'_\bullet$, respectively, we get a double complex $M_\bullet \otimes N_\bullet$ whose i, j term is $M_j \otimes N_i$. Thus, the ith row is

$$\cdots \to M_{j+1} \otimes_R N_i \to M_j \otimes_R N_i \otimes_R M_{j-1} \otimes_R N_i \to \cdots$$

and the j th column is

$$\begin{array}{c} \vdots \\ \downarrow \\ M_j \otimes_R N_{i+1} \\ \downarrow \\ M_j \otimes_R N_i \\ \downarrow \\ M_j \otimes_R N_{i-1} \\ \downarrow \\ \vdots \end{array}$$

The differentials in the i th row are the maps $d_j \otimes \mathrm{id}_{N_i}$ while those in the j th column are the maps $\mathrm{id}_{M_j} \otimes d'_i$. We shall return to the study of double complexes of this form shortly. The total complex $\mathcal{T}_\bullet(M_\bullet \otimes_R N_\bullet)$ is called the *total tensor product* of $M_\bullet$ and $N_\bullet$, and some authors omit the word "total," but we reserve the term "tensor product" for the double complex. Note that the differential of the total tensor product applied to $u_j \times v_i$ has the value $du_j \otimes v_i + (-1)^j u_j \otimes d'v_i$.

Given a double complex, one can take homology first of the rows (giving a new double complex) and then of the columns. The result is called *iterated* homology. One can also take homology first of the columns and then of the rows: this gives the iterated homology for the other order. Third, one can take homology of the total complex. These three objects are related in a complicated way. One of the most important applications of the theory of spectral sequences is to explain the relationship. We shall return to these ideas later.

For the moment, we want to prove two lemmas about double complexes that are of immense importance. They are both special cases of the theory of spectral sequences, but we ignore this for the moment.

The first is the *snake* or *serpent* lemma. One starts with a short exact sequence of complexes

$$0 \to A_\bullet \xrightarrow{\alpha} B_\bullet \xrightarrow{\beta} C_\bullet \to 0,$$

which simply means that for all n, the sequence $0 \to A_n \to B_n \to C_n \to 0$ is exact. We may form from these a double complex in which $A_\bullet$, $B_\bullet$ and $C_\bullet$ are the columns. A typical row is then $0 \to A_n \to B_n \to C_n \to 0$, and so is exact. A key point is that in this situation there is a well-defined map $\gamma_\bullet$ from $H_\bullet(C_\bullet) \to H_{\bullet-1}(A_\bullet)$ called *the connecting homomorphism*, where the subscript $_{\bullet-1}$ indicates that degrees have been shifted by -1, so that the $\gamma_n : H_n(A_\bullet) \to H_{n-1}(C_\bullet)$. We could also have used our graded module conventions and written $H_\bullet(C_\bullet)(-1)$, but we shall use the other convention for shifting the numbering of complexes.

The definition of γ is quite simple: since every map $B_n \to A_n$ is onto, given a cycle $z \in A_n$ we may choose $b \in B_n$ such that $\beta(b) = z$. Since z maps to 0 in A_{n-1}, we have that $\beta(db) = d\big(\beta(b)\big) = dz = 0$ maps to 0 in B_{n-1}, and so db is the image of a unique element

$a \in A_{n-1}$. Moreover $da = 0$, since $d\big(\alpha(a)\big) = d(db) = 0$. Our map will send $[z] \in H_n(C_\bullet)$ to $[a] \in H_{n-1}(A_\bullet)$. Note that if had made another choice of b mapping to z, it would have the form $b + \alpha(a_1)$ for some $a_1 \in A_n$. Then $d(b + \alpha(a_1)) = db + \alpha(da_1)$, and a would change to $a + d(a_1)$, which does not change its homology class. If we change the choice of representative z to $z + dc'$ for some $c' \in C_{n+1}$, we can choose $b' \in B_{n+1}$ that maps to c', and then a new choice for b is $b + db'$. But $d(b + db') = db$. This shows that we have a well-defined map $H_n(C) \to H_{n-1}(A)$. R-linearity follows from the fact that if b_1 and b_2 map to z_1 and z_2, then $rb_1 + b_2$ maps to $rz_1 + z_2$ for $r \in R$. Very briefly, the connecting homomorphism is characterized by the formula $\gamma([\beta(b)] = [\alpha^{-1}(db)]$, which makes sense since α is injective and db is in its image when $\beta(b)$ is a cycle.

Note the following picture:

$$\begin{array}{ccccc} & & b & \mapsto & z \\ & & \downarrow & & \\ a & \mapsto & db & & \\ \downarrow & & & & \\ 0 & & & & \end{array}$$

Proposition (snake or serpent lemma). *If $0 \to A_\bullet \to B_\bullet \to C_\bullet \to 0$ is a short exact sequence of complexes, then there is a long exact sequence of homology:*

$$\cdots \to H_{n+1}(C_\bullet) \xrightarrow{\gamma_{n+1}} H_n(A_\bullet) \xrightarrow{\alpha_{n*}} H_n(B_\bullet) \xrightarrow{\beta_{n*}} H_n(C_\bullet) \xrightarrow{\gamma_n} H_{n-1}(A_\bullet) \to \cdots$$

where α_{n*} and β_{n*} are the maps of homology induced by α_n and β_n, respectively.

Moreover, given a morphism of short exact sequences of complexes (this makes sense, thinking of them as double complexes), we get an induced morphism of long exact sequences, and the construction is functorial.

Proof. It suffices to check exactness at $H_n(C_\bullet)$, $H_n(B_\bullet)$, and $H_n(A_\bullet)$.

A cycle z in C_n is killed by γ iff for b mapping to c, db is the image of $a \in A_{n-1}$ that is a boundary, i.e., that has the form da' for some $a' \in A_{n-1}$. But then $b - a'$ is a cycle in B_n that maps to z, which shows that $[b - a']$ maps to $[z]$, as required. Conversely, if b is a cycle that maps to z, $db = 0$ and it is immediate that $[z]$ is in the kernel of γ_n.

For a cycle in $z \in B_n$, $[z]$ is killed by β_{n*} iff $\beta(z)$ is a boundary in C_n, i.e., $\beta(z) = dc'$, where $c' \in C_{n+1}$. Choose $b' \in B_{n+1}$ that maps onto c'. Then $z - db'$ maps to 0 in C_n, and so is the image of an element $a \in A_n$: moreover, da maps to $dz - d^2b' = 0 - 0$, and $A_{n-1} \hookrightarrow B_{n-1}$, so that a is cycle and $[a]$ maps to $[z]$. Conversely, the fact that the composite $H_n(A_\bullet) \to H_n(B_\bullet) \to H_n(C_\bullet)$ is 0 is immediate from the fact that $\beta\alpha = 0$.

Finally, let $z \in A_n$ be a cycle such that $[z]$ is zero in $H_n(B_\bullet)$. Then $\alpha(z)$ is a boundary, i.e., $\alpha(z) = db$ for $b \in B_{n+1}$. By the definition of γ_{n+1} we have that $\gamma_{n+1}([\beta(b)]) = [a]$. Conversely, if $\gamma_{n+1}([\beta(b)]) = [a]$ we have that $[a]$ maps to $[db] = 0$, so that $\alpha_{n*}\gamma_{n+1} = 0$.

Suppose that one has a morphism of short exact sequences from

$$0 \to A_\bullet \to B_\bullet \to C_\bullet \to 0$$

to

$$0 \to A'_\bullet \to B'_\bullet \to C'_\bullet \to 0.$$

The functoriality of the long exact sequence is immediate from the functoriality of taking homology, except for the commutativity of the squares:

$$\begin{array}{ccc} H_n(C_\bullet) & \longrightarrow & H_{n-1}(A_\bullet) \\ \downarrow & & \downarrow \\ H_n(C'_\bullet) & \longrightarrow & H_{n-1}(A'_\bullet) \end{array} .$$

This follows from the fact that if $\alpha(a) = db$ and $\beta(b) = z$, these relations continue to hold when we map $a \in A_{n-1}$, $b \in B_n$ and $z \in C_n$ to their counterparts in A'_{n-1}, B'_n, and C'_n. $\square$

Corollary. *If $0 \to N_2 \to N_1 \to N_0 \to 0$ is a short exact sequence of R-modules and M is any R-module, then there is a long exact sequence*

$$\cdots \to \mathrm{Tor}_n^R(M,\, N_2) \to \mathrm{Tor}_n^R(M,\, N_1) \to \mathrm{Tor}_n^R(M,\, N_0) \to \mathrm{Tor}_{n-1}^R(M,\, N_2) \to \cdots \to$$
$$\mathrm{Tor}_1^R(M,\, N_2) \to \mathrm{Tor}_1^R(M,\, N_1) \to \mathrm{Tor}_1^R(M,\, N_0) \to M \otimes_R N_2 \to M \otimes_R N_1 \to M \otimes_R N_0 \to 0,$$

where we are identifying $\mathrm{Tor}_0^R(M,\, N)$ with $M \otimes_R N$.

Moreover, the long exact sequence is functorial in the the short exact sequence

$$0 \to N_2 \to N_1 \to N_0 \to 0.$$

Proof. Let $P_\bullet$ be a projective resolution of M (so that $H_0(P_\bullet) = M$), and let $N_\bullet$ be the short exact sequence formed by the N_i. Then $N_\bullet \otimes_R P_\bullet$ is a double complex that may be thought of as the short exact sequence of complexes

$$0 \to N_2 \otimes_R P_\bullet \to N_1 \otimes_R P_\bullet \to N_0 \otimes_R P_\bullet \to 0.$$

The typical row

$$0 \to N_2 \otimes_R P_n \to N_1 \otimes_R P_n \to N_0 \otimes_R P_n \to\to 0$$

is exact because P_n is projective and, therefore, R-flat. The result is now immediate from the definition of Tor and the snake lemma. $\square$

Note that if P is projective, $\mathrm{Tor}_n^R(P, N) = 0$ for $n \geq 1$. This is obvious because with $P_0 = P$, the complex

$$0 \to P_0 \to 0$$

is a projective resolution of P, and may be used to compute Tor. We shall shortly see that this property, the functorial long exact sequence, and the fact that $\mathrm{Tor}_0^R(M,\, N) \cong M \otimes_R N$ canonically as functors of two variables completely characterizes the functor $\mathrm{Tor}_\bullet^R(\_,\, \_)$, up to isomorphism of functors of two variables.

One may ask if there is a comparable long exact sequence for Tor if one starts with a sequence of modules $0 \to M_2 \to M_1 \to M_0 \to 0$. There is such a sequence, and there are several ways to see this. One of them is to prove that there is a canonical isomorphism of functors of two variables $\mathrm{Tor}_n^R(M,\, N) \cong \mathrm{Tor}_n^R(N,\, M)$ for all n, induced by the canonical identification $M \otimes_R N \cong N \otimes_R M$ that lets $u \otimes v$ correspond to $v \otimes u$. But the commutativity of tensor products is not the whole story. The symmetry of Tor is asserting that one can compute $\mathrm{Tor}_n^R(M, N)$ by taking a projective resolution of N, tensoring with M, and then taking homology. It is not obvious how to compare the two. What we shall do is take projective resolutions $P_\bullet$ of M and $Q_\bullet$ of N, and compare the two ways of computing Tor with the homology of $\mathcal{T}_\bullet(P_\bullet \otimes_R Q_\bullet)$. The following fact about double complexes is the key — before stating it, we recall that a left complex is *acyclic* if its homology vanishes in all degrees except degree 0. (The same term is applied to right complexes whose homology vanishes except in degree 0.)

Theorem. *Let $M_{\bullet\bullet}$ be a double complex whose terms all vanish if either component of the bidegree is < 0. Suppose that every row and every column is acyclic, i.e., that the homology of every row is 0 except in degree 0, and the same holds for columns. Let A_i be the augmentation module of the i th row (its 0 th homology module) and B_j be the augmentation module of the j th column (its 0 th homology module). Note that vertical differentials give a map from the i th row to the $i-1$ st row and hence induce maps $A_i \to A_{i-1}$ for all i which makes $A_\bullet$ a complex. Similar, $B_\bullet$ is a complex. Then there are isomorphisms*

$$H_\bullet(A_\bullet) \cong H_\bullet\big(\mathcal{T}_\bullet(M_{\bullet\bullet})\big) \cong H_\bullet(B_\bullet).$$

Math 615: Lecture of February 6, 2012

Proof of the Theorem. Every element of $H_n(\mathcal{T}_\bullet(M_{\bullet\bullet})$ is represented by a cycle of

$$M_{0n} \oplus M_{1,n-1} \oplus \cdots \oplus M_{n-1,0} + \oplus M_{n,0}.$$

Denote this cycle

$$z = u_{0n} \oplus u_{1,n-1} \oplus \cdots \oplus u_{n-1,1} + \oplus u_{n,0}.$$

We work in the signed double complex associated with $M_{\bullet\bullet}$, and assume that horizontal differentials d and the vertical differentials d' anticommute. We shall also write d (respectively, d') for the maps $M_{n,0} \to A_n$ (respectively, $M_{0,n} \to B_n$). A typical term in the sum above has the form u_{ij} where $i + j = n$, and both i and j lie between 0 and n inclusive. The condition that z be a cycle is that for $1 \leq i \leq n$, $du_{i-1,j+1} = -d'u_{ij}$: this

is a condition on the pairs of consecutive terms whose indices sum to n. Given such an element of $\mathcal{T}_n(M_{\bullet\bullet})$, we map it to $H_n(A_\bullet)$ by sending it to $[du_{n0}]$, where $du_{n0} \in A_n$ and the brackets indicate the class of du_{n0} in $H_n(A_\bullet)$. There is a precisely similar map that sends $[z]$ to $[d'(u_{0n})] \in H_n(B_\bullet)$. There are several things that need checking:

(1) du_{n0} is a cycle of $H_n(A_\bullet)$ (the symmetric fact for $[u_{0n}]$ then follows).
(2) $[du_{n0}]$ is independent of the choice of representative of $[z]$ (the symmetric fact for $[d'u_{0n}]$ follows).
(3) The maps $H_n\big(\mathcal{T}_\bullet(M_{\bullet\bullet})\big)$ to $H_n(A_\bullet)$ and to $H_n(B_\bullet)$ obtained in this way are surjective.
(4) These maps are also injective.
(5) These maps are R-linear.

The checks that have some interest are (3) and (4), but we look at them all.

Consider the following diagram, in which the rows are exact, the rightmost squares commute (i.e., d'_* is induced by d'), while other squares, only one of which is shown, anticommute:

$$\begin{array}{ccccccc}
 & & M_{n+1,0} & \xrightarrow{d} & A_{n+1} & \longrightarrow & 0 \\
 & & \downarrow{\scriptstyle d'} & & \downarrow{\scriptstyle d'_*} & & \\
M_{n,1} & \xrightarrow{d} & M_{n,0} & \xrightarrow{d} & A_n & \longrightarrow & 0 \\
\downarrow{\scriptstyle d'} & & \downarrow{\scriptstyle d'} & & \downarrow{\scriptstyle d'_*} & & \\
M_{n-1,1} & \xrightarrow{d} & M_{n-1,0} & \xrightarrow{d} & A_{n-1} & \longrightarrow & 0
\end{array}$$

(1) We have that $d'_*[du_{n0}] = [dd'u_{n,0}] \in A_{n-1}$, and $d'u_{n,0} = -du_{n-1,1}$, and therefore $d'_*[du_{n0}] = [-d^2u_{n-1,1}] = [0] = 0$.

(2) If we change z by adding a boundary in the total complex, $u_{n,0}$ changes by adding a term of the form $du_{n,1} + d'u_{n+1,0}$, where $u_{n,1} \in M_{n,1}$ and $u_{n+1,1} \in M_{n+1,1}$. But $du_{n,1}$ maps to 0 in A_n because $d^2 = 0$, and $d'u_{n+1,0}$ maps to $dd'u_{n+1,0} = d'_*du_{n+1,0}$, the image of $du_{n+1,0} \in A_{n+1}$ in A_n, so that $[du_{n,0}]$ does not change.

(3) Suppose that $\zeta \in A_n$ is a cycle. We can write ζ in the form $du_{n,0}$ for some $u_{n,0} \in M_{n,0}$. We want to show that we can construct elements $u_{n-j,j}$, $1 \le j \le n$, such that

$$u_{0n} \oplus u_{1,n-1} \oplus \cdots \oplus u_{n-1,1} + \oplus u_{n,0}$$

is a cycle in $\mathcal{T}_n(M_{\bullet\bullet})$, i.e., such that we have

$$(*_j) \quad du_{n-(j+1),j+1} = -d'u_{n-j,j}$$

$0 \le j \le n-1$, and we proceed to make the construction by induction on j. Because $du_{n,0} = \zeta$ is a cycle, $d'_*du_{n,0} = 0$, which implies $dd'u_{n,0} = 0$. Since $-d'u_{n,0}$ is in the kernel of d, it is in the image of d, and so we can choose $u_{n-1,1} \in M_{n-1,1}$ such that $du_{n-1,1} = -d'u_{n,0}$. This is $(*_0)$. Now suppose that the $u_{n-h,h}$ have been constructed such that $(*_{h-1})$ holds, $1 \le h \le j$, where $j \ge 1$. In particular, we have $(*_{j-1})$, i.e.,

$$du_{n-j,j} = -d'u_{n-j+1,j-1}.$$

We want to choose $u_{n-j+1,j+1}$ such that

$$du_{n-(j+1),j+1} = -d'u_{n-j,j}$$

so that it suffices to see that $-d'u_{n-j,j}$ is in the image of d, and, therefore, it suffices to see that it is in the kernel of d. but

$$-dd'u_{n-j,j} = d'du_{n-j,j} = d'(-d'u_{n-j+1,j-1}) = 0,$$

as required, since $(d')^2 = 0$. This shows that one can construct a cycle that maps to ζ. If we let $w_{n-j-1,j} = d'u_{n-j,j}$, we have this picture:

$$\begin{array}{ccccccc}
 & & & & u_{n,0} & \mapsto & z \\
 & & & & \downarrow & & \\
 & & & u_{n-1,1} & \mapsto & \pm w_{n-1,0} & \\
 & & & \downarrow & & & \\
 & & & \pm w_{n-2,1} & & & \\
 & \iddots & & \iddots & & \iddots & \\
 & & u_{n-j,j} & \mapsto & \pm w_{n-j,j-1} & & \\
 & & \downarrow & & & & \\
 & u_{n-j-1,j+1} & \mapsto & \pm w_{n-j-1,j} & & & \\
 & \downarrow & & & & & \\
\pm w_{n-j-2,j+1} & & & & & &
\end{array}$$

(4) Now suppose that we have a cycle in $\mathcal{T}_n(M_{\bullet\bullet})$, call it

$$z = u_{0n} \oplus u_{1,n-1} \oplus \cdots \oplus u_{n-1,1} + \oplus u_{n,0}$$

that maps to 0 in $H_n(A_\bullet)$, which means that $du_{n,0} \in A_n$ is the image of some $a_{n+1} = du_{n+1,0} \in A_{n+1}$ under the map induced by d'. This implies that $d(u_{n,0} - d'u_{n+1,0}) = du_{n,0} - d'_* du_{n+1,0} = 0$ in A_n, and therefore has the form $du_{n,1}$ for some $u_{n,1} \in M_{n,1}$. We now use recursion on j to construct

$$u_{n-1,2} \in M_{n-1,2},\ \ldots,\ u_{n-j,j+1} \in M_{n-j,j+1},\ \ldots,\ u_{0,n+1} \in M_{0,n+1}$$

such that for all j, $0 \leq j \leq n$,

$$(*_j) \quad du_{n-j,j+1} + d'u_{n-j+1,j} = u_{n-j,j}.$$

This will show that z is the image of

$$u_{0,n+1} \oplus u_{1,n} \oplus \cdots \oplus u_{n,1} \oplus u_{n+1,0},$$

as required. We have already done the case where $j = 0$. Suppose for a fixed j with $1 \leq j \leq n$ we have constructed these elements $u_{n+1-h,\,h}$, $0 \leq h \leq j$, such that $(*_h)$ holds for $0 \leq h \leq j-1$. In particular, for $h = j-1$, we have

$$(*_{j-1}) \quad du_{n-j+1,j} + d'u_{n-(j-1)+1,j-1} = u_{n-j+1,j-1},$$

and applying d' to both sides we get:

$$(**) \quad d'du_{n+1-j,j} = d'u_{n+1-j,j-1}$$

We want to construct $u_{n-j,j+1}$ such that $(*_j)$ holds, i.e., such that

$$du_{n-j,j+1} = u_{n-j,j} - d'u_{n+1-j,j}.$$

To show that the element on the right is in the image of d, it suffices to prove that it is in the kernel of d, i.e., that

$$du_{n-j,j} = dd'u_{n+1-j,j}.$$

But $du_{n-j,j} = -d'u_{n-j+1,j-1}$ because z is a cycle and by $(**)$,

$$-d'u_{n+1-j,j-1} = -d'du_{n+1-j,j} = dd'u_{n+1-j,j},$$

as required.

(5) R-linearity is immediate from the definitions of the maps, once we know that they are well-defined, since, at the cycle level, the map $H_n\big(\mathcal{T}_\bullet(M_{\bullet\bullet})\big) \to H_n(A_\bullet)$ is induced by restricting the product projection $\displaystyle\prod_{i+j=n} M_{ij} \to M_{n0}$ (identifying $\displaystyle\bigoplus_{i+j=n} M_{ij} \cong \prod_{i+j=n} M_{ij}$). $\square$

We immediately obtain the isomorphism $\operatorname{Tor}_n^R(M,\,N) \cong \operatorname{Tor}_n^R(N,\,M)$ for all n. Let $P_\bullet$ and $Q_\bullet$ be projective resolutions of M and N, respectively. Then $\operatorname{Tor}_n^R(M,\,N) \cong H_n(P_\bullet \otimes_R N) \cong H_n\big(\mathcal{T}_\bullet(P_\bullet \otimes_R Q_\bullet)\big) \cong H_n(M \otimes_R Q_\bullet) \cong H_n(Q_\bullet \otimes_R M) \cong \operatorname{Tor}_n^R(N, M)$. The first and last isomorphisms follow from the definition of Tor, coupled with the fact that any projective resolution may be used to compute it, the second and third isomorphisms follow from the Theorem just proved, and the next to last isomorphism is a consequence of the commutativity of tensor product.

This means that given a short exact sequence of modules $0 \to M_2 \xrightarrow{a} M_1 \xrightarrow{b} M_0 \to 0$ there is also a long exact sequence for Tor:

$$\cdots \to \operatorname{Tor}_n^R(M_2,\,N) \to \operatorname{Tor}_n^R(M_1,\,N) \to \operatorname{Tor}_n^R(M_0,\,N) \to \operatorname{Tor}_{n-1}^R(M_2,\,N) \to \cdots.$$

This sequence can be derived directly without proving the commutativity of Tor, by constructing an exact sequence of projective resolutions of the modules M_j instead. The idea

is to fix resolutions of M_2 and M_0, and use them to build a resolution of M_1. Suppose that we are given projective resolutions $P_\bullet^{(j)}$ of M_j, for $j = 2, 0$, and call the differentials $d^{(j)}$, $j = 0, 2$. From these we can construct a projective resolution $P_\bullet^{(1)}$ of M_1 such that for all n, $P_n^{(1)} = P_n^{(2)} \oplus P_n^{(0)}$. To begin, the map $d^{(0)} : P_0^{(0)} \to M_0$ lifts to a map $f_0 : P^{(0)} \to M_1$ by the universal mapping property of projective modules, because $b : M_1 \twoheadrightarrow M_0$ is onto. One gets a surjection $d^{(1)} : P^{(2)} \oplus P^{(0)} \twoheadrightarrow M_1$ using $d^{(1)} = a \circ d^{(2)} \oplus f_0$. If one lets Z_2, Z_1, and Z_0 be the kernels of the $d^{(j)}$) one has a commutative diagram:

$$\begin{array}{ccccccccc}
 & & & & P_1^{(2)} & & P_1^{(0)} & & \\
 & & & & \downarrow & & \downarrow & & \\
0 & \longrightarrow & Z_2 & \longrightarrow & Z_1 & \longrightarrow & Z_0 & \longrightarrow & 0 \\
 & & \downarrow & & \downarrow & & \downarrow & & \\
0 & \longrightarrow & P_0^{(2)} & \longrightarrow & P_0^{(2)} \oplus P_0^{(0)} & \longrightarrow & P_0^{(0)} & \longrightarrow & 0 \\
 & & \downarrow{\scriptstyle d^{(2)}} & & \downarrow & & \downarrow{\scriptstyle d^{(0)}} & & \\
0 & \longrightarrow & M_2 & \xrightarrow[a]{} & M_1 & \xrightarrow[b]{} & M_0 & \longrightarrow & 0 \\
 & & \downarrow & & \downarrow & & \downarrow & & \\
 & & 0 & & 0 & & 0 & &
\end{array} .$$

where the sequence of kernels $0 \to Z_2 \to Z_1 \to Z_0 \to 0$ is easily checked to be exact, and the problem of constructing the degree 1 part of the resolution of M_1 is now precisely the same problem that we had in constructing the degree 0 part.

Once one has the map $P_1^{(1)} = P_1^{(2)} \oplus P_1^{(0)} \twoheadrightarrow Z_1$, the map

$$P_1^{(1)} = P_1^{(2)} \oplus P_1^{(0)} \to P_0^{(2)} \oplus P_0^{(0)} = P_0^{(1)}$$

is constructed as the composition of the map $P_1^{(2)} \oplus P_1^{(0)} \twoheadrightarrow Z_1$ with the inclusion of Z_1 in $P_0^{(2)} \oplus P_0^{(0)}$. By a straightforward induction, one can continue in this way to build an entire projective resolution $P_\bullet^{(1)}$ of M_1, and a short exact sequence of complexes

$$0 \to P_\bullet^{(2)} \to P_\bullet^{(1)} \to P_\bullet^{(0)} \to 0$$

such that for all n,

$$P_n^{(1)} = P_n^{(2)} \oplus P_n^{(0)},$$

and the induced sequence of maps on the augmentations M_j is the short exact sequence $0 \to M_2 \xrightarrow{a} M_1 \xrightarrow{b} M_0 \to 0$ that we started with.

We next note that if $r \in R$ and M, N are R-modules, then the map

$$\mathrm{Tor}_n^R(M, N) \to \mathrm{Tor}_n^R(M, N)$$

induced by multiplication by r on N is given by multiplication by r on $\mathrm{Tor}_n^R(M,\, N)$. This may be seen as follows. Choose a projective resolution $P_\bullet$ of M. When we tensor with $N \xrightarrow{r} N$, we get the map of complexes $P_\bullet \otimes_R N \xrightarrow{r} P_\bullet \otimes_R N$ induced by multiplication by r, and this induces the map of homology. The same fact holds when we use $M \xrightarrow{r} M$ to induce a map

$$\mathrm{Tor}_n^R(M,\, N) \to \mathrm{Tor}_n^R(M,\, N),$$

by the symmetry of Tor. (Alternatively, use multiplication by r on every P_n to left $M \xrightarrow{r} M$ to a map $P_\bullet \xrightarrow{r} P_\bullet$ of the projective resolution of M to itself. Then apply $\_ \otimes_R N$ and take homology.)

If $r \in \mathrm{Ann}_R N$, then multiplication $N \xrightarrow{r} N$, is the zero map, and hence induces the 0 map

$$\mathrm{Tor}_n^R(M,\, N) \to \mathrm{Tor}_n^R(M,\, N),$$

which is also the map given by multiplication by r. In consequence, we have that $\mathrm{Ann}_R N$ kills every $\mathrm{Tor}_n^R(M,\, N)$. The same holds for $\mathrm{Ann}_R M$, and so $\mathrm{Ann}_R M + \mathrm{Ann}_R N$ kills every $\mathrm{Tor}_n^R(M,\, N)$.

The following fact, while very simple, is of great utility:

Proposition. *If $x \in R$ is not a zerodivisor and M is any R-module, then $\mathrm{Tor}_n^R(M,\, R/xR)$ (which is also $\mathrm{Tor}_n^R(R/xR,\, M)$) is M/xM if $n = 0$, is $Ann_M x$ if $n = 1$, and is 0 if $n \neq 0,\, 1$.*

Proof. We may use the projective resolution $0 \to R \xrightarrow{x} R \to 0$, whose augmentation is R/xR, to compute Tor. Here, the left hand copy of R is in degree 1 and the right hand copy in degree 0. When we apply $M \otimes_R \_$, we find that the values of Tor are given by the homology of the complex $0 \to M \xrightarrow{x} M \to 0$. $\square$

We next want to introduce Koszul complexes. In doing so, we first want to discuss iterated total tensor products of complexes. Given k complexes $M_\bullet^{(1)}, \ldots, M_\bullet^{(k)}$, with differential $d^{(j)}$ on $M^{(j)}$, we may define a total tensor product, which we denote

$$\mathcal{T}_\bullet(M_\bullet^{(1)} \otimes_R \cdots \otimes_R M_\bullet^{(k)}),$$

recursively by the rule that for $k = 1$ it is simply the original complex, for $k = 2$ it is the total tensor product of two complexes already defined, while for $k > 2$ it is

$$\mathcal{T}_\bullet\big((\mathcal{T}_\bullet(M_\bullet^{(1)} \otimes_R \cdots \otimes_R M_\bullet^{(k-1)}) \otimes_R M_\bullet^{(k)}\big).$$

It is easy to work out that up to obvious isomorphism this is the complex $T_\bullet$ such that

$$T_n = \bigoplus_{j_1 + \cdots j_k = n} M_{j_1} \otimes_R \cdots \otimes_R M_{j_k}.$$

The differential on T_n is determined by the formula

$$d(u_{j_1} \otimes \cdots \otimes u_{j_k}) = \sum_{\nu=1}^{k} (-1)^{j_1 + \cdots + j_{\nu-1}} u_{j_1} \otimes \cdots \otimes u_{j_{\nu-1}} \otimes d^{(j_\nu)} u_{j_\nu} \otimes u_{j_{\nu+1}} \otimes \cdots \otimes u_{j_k}.$$

We now define the Koszul complex of a sequence of elements $x_1, \ldots, x_k$ of the ring R, which we denote $\mathcal{K}_\bullet(x_1, \ldots, x_k; R)$, as follows. If $k = 1$, $\mathcal{K}_\bullet(x_1; R)$ is the complex $0 \to R \xrightarrow{x_1} R \to 0$, where the left hand copy of R is in degree 1 and the right hand copy in degree 0. Recursively, for $k > 1$,

$$\mathcal{K}_\bullet(x_1, \ldots, x_k; R) = \mathcal{T}_\bullet\big(\mathcal{K}_\bullet(x_1, \ldots, x_{k-1}; R) \otimes_R \mathcal{K}_\bullet(x_k; R)\big)$$

Said differently,

$$\mathcal{K}_\bullet(x_1, \ldots, x_k; R) = \mathcal{T}_\bullet\big(\mathcal{K}_\bullet(x_1; R) \otimes_R \cdots \otimes_R \mathcal{K}_\bullet(x_k; R)\big).$$

We shall look very hard at these complexes. Very soon, we will prove that if $x_1, \ldots, x_k$ is an improper regular sequence in R, then $\mathcal{K}_\bullet(x_1, \ldots, x_k; R)$ is a free resolution of $R/(x_1, \ldots, x_k)$. This fact can be used, in conjunction with tricks, to compute or gain information about Tor in a remarkable number of instances.

Math 615: Lecture of February 8, 2012

We first prove that Koszul complexes give free resolutions for improper regular sequences such that every element is a nonzerodivisor. The hypothesis that every element is a nonzerodivisor is not needed: we will get rid of it shortly. But the case we prove is the most important.

Theorem. *Let $x_1, \ldots, x_k$ be an improper regular sequence in R such that every x_j is a nonzerodivisor in R. Then the Koszul complex $\mathcal{K}_\bullet(x_1, \ldots, x_k; R)$ is acyclic, and gives a free resolution of $R/(x_1, \ldots, x_k)R$.*

Proof. The case where $k = 1$ is obvious. We proceed by induction on k. Thus, we may assume that $k > 1$, and then we know that $\mathcal{K}_\bullet(x_1, \ldots, x_{k-1}; R)$ and $\mathcal{K}_\bullet(x_k; R)$ give free resolutions of $R/(x_1, \ldots, x_{k-1})R$ and R/x_kR respectively. We may use the homology of the total tensor product to compute the values of

$$\operatorname{Tor}_n^R(R/(x_1, \ldots, x_{k-1})R,\ R/x_kR).$$

This is

$$\mathcal{T}_n\big(\mathcal{K}_\bullet(x_1, \ldots, x_{k-1}; R) \otimes_R \mathcal{K}_\bullet(x_k; R)\big),$$

which *is* $\mathcal{K}_\bullet(x_1, \ldots, x_k; R)$. By the Proposition from the previous lecture, when x is a nonzerodivisor in R, $\operatorname{Tor}_n^R(M, R/xR)$ vanishes when $n \neq 0, 1$, and

$$\operatorname{Tor}_1^R(M,\ R/xR) \cong \operatorname{Ann}_M x.$$

In our current situation, x_k is not a zerodivisor on $R/(x_1, \ldots, x_{k-1})R$ by the definition of a regular sequence, and so all of the

$$\operatorname{Tor}_n^R(R/(x_1, \ldots, x_{k-1})R,\ R/x_kR)$$

vanish except possibly when $n = 0$, where one has

$$R/(x_1, \ldots, x_{k-1})R \otimes_R R/x_kR \cong R/(x_1, \ldots, x_k)R,$$

since $R/I \otimes_R R/J \cong R/(I + J)$ quite generally. This shows that $\mathcal{K}_\bullet(x_1, \ldots, x_k; R)$ is a free resolution of $R/(x_1, \ldots, x_k)R$, as claimed. $\square$

Koszul complexes of this sort are, by no small measure, the best understood free resolutions. We shall look at them closely. Later, we will use our understanding of Koszul complexes to prove the following theorem, which as established by M. Auslander in the equicharacteristic case and by S. Lichtenbaum in general.

Theorem (rigidity of Tor over regular rings). *Let M and N be finitely generated modules over a Noetherian ring R whose local rings are regular. Suppose that $\operatorname{Tor}_i^R(M, N) = 0$. Then $\operatorname{Tor}_j^R(M, N) = 0$ for all $j \geq i$.*

It will be quite a while before we can prove this.

We want to give a more explicit description of the Koszul complex. Experience has shown that it is useful in considering the complexes

$$0 \to R \xrightarrow{x_j} R \to 0$$

to give separate names to the generators of the free modules, instead of calling them all 1. We therefore write

$$0 \to Ru_j \xrightarrow{x_j} Rv_j \to 0$$

for $\mathcal{K}_\bullet(x_j; R)$, although $u_j = v_j = 1$. The differential is described by the rule $du_j = x_jv_j$, although we might also write $du_j = x_j$. To describe the total tensor product of k such complexes, we note that from our general description of total tensor products, $\mathcal{K}_i(x_1, \ldots, x_k; R)$ will consist of the direct sum of all k-fold tensor products consisting of one term chosen from each complex, and such that the sum of the degrees from which these terms come is i. Notice that there will by 2^k terms if we look at all degrees. There will be one term in degree i for every choice of terms such that exactly i of them are the degree one copy of R from the complex. There are $\binom{k}{i}$ such terms; if we choose the degree one factors to be from

$$\mathcal{K}(x_{j_1}; R), \ldots, \mathcal{K}(x_{j_i}; R)$$

with $1 \leq j_1 < \cdots < j_i \leq k$, we write $u_{j_1, \ldots, j_i}$ for the obvious generator: it is a tensor product of k terms, each of which is either u_t or v_t. Specifically, the generator can be described as $w_1 \otimes \cdots w_k$, where if $t = j_i$ for some i then $w_t = u_{j_i}$, while $w_t = v_t$ otherwise. Note that the degree in which $u_{j_1, \ldots, j_i}$ occurs is i, the number of elements in the string of subscripts. With this notation, we can write down the differential explicitly as follows:

$$du_{j_1, \ldots, j_i} = \sum_{t=1}^{i} (-1)^{t-1} x_{j_t} u_{j_1, \ldots, j_{t-1}, j_{t+1}, \ldots, j_i}.$$

The matrices of the maps with respect to the bases we are using will have entries each of which is $\pm x_s$ or 0.

This is simpler than it may seem at first sight. Consider the case where $k = 2$. The Koszul complex looks like this:

$$0 \to Ru_{12} \xrightarrow{\alpha_2} Ru_1 \oplus Ru_2 \xrightarrow{\alpha_1} R \to 0.$$

u_1 maps to x_1 and u_2 maps to x_2, while u_{12} maps to $x_1u_2 - x_2u_1 = -x_2u_1 + x_1u_2$. Thus, then matrices of the maps are $\alpha_1 = \begin{pmatrix} x_1 & x_2 \end{pmatrix}$ and

$$\alpha_2 = \begin{pmatrix} -x_2 \\ x_1 \end{pmatrix}.$$

The map α_1 sends $r_1u_1 + r_2u_2$ to $r_1x_1 + r_2x_2$. Its kernel is the set of relations on x_1 and x_2. The "obvious" relations are given by the multiples of $(-x_2, x_1)$, and when the Koszul complex is acyclic (e.g., when the x_1, x_2 is a regular sequence), the "obvious" relations are the only relations.

When $k = 3$ the Koszul complex is

$$0 \to Ru_{123} \xrightarrow{\alpha_3} Ru_{23} \oplus Ru_{13} \oplus R_{12} \xrightarrow{\alpha_2} Ru_1 \oplus Ru_2 \oplus R_3 \xrightarrow{\alpha_1} R \to 0.$$

The images of u_1, u_2, and u_3 are x_1, x_2, and x_3, respectively. The images of u_{23}, u_{13}, and u_{12} are $-x_3u_2 + x_2u_3$, $-x_3u_1 + x_1u_3$, and $-x_2u_1 + x_1u_2$, respectively. The image of u_{123} is $x_1u_{23} + x_2u_{1,3} + x_3u_{12}$. If we use the obvious bases except that we replace u_{13} by $-u_{13}$, then the matrices of the maps are $\alpha_1 = \begin{pmatrix} x_1 & x_2 & x_3 \end{pmatrix}$,

$$\alpha_2 = \begin{pmatrix} 0 & x_3 & -x_2 \\ -x_3 & 0 & x_1 \\ x_2 & -x_1 & 0 \end{pmatrix},$$

and

$$\alpha_3 = \begin{pmatrix} x_1 \\ -x_2 \\ x_3 \end{pmatrix}.$$

The columns of each α_{i+1} give relations on the columns of α_i, $i = 1, 2$. When the Koszul complex is acyclic, these generate all the relations.

Note that over a Noetherian ring R, whenever M and N are finitely generated, so are all the modules $\operatorname{Tor}_n^R(M, N)$. To see this, note that we can choose a free resolution of M by finitely generated free modules. The resolution may go on forever, but each new kernel (or module of syzygies) is a submodule of a finitely generated free module, hence, Noetherian, and one can map a finitely generated free module onto it. Applying $\_ \otimes_R N$ produces a complex of Noetherian modules, and it follows at once that all of its homology modules are Noetherian.

Things are even better when we take free resolutions of finitely generated modules over a local ring (R, m, K). We start with a free module M. We may choose a minimal set of generators for M: these are elements whose images in $K \otimes_R M \cong M/mM$ are K-vector

space basis. This gives $F_0 \twoheadrightarrow M$ where F_0 is free. The kernel Z_1 is a finitely generated R-module. Again, we may choose a minimal set of generators of Z_1 and map a free module F_1 onto Z_1 using these generators. We can continue in this way, and so obtain a free resolution

$$\cdots \xrightarrow{\alpha_{n+1}} F_n \xrightarrow{\alpha_n} F_{n-1} \xrightarrow{\alpha_{n-1}} \cdots \xrightarrow{\alpha_2} F_1 \xrightarrow{\alpha_1} F_0 \xrightarrow{\alpha_0} M \to 0$$

such that the image of the free basis for F_i is a minimal set of generators for $Z_i = \alpha_i(F_i)$ for all $i \geq 0$. In this notation, $Z_0 = M$ itself. Such a free resolution is called a *minimal* free resolution of M. If $F_i = R^{\oplus b_i}$, the integer b_i is called the ith Betti number of M: we shall see momentarily that it is independent of the choice of the minimal resolution of M.

Note that the columns of the matrix α_i generate the relations on the generators for Z_i given by the image of the the free basis for F_i. These generators will be minimal if and only if none of them is a linear combination of the others, which is equivalent to the condition that no coefficient on a relation among them be a unit. (If any coefficient is a unit, one can solve for that generator in terms of the others.) Therefore, a resolution with matrices α_i is a minimal free resolution if and only if every entry of every matrix is in the maximal ideal m of R.

Theorem. *let (R, m, K) be a local ring, and let M be a finitely generated module. Let $F_\bullet$ be a minimal free resolution of M, and suppose that $F_i \cong R^{b_i}$. Then $\operatorname{Tor}_i(M, K) \cong K^{b_i}$. Thus, the ith Betti number of M is the same as $\dim_K \operatorname{Tor}_i^R(M, K)$.*

M has a finite resolution by free modules if and only if $\operatorname{Tor}_i^R(M, K) = 0$ for some $i \geq 1$, and then a minimal free resolution is finite and is at least as short as any other free resolution of M.

Proof. When we use a minimal resolution $F_\bullet$ to compute Tor, we form the complex of K-vector spaces $F_\bullet \otimes_R K$. At the ith spot we have

$$F_i \otimes_R K \cong R^{\oplus b_i} \otimes_R K \cong K^{\oplus b_i}.$$

Because all the matrices have entries in m, when we map to K all the matrices become 0. Thus, all the maps in $F_\bullet \otimes K$ are 0, and the complex is its own homology, i.e.,

$$H_i(F_\bullet \otimes K) \cong F_i \otimes_R K \cong K^{b_i},$$

as claimed.

If M has a finite free resolution of length h, it may be used to compute Tor. It follows that $\operatorname{Tor}_i^R(M, K) = 0$ for $i > h$. On the other hand, suppose that $\operatorname{Tor}_i^R(M, K) = 0$. This means that in a minimal free resolution of M, $b_i = 0$, i.e., the ith module is 0. But then the minimal free resolution continues with modules all of which are 0. $\square$

Putting this together with our knowledge of the Koszul complex, we obtain the following result with amazing ease:

Theorem. *Let (R, m, K) be a regular local ring of dimension d, and let $x_1, \dots, x_d$ be a minimal set of generators of m. Then $\mathcal{K}_\bullet(x_1, \dots, x_d; R)$ is a minimal free resolution of K over R. In consequence,* $\operatorname{Tor}_i^R(K, K) \cong K^{\binom{d}{i}}$, $0 \le i \le d$, *and is 0 otherwise.*

Moreover, every finitely generated R-module M has a finite free resolution over R of length at most d.

Proof. We know that $x_1, \dots, x_d$ is a regular sequence in R consisting of nonzerodivisors (since R is a domain). Thus, $\mathcal{K}_\bullet(x_1, \dots, x_d; R)$ is a free resolution of $R/(x_1, \dots, x_d) \cong K$. Since every entry of every matrix is either $\pm x_j$ for some j or 0, this is a minimal free resolution of K. The calculation of $\operatorname{Tor}_i^R(K, K)$ is immediate.

Now let M be any finitely generated R-module. Since K has a free resolution of length d, $\operatorname{Tor}_i^R(K, M) = 0$ for $i > d$. But this is the same as $\operatorname{Tor}_i^R(M, K)$, and therefore the minimal resolution of M has length at most d. $\square$

Notice that the symmetry of Tor plays a key role in the proof that M has a finite free resolution: in some sense, the symmetry is a rather trivial fact, but it is often the case that the information it provides is not easily obtained by other methods.

The final statement is a version of the Hilbert syzygy theorem. Hilbert did the case of finitely generated graded modules over the polynomial ring in d variables over the complex numbers. Note that the fact that one has a finite free resolution is equivalent to the assertion that when one takes iterated modules of syzygies, one eventually gets one that is free.

Horrocks raised the following question. Given a module $M \neq 0$ of finite length over a regular local ring (R, m, K) of dimension d, is it true that the ith Betti number of M is at least $\binom{d}{i}$, $0 \le i \le d$? The question was given in a list by Hartshorne. Buchsbaum and Eisenbud conjectured that this is true. The problem, although simple to state, is open.

We shall relate the homology of Koszul complexes to the notion of multiplicity of an m-primary ideal discussed earlier. Recall that if $\mathfrak{A}$ is m-primary in a local ring (R, m, K) of Krull dimension d, then the Hilbert function $\ell(R/\mathfrak{A}^{n+1})$ agrees with a polynomial of degree d in n for large n, whose leading term has the form $\dfrac{e_{\mathfrak{A}}}{d!}n^d$, where $e_{\mathfrak{A}}$ is a positive integer called the *multiplicity of* $\mathfrak{A}$. We shall prove that if $x_1, \dots, x_d$ is a system of parameters of the local ring R and $\mathfrak{A} = (x_1, \dots, x_d)R$, then

$$e_{\mathfrak{A}} = \sum_{i=0}^{d} (-1)^i \ell\big(H_i\big(\mathcal{K}_\bullet(x_1, \dots, x_d; R)\big)\big).$$

It does turn out that the modules $H_i\big(\mathcal{K}_\bullet(x_1, \dots, x_d; R)\big)$ have finite length, so that the right hand side makes sense. We will prove this formula, which is due to Serre, using spectral sequences. It will be a while before we are able to accomplish this.

Open questions in this area are abundant. Here is one that sounds very simple. First recall that the multiplicity e_m of the maximal ideal m of R is also called the *multiplicity* of R. Let

$$(R, m, K) \to (S, n, L)$$

be a local homomorphism of local rings such that S is flat over R. Is the multiplicity of R bounded by the multiplicity of S? I.e., is $e_m \leq e_n$? This was conjectured by C. Lech, and is open even when S is a finitely generated free R-module.

Math 615: Lecture of February 10, 2012

If $x_1, \ldots, x_n \in R$ and M is an R-module, we define the *Koszul complex of M with respect to $x_1, \ldots, x_n$*, denoted $\mathcal{K}_\bullet(x_1, \ldots, x_n; M)$, as

$$\mathcal{K}_\bullet(x_1, \ldots, x_n; R) \otimes_R M.$$

At the ith spot we have $R^{\binom{n}{i}} \otimes_R M$. When $n = 2$ we have

$$0 \to M \xrightarrow{d_2} M \oplus M \xrightarrow{d_1} M \to 0$$

where

$$d_2(u) = -x_2 u \oplus x_1 u$$

and

$$d_1(v \oplus w) = x_1 v + x_2 w.$$

We shall often abbreviate $\underline{x}$ for $x_1, \ldots, x_n$, and write $\mathcal{K}_\bullet(\underline{x}; M)$ instead. The *Koszul homology modules* $H_\bullet(\underline{x}; M)$ are then defined as

$$H_\bullet\big(\mathcal{K}_\bullet(\underline{x}; M)\big).$$

We note the following facts:

(1) A an R-linear map $f : M \to N$ induces, in a covariantly functorial way, a map of Koszul complexes $\mathcal{K}_\bullet(\underline{x}; M) \to \mathcal{K}_\bullet(\underline{x}; N)$ and, hence, a map of Koszul homology $H_\bullet(\underline{x}; M) \to H_\bullet(\underline{x}; N)$. If $M = N$ and the map is multiplication by $r \in R$, the induced map on Koszul complexes and on their homology is also given by multiplication by the ring element r.

(2) By the right exactness of tensor product,

$$H_0(\underline{x}; M) \cong \big(R/(x_1, \ldots, x_n)R\big) \otimes_R M \cong M/(x_1, \ldots, x_n).M$$

The last map

$$\mathcal{K}_n(\underline{x}; M) \cong M \to M^{\oplus n} \cong \mathcal{K}_{n-1}(\underline{x}; M)$$

has the form

$$u \mapsto (\pm x_1 u, \ldots, \pm x_n u)$$

for some choice of signs (which depends on the choices of free basis). However, for any choice, the kernel is clearly $\mathrm{Ann}_M(x_1, \ldots, x_n)R$, i.e.,

$$H_n(\underline{x}; M) \cong \mathrm{Ann}_M(x_1, \ldots, x_n)R.$$

(3) Given a short exact sequence of modules

$$0 \to M_2 \to M_1 \to M_0 \to 0$$

there is a functorial short exact sequence of complexes

$$0 \to \mathcal{K}_\bullet(\underline{x};\, M_2) \to \mathcal{K}_\bullet(\underline{x};\, M_1) \to \mathcal{K}_\bullet(\underline{x};\, M_0) \to 0$$

induced by forming the tensor product of the given short exact sequence with $\mathcal{K}_\bullet(\underline{x}; R)$ (which we think of as a column). The rows are all exact because each is obtained by tensoring

$$0 \to M_2 \to M_1 \to M_0 \to 0$$

with a free R-module. By the snake lemma there is a functorial long exact sequence of Koszul homology:

$$\begin{aligned} 0 \to H_n(\underline{x};\, M_2) \to H_n(\underline{x};\, M_1) \to H_n(\underline{x};\, M_0) \to \cdots \\ \to H_i(\underline{x};\, M_2) \to H_i(\underline{x};\, M_1) \to H_i(\underline{x};\, M_0) \to H_{i-1}(\underline{x};\, M_2) \to \cdots \\ \to H_0(\underline{x};\, M_2) \to H_0(\underline{x};\, M_1) \to H_0(\underline{x};\, M_0) \to 0. \end{aligned}$$

(4) Let $h : R \to S$ be a ring homomorphism and let $x_1, \ldots, x_n \in R$. Let M be an S-module. Then M becomes R-module by restriction of scalars, i.e., we let $r \in R$ act by the rule $r \cdot u = h(r)u$. The Koszul complexes

$$\mathcal{K}_\bullet(x_1, \ldots, x_n;\, M)$$

and

$$\mathcal{K}_\bullet(h(x_1), \ldots, h(x_n); M)$$

are isomorphic in a very strong sense. As R-modules, the terms are identical. The maps are also identical: each map is completely determined by the manner in which the x_i (respectively, the $h(x_i)$) act on M, and multiplication by x_i is, by definition, the same endomorphism of M as multiplication by $h(x_i)$. The only issue is whether one is "remembering" or "forgetting" that M is an S-module as well as an R-module. Thus, there is a sense in which $H_\bullet(x_1, \ldots, x_n;\, M)$ and $H_\bullet(h(x_1), \ldots, h(x_n);\, M)$ are equal, not just isomorphic. Even if one "forgets" for a while that M is an S-module, the S-module structure on $H_\bullet(x_1, \ldots, x_n; M)$ can be recovered. If $s \in S$, multiplication by s gives an R-linear map $M \to M$, and so induces a map $H_\bullet(x_1, \ldots, x_n;\, M) \to H_\bullet(x_1, \ldots, x_n;\, M)$, and this recovers the S-module structure on $H_\bullet(x_1, \ldots, x_n;\, M)$.

5) We want to see that Koszul homology may be regarded as an instance of Tor. Let $x_1, \ldots, x_n \in R$ and M be an R-module. Let A be any ring that maps to R. We may always choose $A = \mathbb{Z}$ or $A = R$. If R happens to contain a field K we may want to choose $A = K$. In any case, think of R as an A-algebra. Let $X_1, \ldots, X_n$ be indeterminates over A, and let $B = A[X_1, \ldots, X_n]$, the polynomial ring in n variables over A. Extend $A \to R$

to a ring homomorphism $B \to R$ by mapping $X_i \mapsto x_i$, $1 \leq i \leq n$. We can do this by virtue of the universal mapping property of polynomial rings. Then multiplication by X_i on M is the same as multiplication by x_i, $1 \leq i \leq n$. In B, $X_1, \ldots, X_n$ is a regular sequence, and every X_i is a nonzerodivisor (this typically is not true at all for the x_i in R). Then $\mathcal{K}_\bullet(X_1, \ldots, X_n; B)$ is a free resolution of $B/(X_1, \ldots, X_n)B \cong A$, but keep in mind that when we view A as a B-module here, all of the X_i act trivially. Then $\operatorname{Tor}_i^B(A, M)$ is the i th homology module of

$$\mathcal{K}_\bullet(X_1, \ldots, X_n; B) \otimes_B M = \mathcal{K}_\bullet(X_1, \ldots, X_n; M) = \mathcal{K}_\bullet(\underline{x}; M),$$

which leads to an identification

$$\operatorname{Tor}_i^B(A, M) \cong H_i(\underline{x}; M).$$

The long exact sequence for Koszul homology is simply an instance of the long exact sequence for Tor if one takes this point of view. The R-module structure of $\operatorname{Tor}_i^B(A, M)$ can be recovered: multiplication by an element $r \in R$ is a B-linear map $M \to M$, and so induces a map

$$\operatorname{Tor}_i^B(A, M) \to \operatorname{Tor}_i^B(A, M)$$

which gives the action of multiplication by r on $\operatorname{Tor}_i^B(A, M)$.

6) It is obvious that $\operatorname{Ann}_R M$ kills all the Koszul homology modules $H_i(\underline{x}; M)$, since it kills M and therefore every module in the complex $\mathcal{K}_\bullet(\underline{x}; M)$. Less obvious is the fact that $(x_1, \ldots, x_n)R$ kills every $H_i(\underline{x}; M)$. We may see this as follows. With notation as in 5), we may view $H_i(\underline{x}; M) \cong \operatorname{Tor}_i^B(A, M)$, and since every X_i kills A, multiplication by X_i kills $\operatorname{Tor}_i^B(A, M)$. This implies that multiplication by X_i on M induces the zero map $\operatorname{Tor}_i^B(A, M) \to \operatorname{Tor}_i^B(A, M)$. But that means that multiplication by x_i acting on M induces the zero map $\operatorname{Tor}_i^B(A, M) \to \operatorname{Tor}_i^B(A, M)$, and this implies that x_i kills $\operatorname{Tor}_i^B(A, M) \cong H_i(\underline{x}; M)$, as required. In particular, if $x_1, \ldots, x_n$ generate the unit ideal, then all of the Koszul homology modules $H_i(\underline{x}; M) = 0$.

We have seen that Koszul homology can be viewed as an instance of Tor. It is worth pointing out that it is often profitable to interpret Tor as some kind of Koszul homology if one can: Koszul homology is typically better understood than other instances of Tor.

Suppose that we have a short exact sequence

$$0 \to M_1 \to P \to M \to 0,$$

i.e., that M_1 is a first module of syzygies of M. Let N be any R-module. The long exact sequence for Tor yields a four term exact sequence

$$0 \to \operatorname{Tor}_1^R(M\, N) \to M_1 \otimes_R N \to P \otimes_R N \to M \otimes_R N \to 0,$$

because $\operatorname{Tor}_i^R(P, N) = 0$ for $i \geq 1$. In particular, $\operatorname{Tor}_1^R(P, N) = 0$. This characterizes $\operatorname{Tor}_1^R(M, N)$ as $\operatorname{Ker}(M_1 \otimes_R N \to P \otimes_R N)$. Because the higher values of $\operatorname{Tor}_i^R(P, N)$ are 0, the long exact sequence also yields isomorphisms

$$\operatorname{Tor}_{i+1}^R(M\, N) \cong \operatorname{Tor}_i(M_1, N)$$

for $i \geq 1$. More generally, if M_j is any jth module of syzygies of M, which means that there is an exact sequence

$$0 \to M_j \to P_{j-1} \to \cdots P_1 \to P_0 \to M \to 0$$

such that the P_t are projective, $0 \leq h \leq j$ (but we also define M to be a zeroth module of syzygies of M), then, by a trivial induction

$$\mathrm{Tor}_{i+j}^R(M,\, N) \cong \mathrm{Tor}_i^R(M_j,\, N)$$

for $i \geq 1$ and $j \geq 0$. In particular,

$$\mathrm{Tor}_{j+1}^R(M,\, N) \cong \mathrm{Tor}_1^R(M_j,\, N).$$

If we also have an exact sequence

$$0 \to M_{j+1} \to P_j \to M_j \to 0,$$

with P_j projective then

$$\mathrm{Tor}_{j+1}^R(M,\, N) \cong \mathrm{Ker}\,(M_{j+1} \otimes_R N \to P_j \otimes_R N).$$

This reduces the calculation of Tor to the calculation of modules of syzygies and the kernels of maps of tensor products. It also proves the assertion made earlier that Tor is completely determined by the three conditions (1) Tor_0^R agrees with $\otimes_R$, (2) higher Tor vanishes if the first given module is projective, and (3) there is a functorial long exact sequence.

Modules of syzygies are not uniquely determined. But they are determined up to taking direct sums with projective modules, as shown by the following result.

Theorem (Schanuel's Lemma). *Let*

$$0 \to M_1 \to P \xrightarrow{\alpha} M \to 0$$

and

$$0 \to M_1' \to P' \xrightarrow{\alpha'} M \to 0$$

be exact sequences, where P and P' are projective. Then

$$M_1 \oplus P' \cong M_1' \oplus P.$$

Proof. We have a surjection $\beta : P \oplus P' \twoheadrightarrow M$ that sends $u \oplus u'$ to $\alpha(u) + \alpha'(u')$. Let N be the kernel. It will suffice to show that $N \cong M_1' \oplus P$. The isomorphism $N \cong M_1 \oplus P'$ then follows by symmetry. Consider the map $\pi : N \to P$ that sends $u \oplus u' \in N$ to $u \in P$. Given $u \in P$, we can choose $u' \in P'$ such that $\alpha'(u') = -\alpha(u)$, since α' is surjective. It

follows that π is surjective. $u \oplus u' \in \mathrm{Ker}\,(\pi)$ iff $u = 0$ and $u' \in \mathrm{Ker}\,(\alpha') = M_1'$. Thus, $\mathrm{Ker}\,(\pi) \cong M_1'$, and we have a short exact sequence

$$(*) \quad 0 \to M_1' \to N \to P \to 0.$$

Since P is projective, and since $N \to P \to 0$ is surjective, the identity map $P \to P$ lifts to a map $\gamma : P \to N$ such that $\pi \circ \gamma$ is the identity map on P. This means that the short exact sequence $(*)$ is split, and so $N \cong M_1' \oplus P$, as required. $\square$

It follows by a straightforward induction that for any two k th modules of syzygies M_k and M_k' of M, there are projectives P and P' such that

$$M_k \oplus P' \cong M_k' \oplus P.$$

Note that if R and M are Noetherian, we may take all the projectives used to be finitely generated, and then all the modules of syzygies will be finitely generated. Given two finitely generated k th modules of syzygies M_k and M_k' of M obtained in this way, we can find finitely generated projectives P and P' such that

$$M_k \oplus P' \cong M_k' \oplus P.$$

If R is local, the situation is simplified by the fact that finitely generated projective modules are free. (This is also true for infinitely generated projective modules, by a theorem of Kaplansky, but we have not proved it.)

Let R be a nonzero ring. A module M is said to have *finite projective dimension* if it has a finite projective resolution. The *projective dimension* of the 0 module is defined to be -1. The *projective dimension* of a nonzero projective module is defined to be 0. Recursively, the *projective dimension* of a module M is defined to be n if it has a projective resolution

$$0 \to P_n \to \cdots \to P_1 \to P_0 \to 0$$

(where $M \cong P_0/\mathrm{Im}\,(P_1)$) and it does not have projective dimension $n-1$. That is, a nonzero module M has projective dimension n if and only if a shortest projective resolution of M has length n. Modules that do not have a finite projective resolution are said to have *infinite projective dimension*, or projective dimension $+\infty$. The projective dimension of M is denoted $\mathrm{pd}_R M$ or simply $\mathrm{pd}\, M$.

From what we have said, if M is not 0, $\mathrm{pd}\, M \leq n$ iff some (equivalently, every) n th module of syzygies of M is projective. It is straightforward to see that if M is not projective and M_1 is a first module of syzygies of M, then $\mathrm{pd}\, M_1 = \mathrm{pd}\, M - 1$, where we define $+\infty - 1 = +\infty$.

From the results proved in the previous lecture, it is clear that a finitely generated nonzero module M over a local ring has finite projective dimension if and only if its minimal resolution is finite, which happens if and only if some $\mathrm{Tor}_i^R(M, K) = 0$, $i \geq 1$, in which case $\mathrm{pd}_R M < i$. What happens is that either no $\mathrm{Tor}_i^R(M, K)$ vanishes for $i \geq 0$, which is the case where M has infinite projective dimension, or that these vector spaces are nonzero up to the projective dimension of M, and then are all 0. In particular:

Corollary. *Let M be a finitely generated nonzero module over a local ring (R, m, K). Then M has finite projective dimension if and only if some $\operatorname{Tor}_i^R(M, K) = 0$, $i \geq 1$, and the projective dimension is the largest value of i such that $\operatorname{Tor}_i^R(M, K) \neq 0$.* $\square$

Our next goal is to prove:

Theorem (Auslander-Buchsbaum-Serre). *Let (R, m, K) be a local ring of Krull dimension d. Then the following conditions are equivalent:*
(1) *K has finite projective dimension over R.*
(2) *Some $\operatorname{Tor}_i^R(K, K)$ vanishes for $i \geq 1$.*
(3) *$\operatorname{pd}_R K = d$.*
(4) *Every finitely generated R-module has finite projective dimension.*
(5) *R is a regular local ring.*

We have already shown that (5) implies both (3) and (4), both of which clearly imply (1), and that (1) and (2) are equivalent. What remains to be done is to show that (1) implies (4). Once we have proved this, we can show easily that if we localize a regular local ring at any prime, we get a regular local ring. I do not know how to prove this without using the equivalence of (1) and (5). It was an open question for a long time, until homological methods were introduced into commutative algebra.

Math 615: Lecture of February 13, 2012

Note that if $R = K[[x, y]]$, the formal power series ring in two variables, and m is the maximal ideal of R, then we have a map $m \otimes_R m \to m^2$ sending $u \otimes v$ to uv. In problem **5.** of Problem Set #4 in Math 614, one was asked to show for $R = K[x, y]$ that the kernel of this map is spanned by $x \otimes y - y \otimes x$, which is killed by (x, y) and generates a copy of K in $m \otimes_R m$. The present situation is entirely analogous. We want to see what the long exact sequence for Tor implies here. We have a short exact sequence

$$0 \to m \to R \to K \to 0.$$

Applying $\_ \otimes_R m$ we get:

$$0 \to \operatorname{Tor}_1^R(K, m) \to m \otimes_R m \to m \to m/m^2 \to 0,$$

where the map $m \otimes_R m \to m$ is easily checked to send $u \otimes v$ to uv and so has image m^2. Since m is a first module of syzygies of K,

$$\operatorname{Tor}_1^R(K, m) \cong \operatorname{Tor}_2^R(K, K),$$

which we have already seen is K. Thus, understanding Tor tells us that Ker $(m \otimes_R m \twoheadrightarrow m^2)$ will be a copy of $K = R/m$.

Note that if I and J are any two ideals of R, applying $\_ \otimes_R R/J$ to

$$0 \to I \to R \to R/I \to 0$$

produces

$$0 \to \operatorname{Tor}_1^R(R/I,\, R/J) \to I/IJ \to R/J \to R/(I+J) \to 0$$

showing that

$$\operatorname{Tor}_1^R(R/I,\, R/J) \cong \operatorname{Ker}\,(I/IJ \to R/J),$$

where $[i]$ mod IJ maps to $[i]$ mod J. The kernel is evidently $(I/\cap J)/IJ$, so that

$$\operatorname{Tor}_1^R(R/I,\, R/J) = (I \cap J)/IJ.$$

The condition that $\operatorname{Tor}_1^R(R/I,\, R/J) = 0$ may be thought of as saying that I and J are "relatively prime." It always holds when I and J are comaximal (since the Tor is killed by $I + J = R$), and it holds for nonzero principal ideals $I = fR$ and $J = gR$ in a UFD R if and only if f and g have no common prime factor.

We want to make one more observation about modules of syzygies. Suppose that an R-module M has generators $u_1, \ldots, u_n$ and that one maps a free module $R^n \twoheadrightarrow M$ by sending $(r_1, \ldots, r_n)$ to $\sum_{j=1}^n r_j u_j$. The kernel is a first module of syzygies of M, but it also the module of all relations on the generators $u_1, \ldots, u_n$ of M, and is called the *module of relations* on $u_1, \ldots, u_n$. Thus, when the projective used is free, we may think of the first module of syzygies as a module of relations.

Proposition. *Let (R, m, K) a local ring.*

Given a finite exact sequence of finitely generated R-modules such that every term but one has finite projective dimension, then every term has finite projective dimension.

In particular, given a short exact sequence

$$0 \to M_2 \to M_1 \to M_0 \to 0$$

of finitely generated R-modules, if any two have finite projective dimension over R, so does the third. Moreover:

(a) $\operatorname{pd} M_1 \leq \max\{\operatorname{pd} M_0,\, \operatorname{pd} M_2\}$.
(b) *If* $\operatorname{pd} M_1 < \operatorname{pd} M_0$ *are finite, then* $\operatorname{pd} M_2 = \operatorname{pd} M_0 - 1$. *If* $\operatorname{pd} M_1 \geq \operatorname{pd} M_0$, *then* $\operatorname{pd} M_2 \leq \operatorname{pd} M_1$.
(c) $\operatorname{pd} M_0 \leq \max\{\operatorname{pd} M_1, \operatorname{pd} M_2 + 1\}$.

Proof. Consider the long exact sequence for Tor:

$$\cdots \to \operatorname{Tor}_{n+1}^R(M_1, K) \to \operatorname{Tor}_{n+1}^R(M_0, K) \to \operatorname{Tor}_n(M_2, K)$$
$$\to \operatorname{Tor}_n^R(M_1, K) \to \operatorname{Tor}_n^R(M_0, K) \to \cdots$$

If two of the M_i have finite projective dimension, then two of any three consecutive terms are eventually 0, and this forces the third term to be 0 as well.

The statements in (a), (b), and (c) bounding some $\operatorname{pd} M_j$ above for a certain $j \in \{0, 1, 2\}$ all follow by looking at trios of consecutive terms of the long exact sequence such that the middle term is $\operatorname{Tor}_n^R(M_j, K)$. For n larger than the specified upper bound for $\operatorname{pd}_R M_j$, the

Tor on either side vanishes. The equality in (b) for the case where $\operatorname{pd} M_1 < \operatorname{pd} M_0$ follows because with $n = \operatorname{pd} M_0 - 1$, $\operatorname{Tor}^R_{n+1}(M_0, K)$ injects into $\operatorname{Tor}^R_n(M_2, K)$.

The statement about finite exact sequences of arbitrary length now follows by induction on the length. If the length is smaller than three we can still think of it as 3 by using terms that are 0. The case of length three has already been handled. For sequences of length 4 or more, say

$$0 \to M_k \to M_{k-1} \to \cdots \to M_1 \to M_0 \to 0,$$

either M_k and M_{k-1} have finite projective dimension, or M_1 and M_0 do. In the former case we break the sequence up into two sequences

$$0 \to M_k \to M_{k-1} \to B \to 0$$

and

$$(*) \quad 0 \to B \to M_{k-2} \to \cdots \to M_1 \to M_0 \to 0.$$

The short exact sequence shows that $\operatorname{pd} B$ is finite, and then we may apply the induction hypothesis to $(*)$. If M_1 and M_0 have finite projective dimension we use exact sequences

$$0 \to Z \to M_1 \to M_0 \to 0$$

and

$$0 \to M_k \to M_{k-1} \to \cdots \to M_2 \to Z \to 0$$

instead. $\square$

Lemma. *If M has finite projective dimension over (R, m, K) local, and $m \in \operatorname{Ass}(R)$, then M is free.*

Proof. If not, choose a minimal free resolution of M of length $n \geq 1$ and suppose that the left hand end is

$$0 \to R^b \xrightarrow{A} R^a \to \cdots$$

where A is an $a \times b$ matrix with entries in m. The key point is that the matrix A cannot give an injective map, because if $u \in m - \{0\}$ is such that $\operatorname{Ann}_R u = m$, then A kills a column vector whose only nonzero entry is u. $\square$

Lemma. *If M has finite projective dimension over R, and x is not a zerodivisor on R and not a zerodivisor on M, then M/xM has finite projective dimension over both R and over R/xR.*

Proof. Let $P_\bullet$ be a finite projective resolution of M over R. Then $P_\bullet \otimes_R R/xR$ is a finite complex of projective R/xR-modules whose homology is $\operatorname{Tor}^R_n(M, R/xR)$, which is 0 for $n \geq 1$ when x is not a zerodivisor on R or M. This gives an (R/xR)-projective resolution of M over R/xR. The short exact sequence

$$0 \to P \xrightarrow{x} P \to P/xP \to 0$$

shows that each P/xP has projective dimension at most 1 over R, and then M/xM has finite projective dimension over R by the Proposition above. $\square$

Lemma. *Let (R, m, K) be local, let I_n denote the $n \times n$ identity matrix over R, let x be an element of $m - m^2$, and let A, B be $n \times n$ matrices over R such that $xI_n = AB$. Suppose that every entry of A is in m. Then B is invertible.*

Proof. We use induction on n. If $n = 1$, we have that $(x) = (a)(b) = (ab)$, where $a \in m$. Since $x \notin m^2$, we must have that b is a unit. Now suppose that $n > 1$. If every entry of B is in m, the fact that $xI_n = AB$ implies that $x \in m^2$ again. Thus, some entry of B is a unit. We permute rows and columns of B to place this unit in the upper left hand corner. We multiply the first row of B by its inverse to get a 1 in the upper left hand corner. We next subtract multiples of the first column from the other columns, so that the first row becomes a 1 followed by a string of zeros. We then subtract multiples of the first row from the other rows, so that the first column becomes 1 with a column of zeros below it. Each of these operations has the effect of multiplying on the left or on the right by an invertible $n \times n$ matrix. Thus, we can choose invertible $n \times n$ matrices U and V over R such that $B' = UBV$ has the block form

$$B' = \begin{pmatrix} 1 & 0 \\ 0 & B_0 \end{pmatrix},$$

where the submatrices 1, 0 in in the first row are 1×1 and $1 \times (n-1)$, respectively, while the submatrices 0, B_0 in the second row are $(n-1) \times 1$ and $(n-1) \times (n-1)$, respectively.

Now, with

$$A' = V^{-1}AU^{-1},$$

we have

$$A'B' = V^{-1}AU^{-1}UBV = V^{-1}(AB)V = V^{-1}(xI_n)V = x(V^{-1}I_nV) = xI_n,$$

so that our hypothesis is preserved: A' still has all entries in m, and the invertibility of B has not been changed. Suppose that

$$A' = \begin{pmatrix} a & \rho \\ \gamma & A_0 \end{pmatrix}$$

where $a \in R$ (technically a is a 1×1 matrix over R), ρ is $1 \times (n-1)$, γ is $(n-1) \times 1$, and A_0 is $(n-1) \times (n-1)$. Then

$$xI_n = A'B' = \begin{pmatrix} a(1) + \rho(0) & a(0) + \rho B_0 \\ \gamma(1) + A_0(0) & \gamma(0) + A_0B_0 \end{pmatrix} = \begin{pmatrix} a & \rho B_0 \\ \gamma & A_0B_0 \end{pmatrix}$$

from which we can conclude that $xI_{n-1} = A_0B_0$. By the induction hypothesis, B_0 is invertible, and so B' is invertible, and the invertibility of B follows as well. $\square$

The following is critical in proving that if K has finite projective dimension over (R, m, K) then R is regular.

Theorem. *If M is finitely generated and has finite projective dimension over R, and $x \in m - m^2$ kills M and is not a zerodivisor in R, then M has finite projective dimension over R/xR.*

Proof. We may assume M is not 0. M cannot be free over R, since $xM = 0$. Thus, we may assume $\mathrm{pd}_R M \geq 1$. We want to reduce to the case where $\mathrm{pd}_R M = 1$. If $\mathrm{pd}_R M > 1$, we can think of M as a module over R/xR and map $(R/xR)^{\oplus h} \twoheadrightarrow M$ for some h. The kernel M_1 is a first module of syzygies of M over R/xR. By part (b) of the Proposition, $\mathrm{pd}_R M_1 = \mathrm{pd}_R M - 1$. Clearly, if M_1 has finite projective dimension over R/xR, so does M. By induction on $\mathrm{pd}_R M$ we have therefore reduced to the case where $\mathrm{pd}_R M = 1$. To finish the proof, we shall show that if $x \in m - m^2$ is not a zerodivisor in R, $xM = 0$, and $\mathrm{pd}_R M = 1$, then M is free over R/xR.

Consider a minimal free resolution of M over R, which will have the form

$$0 \to R^n \xrightarrow{A} R^k \to M \to 0$$

where A is an $k \times n$ matrix with entries in m. If we localize at x, we have $M_x = 0$, and so

$$0 \to R_x^n \to R_x^k \to 0$$

is exact. Thus, $k = n$, and A is $n \times n$. Let e_j denote the j th column of the identity matrix I_n. Since $xM = 0$, every xe_j is in the image of A, and so we can write $xe_j = Ab_j$ for a certain $n \times 1$ column matrix b_j over R. Let B denote the $n \times n$ matrix over R whose columns are $b_1, \ldots, b_n$. Then $xI_n = AB$. By the preceding Lemma, B is invertible, and so A and $AB = xI_n$ have the same cokernel, up to isomorphism. But the cokernel of xI_n is $(R/xR)^{\oplus n} \cong M = \mathrm{Coker}\,(A)$, as required. $\square$

We can now prove the result that we are aiming for, which completes the proof of the Theorem stated at the end of the previous lecture.

Theorem. *Let (R, m, K) be a local ring such that $\mathrm{pd}_R K$ is finite. Then R is regular.*

Proof. If $m \in \mathrm{Ass}\,(R)$, then we find that K is free. But $K \cong R^n$ implies that $n = 1$ and R is a field, as required. We use induction on $\dim(R)$. The case where $\dim(R) = 0$ follows, since in that case $m \in \mathrm{Ass}\,(R)$.

Now suppose that $\dim(R) \geq 1$ and $m \notin \mathrm{Ass}\,(R)$. Then m is not contained in m^2 nor any of the primes in $\mathrm{Ass}\,(R)$, and so we can choose $x \in m$ not in m^2 nor in any associated prime. This means that x is not a zerodivisor in R. By the preceding Theorem, the fact that K has finite projective dimension over R implies that it has finite projective dimension over R/xR. By the induction hypothesis, R/xR is regular. Since $x \notin m^2$ and x is not a zerodivisor, both the least number of generators of the maximal ideal and the Krull dimension drop by one when we pass from R to R/xR. Since R/xR is regular, so is R. $\square$

Math 615: Lecture of February 15, 2012

We can give some immediate corollaries of our homological characterization of regular local rings. First note:

Proposition. *Let R be a ring and M an R-module.*
(a) *If $\mathrm{pd}_R M = n$ and S is flat over R, then $\mathrm{pd}_S S \otimes_R M \leq n$. In particular, this holds when S is a localization of R.*
(b) *If $(R, m) \to (S, Q)$ is local homomorphism of local rings (i.e., m maps into Q), S is R-flat, M is finitely generated, and $\mathrm{pd}_R M = n$ (whether finite or infinite) then $\mathrm{pd}_S S \otimes_R M = n$.*

Proof. For part (a) take a projective resolution $P_\bullet$ of M. Then $S \otimes_R P_\bullet$ gives a projective resolution of the same length for $S \otimes_R M$: because S is flat, $S \otimes_R \_$ preserves exactness. For part (b), choose $P_\bullet$ to be a minimal projective resolution for M over R, whether finite or infinite. Applying $S \otimes_R \_$ gives a minimal resolution of $S \otimes_R M$: the entries of each matrix occurring in $P_\bullet$ map into Q because the homomorphism is local. The two minimal resolutions have the same length. $\square$

Corollary. *If (R, m) is a regular local ring, then for every prime ideal Q of R, R_Q is regular.*

Proof. $\mathrm{pd}_{R_Q} R_Q/QR_Q \leq \mathrm{pd}_R R/Q$ by (a) of the Proposition just above, and so is finite. $\square$

Corollary. *If $(R, m) \to (S, Q)$ is a flat local homomorphism of local rings and S is regular, then R is regular.*

Proof. $\mathrm{pd}_R R/m = \mathrm{pd}_S S \otimes_R (R/m)$ and so is finite, by part (b) of the proposition just above. $\square$

We define a Noetherian ring to be *regular* if all of its local rings at prime ideals are regular. By the first Corollary above, it is equivalent to require that its local rings at maximal ideals be regular.

Corollary. *Over a regular ring of Krull dimension d,* $\mathrm{pd} M \leq d$ *for every finitely generated R-module M.*

Proof. Consider a projective resolution of M by finitely generated projective modules, say $P_\bullet$, and let $M_d = \mathrm{Ker}\,(P_{d-1} \to P_{d-2})$, so that

$$0 \to M_d \to P_{d-1} \to P_{d-2} \to \cdots \to P_1 \to P_0 \to M \to 0$$

is exact. It suffices to prove that M_d is projective. By the Theorem proved at the beginning of the Lecture Notes from November 7 for Math 614 last semester, projective is equivalent to locally free (and to flat) for finitely generated modules over a Noetherian ring. Localize the sequence at some prime ideal Q of R. Then R_Q is regular of dimension at most d, and so $(M_d)_Q$ is R_Q-free, since it is a dth module of syzygies over a regular local ring of Krull dimension at most d. $\square$

There are regular Noetherian rings of infinite Krull dimension. An example of such a ring was given in problem **2.** of Problem Set #6 from Math 614 last semester. But even over such a ring, every finitely generated module has finite projective dimension, by the result of **5.** in the current problem set, #3.

Let $R \to S$ be a homomorphism of Noetherian rings, let I be an ideal of R, and choose generators of I, say $I = (x_1, \ldots, x_n)R$. Let be M a finitely generated S-module. In this

situation, we want to define the *depth* of of M on I: we let the depth be $+\infty$ if $IM = M$, while if $IM \neq M$, we let it be the length of any maximal regular sequence in I on M. To justify this definition we need to prove that all maximal regular sequences have the same length: in the course of doing so, we shall show that the depth is at most the number of generators of I.

Note first that $IM = M$ iff $IS + \mathrm{Ann}_S M = S$. For $IM = M$ iff $ISM = M$ iff $S/IS \otimes_S M = 0$. By the Proposition at the top of the third page of the Lecture Notes from November 5 for Math 614, the support of a tensor product of two finitely generated modules over a Noetherian ring is the intersection of their supports: this means that the tensor product is 0 if and only if the sum of the annihilators is the unit ideal, since the support of a finitely generated module is the set of primes containing its annihilator. Thus, in the situation where depth is taken to be $+\infty$, the Koszul homology $\mathcal{K}_\bullet(\underline{x};\, M)$ all vanishes, since it is killed by $(x_1, \ldots, x_n)$ and by $\mathrm{Ann}_S M$.

We shall prove very shortly that the length of a maximal regular sequence on M in $I = (x_1, \ldots, x_n)R$ can be recovered by looking at the number of Koszul homology modules, starting the count with $H_n(\underline{x};\, M)$, that vanish. We prove a preliminary result that does not need any finiteness hypotheses.

Lemma. *Let R be any ring, let $I = (x_1, \ldots, x_n)R$, and let M be any R-module. Suppose that $f_1, \ldots, f_d \in I$ is an improper regular sequence on M. Then $H_{n-j}(\underline{x};\, M) = 0$, $0 \leq j < d$. In particular, if $x_1, \ldots, x_n$ is an improper regular sequence on M, then $H_i(\underline{x};\, M) = 0$ for all $i \geq 1$.*

Proof. We use induction on d. Note that $H_i(\underline{x};\, M) = 0$ for $i \geq n+1$ and any M. If $d = 1$, we use the fact that $H_n(\underline{x};\, M) \cong \mathrm{Ann}_M(x_1, \ldots, x_n)$: since $f_1 \in I$ is a nonzerodivisor on M, then annihilator vanishes. Now suppose that $d > 1$ and that we know that the result for smaller integers. We have the exact sequence

$$0 \to M \xrightarrow{f_1} M \to M/f_1 M \to 0.$$

In the long exact sequence for Koszul homology, the maps given by multiplication by any element of I, including f_1, are 0. This implies that the long exact sequence can be broken up into short exact sequences:

$$(*_j) \quad 0 \to H_{j+1}(\underline{x};\, M) \to H_{j+1}(\underline{x};\, M/f_1 M) \to H_j(\underline{x};\, M) \to 0.$$

But we know that $f_2, \ldots, f_d$ is a regular sequence on $M/f_1 M$, from which we deduce that $H_{j+1}(\underline{x};\, M/f_1 M) = 0$ for all $j + 1 > n - (d-1) = n - d + 1$, by the induction hypothesis. The result we want now follows at once from the sequences $(*_j)$, since the vanishing of the middle term implies the vanishing of both end terms. $\square$

Theorem (Koszul complex characterization of depth). *Let R, S be Noetherian rings such that S is an R-algebra, let $I = (x_1, \ldots, x_n)R$, and let M be a Noetherian S-module. If $IM \neq M$ then any regular sequence in I on M has length at most n, and if d is the length of any maximal regular sequence, then $H_{n-j}(\underline{x};\, M) = 0$ for $j < d$, while $H_{n-d}(\underline{x};\, M) \neq 0$. Thus, all maximal regular sequences on M in I have the same length.*

Moreover, $\operatorname{depth}_I M = \operatorname{depth}_{IS} M$.

Proof. We already know from the Lemma that if there is a regular sequence of length d, then $H_{n-j}(\underline{x};\, M) = 0$ for $j < d$. Since $H_0(\underline{x};\, M) = M/IM$ does not vanish here, we immediately see that the length of any regular sequence on M in I is bounded by n. It remains only to show that if $f_1, \ldots, f_d \in I$ is a maximal regular sequence, then $H_{n-d}(\underline{x}; M) \neq 0$.

We use induction on d. If $d = 0$, this means that $(x_1, \ldots, x_d)R$ consists entirely of zerodivisors on M, which means in turn that it is contained in the union of inverse images in R of the associated primes of M in S. Therefore, it is contained in one of these, and there exists $u \in M - \{0\}$ killed by $(x_1, \ldots, x_d)$. But then $u \in Ann_M(x_1, \ldots, x_n)R = H_n(\underline{x};\, M)$. Now suppose that $d > 0$ and we know the result for smaller d. Now we know that $f_2, \ldots, f_d$ is a *maximal* regular sequence on M/f_1M, so that $H_{n-d+1}(\underline{x};\, M/f_1M) \neq 0$. With notation as in the proof of the Lemma, we have for $j = n - d$ an exact sequence:

$$(*_{n-d}) \quad 0 \to H_{n-d+1}(\underline{x};\, M) \to H_{n-d+1}(\underline{x};\, M/f_1M) \to H_{n-d}(\underline{x};\, M) \to 0.$$

We know that $H_{n-d+1}(\underline{x};\, M) = 0$ from the Lemma, and so the other two terms are isomorphic, yielding that $H_{n-d}(\underline{x};\, M) \cong H_{n-d+1}(\underline{x};\, M/f_1M) \neq 0$.

The final statement follows because the Koszul complex of S with respect to the images of the x_j in S is the same as $\mathcal{K}_\bullet(\underline{x};\, M)$ over R. $\square$

Thus, our notion of depth is well-defined. If $(R,\, m)$ is local, $\operatorname{depth} M$ means $\operatorname{depth}_m M$. Some authors ambiguously refer to $\operatorname{depth}_I R$ as $\operatorname{depth} I$, which can lead to confusion in the case where I is an ideal of a local ring, where it might mean $\operatorname{depth}_m I$ with I considered as a module rather than an ideal. We shall not use $\operatorname{depth} I$ for $\operatorname{depth}_I R$.

We are now in a position to prove that a regular domain is normal.

Theorem. *If R is a regular domain, then R is normal.*

Proof. By the Theorem on the second page of the Lecture Notes of December 1 for Math 614, it suffices to see that an associated prime of a principal ideal has height one, and that the localization at a height one prime is a DVR. To see the first statement, we can localize at such an associated prime. Then we have a regular local ring $(R,\, m)$ such that one nonzero element gives a maximal regular sequence in m on R. Take $x \in m - m^2$. Since all maximal regular sequences have the same length, x also gives a maximal regular sequence. But R/xR is a domain, and so this can only be true if $m = xR$ is maximal. Finally, a one-dimensional regular ring has a maximal ideal that is generated by one element, and so it must be a DVR. $\square$

Math 615: Lecture of February 17, 2012

We discuss a method for determining the ideal of all leading forms of an ideal generated by polynomials with constant term zero in a formal power series ring $K[[x_1, \ldots, x_n]]$ over a field K.

Suppose that

$$f_1, \ldots, f_h \in m = (x_1, \ldots, x_n)R,$$

where $R = K[[x_1, \ldots, x_n]]$, a formal power series ring. Let $I = (f_1, \ldots, f_h)$. To find

$$\mathcal{L}(I) \subseteq \mathrm{gr}_m R \cong K[x_1, \ldots, x_n],$$

first note that if $g \neq 0, g_1, \ldots, g_n \in R$ are such that $g = \sum_{i=1}^m f_i g_i$, and $\deg \mathcal{L}(g) = d$, then $\mathcal{L}(g)$ is unchanged if we drop all terms of degree $> d$ from the g_i, although the value of g changes. Thus, we may assume that the $g_i \in K[x_1, \ldots, x_n] \subseteq R$. There is a K-homomorphism

$$\Theta : K[x_1, \ldots, x_n] \to K[t, x_1, \ldots, x_n] = B$$

with $x_i \mapsto x_i t$. Let $f^\diamondsuit$ denote $\Theta(f)$. Then $g^\diamondsuit = t^d G$, where $G|_{t=0} = \mathcal{L}(g)$. In other words, when $g^\diamondsuit$ is regarded as a polynomial in t, its constant term is $\mathcal{L}(g)$.

Let

$$J_s = (f_1^\diamondsuit, \ldots, f_n^\diamondsuit) :_B t^s.$$

The argument above shows that every leading form of an element of I is the constant term of some element of J_s for some s. Note that the ideals J_s ascend with s and so are eventually all equal. The converse is also true: if $t^s G \in (f_1^\diamondsuit, \ldots, f_h^\diamondsuit)B$, we may substitute $t = 1$ to obtain that $G(1, x_1, \ldots, x_n) \in (f_1, \ldots, f_n)K[x_1, \ldots, x_n]$, and it follows that the constant term of G when viewed as a polynomial in t is in $\mathcal{L}(I)$.

Therefore, to get generators of $\mathcal{L}(f_1, \ldots, f_m)$, think of the generators of J_s for s sufficiently large as polynomials in t and take their constant terms.

Evidently, $tu \in J_s$ iff $t^s(tu) \in (f_1^\diamondsuit, \ldots, f_n^\diamondsuit) = J_0$, and so $J_{s+1} = J_s :_B t$. Therefore, the sequence J_s is stable as soon as $J_s = J_{s+1}$ for one value of s, for then t is not a zerodivisor on J_s. We indicate how to find J_{s+1} once J_s is known. Suppose that $a_1, \ldots, a_k \in B$ are generators in J_s. Then the elements b of J_{s+1} are those that satisfy $bt = \sum_{j=1}^k q_j a_j$ for some choice of q_j. If we have a set of generators for the relations on t, $a_1, \ldots, a_k$, the coefficients of t will generate J_{s+1}. In considering such relations, if $q_j = Q_j + tH_j$ where $Q_j \in K[x_1, \ldots, x_n]$, then we have

$$(b - \sum_{j=1}^k H_j a_j)t = \sum_{j=1}^k Q_j a_j.$$

Since $\sum_{j=1}^k H_j a_j \in J_s$, the additional generators for J_{s+1} over J_s all come from relations $b't = \sum_{j=1}^k Q_j a_j$ where the $Q_j \in K[x_1, \ldots, x_n]$. Let $a_j = A_j + tW_j$ with $A_j \in K[x_1, \ldots, x_n]$. Then the Q_j must give a relation on the A_j. Each relation on the A_j gives rise to a value of b', and we get generators for J_{s+1} if we take the generators of J_s and those values of b' coming from generators for the relations on the A_j in $K[x_1, \ldots, x_n]$.

We now consider the specific example in $K[[x, y, z]]$ where $f_1 = x^2 - y^3 + z^6$ and $f_2 = xy - z^3$.

Then $(x^2-y^3+z^6)^\diamondsuit = t^2a$ for $a = x^2-ty^3+t^4z^6$ and $(xy-z^3)^\diamondsuit = t^2b$ for $b = xy-tz^3$, and so $a, b \in J_2$. Then $ya - xb = tc$ (using the obvious generator for the relations on x^2, xy) where $c = -y^4 + xz^3 + t^3yz^6 \in J_3$. We will show that t is not a zerodivisor mod $(a, b, c) = J_3$. The constant terms of a, b, c are x^2, xy, $-y^4 + xz^3$. Clearly, in any relation $Q_1x^2 + Q_2xy + Q_3(-y^4 + xz^3) = 0$, we must have that $x \mid Q_3$. One such relation is $(-z^3, y^3, x)$. Given any other, we can subtract a multiple of $(-z^3, y^3, x)$ from it so as to make $Q_3 = 0$. This leaves a relation of the form $(Q_1',\, Q_2',\, 0)$, which is essentially a relation on x^2, xy, and so must be a multiple of $(y,\, -x,\, 0)$. That is, $(y, -x, 0)$ and $(-z^3, y^3, x)$ span the relations. $ya - xb$ gives nothing new, while

$$-z^3a + y^3b + xc = ty^3z^3 - t^4z^9 - ty^3z^3 + t^3xyz^6 = t^3xyz^6 - t^4z^9 = t^3z^6b,$$

and so $t^2z^6b \in J_4$. Since $b \in J_2 \subseteq J_3$, $J_4 = J_3$ and t is not a zerodivisor on $(a, b, c) = J_3$. This shows that $\mathcal{L}(I) = (x^2,\, xy,\, -y^4 + xz^3)$.

Example. When the leading form of f in $\operatorname{gr}_m R$ is L and one kills an ideal $\mathfrak{A} \subseteq m$, even if it is principal, it need not be true that the leading form of the image $\overline{f}$ in $\operatorname{gr}_{\overline{m}}(R/I)$ is the image of L. For example, suppose that $R = K[[x, y, z]]$ with $f = xy + y^{101}z^{997}$. The leading form of f is xy. But in the quotient R/xR, the leading form of the image of f is $y^{101}z^{997}$.

Our next goal is to prove a famous theorem of Auslander and Buchsbaum connecting depth and projective dimension. We first want to observe some basic facts about the behavior of depth.

Proposition. *Let $R \to S$ be a homomorphism of Noetherian rings, let M be a finitely generated S-module, and let I be an ideal of R. Let I and J be ideals of R.*

(a) *Let T be a flat Noetherian S-algebra. Then* $\operatorname{depth}_I T \otimes_S M \geq \operatorname{depth}_I M$, *with equality if T is faithfully flat. In particular, depth can only increase if T is a localization of S.*

(b) $\operatorname{depth}_I M = \inf_{Q \in \operatorname{Supp}_S(M/IM)} \operatorname{depth}_I M_Q = \inf_{Q \in \operatorname{Spec}(S)} \operatorname{depth}_I M_Q$. *(The infimum of the empty set is defined to be $+\infty$.)*

(c) *If I and J have the same radical,* $\operatorname{depth}_I M = \operatorname{depth}_J M$.

Proof. (a) Let $I = (x_1, \ldots, x_n)$. Then for all j,

$$H_j(\underline{x};\, T \otimes_S M) \cong T \otimes_S H_j(\underline{x}; M),$$

since T is S-flat. Thus, the number of vanishing Koszul homology modules cannot decrease when we tensor with T. Moreover, if T is faithfully flat, neither can it increase. Note that the case of infinite depth corresponds to the case where all Koszul homology vanishes.

(b) By part (a), localizing can only increase the depth. It suffices to show that if $M \neq IM$, we can localize at a prime while preserving the depth. Let $f_1, \ldots, f_d$ be a maximal regular sequence in I on M. Then $M/(f_1, \ldots, f_d)M$ has depth 0, and so I is contained in the union of the inverse images of the finitely many primes in $\operatorname{Ass}_S\big(M/(f_1, \ldots, f_d)M\big)$. Thus, it is contained in the inverse image of one of these primes: call it Q. Replace M by M_Q.

We still have $QS_Q \in \operatorname{Ass}_S\big((M/(x_1, \ldots, x_n)M)_Q\big)$, and so $f_1, \ldots, f_d \in I$ is a maximal regular sequence on M_Q.

(c) It suffices to consider the case where J is the radical of I. A regular sequence in I is automatically a regular sequence in J. Given a regular sequence $f_1, \ldots, f_d$ in J, each f_j has a power $f_j^{N_j} \in I$. By the final problem of Problem Set #3, $f_1^{N_1}, \ldots, f_d^{N_d}$ is a regular sequence on M in I. $\square$

The next result is very similar to the Proposition at the top of the second page of the Notes from February 13, and its proof is very similar, although Koszul homology is used instead of $\operatorname{Tor}_\bullet^R(\_, K)$.

Proposition. *Let $R \to S$ be a homomorphism of Noetherian rings, let*

$$0 \to M_2 \to M_1 \to M_0 \to 0$$

be an exact sequence of finitely generated S-modules, and let I be an ideal of R. The following statements hold, even if one or more of the depths is $+\infty$ (with the conventions $+\infty \pm 1 = +\infty$ and if $u \in \mathbb{N} \cup \{+\infty\}$, $\min\{u, +\infty\} = u$).

(a) $\operatorname{depth}_I M_1 \geq \min\{\operatorname{depth}_I M_0, \operatorname{depth}_I M_2\}$.

(b) *If*

$$\operatorname{depth}_I M_1 > \operatorname{depth}_I M_0,$$

then

$$\operatorname{depth}_I M_2 = \operatorname{depth}_I M_0 + 1.$$

If $\operatorname{depth}_I M_1 \leq \operatorname{depth}_I M_0$, *then* $\operatorname{depth}_I M_2 \geq \operatorname{depth}_I M_1$.

(c) $\operatorname{depth}_I M_0 \geq \min\{\operatorname{depth}_I M_1, \operatorname{depth}_I M_2 - 1\}$.

Proof. Let $x_1, \ldots, x_s$ denote generators of the ideal I and consider the long exact sequence for Koszul homology:

$$\cdots \to H_{n+1}(\underline{x};\, M_1) \to H_{n+1}(\underline{x};\, M_0) \to H_n(\underline{x};\, M_2) \\ \to H_n(\underline{x};\, M_1) \to H_n(\underline{x};\, M_0) \to \cdots$$

If M_2 has infinite depth, then $H_n(\underline{x};\, M_1) \cong H_n(\underline{x};\, M_0)$ for all n, so that M_1 and M_0 have the same depth, and all of (a), (b), (c) hold. If M_1 has infinite depth, then $H_{n+1}(\underline{x};\, M_0) \cong H_n(\underline{x};\, M_2)$ for all n and $\operatorname{depth}_I M_2 = \operatorname{depth}_I M_0 + 1$. Again, all three statements hold. If M_0 has infinite depth then $H_n(\underline{x};\, M_2) \cong H_n(\underline{x};\, M_1)$ for all n, and $\operatorname{depth}_I M_2 = \operatorname{depth}_I M_1$. Again, all three statements hold. We may assume that all three depths are finite.

Part (a) follows from the long exact sequence because of $H_n(\underline{x};\, M_2) = 0 = H_n(\underline{x};\, M_0)$ for all $n > d$, then $H_n(\underline{x};\, M_1) = 0$ for all $n > d$. All of the other statements follow similarly from the long exact sequence for Koszul homology: each of the Koszul homology modules one needs to vanish is surrounded by two Koszul homology modules that vanish from the hypothesis. For the equality in part (b), let $d = \operatorname{depth}_I M_0$. We must show as well that $H_{s-(d+1)}(\underline{x};\, M_2) \neq 0$. Let $n = s - d - 1$ in the long exact sequence, which becomes:

$$\cdots \to 0 \to H_{s-d}(\underline{x};\, M_0) \to H_{s-d-1}(\underline{x};\, M_2) \to \cdots$$

and we know that $H_{s-d}(\underline{x};\, M_0) \neq 0$. $\square$

We also observe:

Lemma. *If (R, m, K) is local, M is a finitely generated nonzero R-module, $\mathrm{pd}_R M$ is finite, and $x \in m$ is a nonzerodivisor on R and on M, then and $\mathrm{pd}_{R/xR} M/xM = \mathrm{pd}_R M$.*

Proof. This sharpens the result of the second Lemma on the third page of the notes from February 13. Take a minimal resolution $P_\bullet$ of M over R. As in the proof of that Lemma, $R/xR \otimes_R P_\bullet$ is a resolution of M/xM over R/xR, but now we note that it is minimal, so that the projective dimension does not change. □

Theorem (M. Auslander and D. Buchsbaum). *Let (R, m, K) be local and $M \neq 0$ a finitely generated R-module. If M has finite projective dimension then*

$$\mathrm{pd}_R M + \mathrm{depth}\, M = \mathrm{depth}\, R.$$

Proof. If the depth of R is 0, then M is free, by the first Lemma on the third page of the Notes from February 13, and the result is clear. If the depth$R > 0$, and depth $M > 0$ as well, the maximal ideal of R is not contained in the union of all associated primes of R and of M. Thus, we can choose $x \in m$ that is not in any associated prime of M or of R, and so x is a nonzerodivisor on both R and M. By the Lemma just above, $\mathrm{pd}_{R/xR} M/xM = \mathrm{pd}_R M$, and by the induction hypothesis this is

$$\mathrm{depth}\, R/xR - \mathrm{depth}\, M/xM = \mathrm{depth}\, R - 1 - (\mathrm{depth}\, M - 1) = \mathrm{depth}\, R - \mathrm{depth}\, M,$$

as required. If the depth of R is positive and the depth of M is 0, form a short exact sequence

$$0 \to M' \to R^b \to M \to 0,$$

so that M' is a first module of syzygies of M. Then M' will have depth $0 + 1 = 1$ by part (b) of the preceding Proposition, while $\mathrm{pd}\, M' = \mathrm{pd}\, M - 1$. Working with M' we have that both depth R and depth M' are positive, and so we are in a case already done. Thus,

$$\mathrm{pd}\, M = \mathrm{pd}\, M' + 1 = (\mathrm{depth}\, R - \mathrm{depth}\, M') + 1 = \mathrm{depth}\, R - 1 + 1 = \mathrm{depth}\, R,$$

as required, since depth $M = 0$. □

Math 615: Lecture of February 20, 2012

We review some basic facts about the tensor and exterior algebras of a module over a commutative ring R. See also the Lecture Notes from Math 614 for December 5.

The tensor product of n copies of M with itself is denoted $M^{\otimes n}$ or $T_R^n(M) = T^n(M)$. By convention, $T^0(V) = R$. Then

$$T(M) = \bigoplus_{n=0}^{\infty} T^n(M)$$

becomes an associative (usually non-commutative) $\mathbb{N}$-graded ring with identity, with R in the center: the multiplication is induced by the obvious bilinear maps

$$T^m(M) \otimes_R T^n(M) \to T^{m+n}(M)$$

(each of these maps is an isomorphism). Note that this *tensor algebra* is generated as a ring over R by $T^1(M)$, which we may identify with M. Of course, $T^n(M)$ is the degree n component. Note that if $L : M \to N$ is an R-linear map, there is an induced map $T^n(L) : T^n(M) \to T^n(N)$, and $T^n(L' \circ L) = T^n(L') \circ T^n(L)$ when the composition $L' \circ L$ is defined. Together these maps give a degree preserving ring homomorphism $T(M) \to T(N)$, which is surjective whenever L is. T is a covariant functor from R-modules to $\mathbb{N}$-graded associative R-algebras such that R is in the center. Moreover, T has the following universal property: if $f : M \to S$ is any R-linear map of the R-module M into an associative R-algebra S with R in the center, then f extends uniquely to an R-linear ring homorphism $T(M) \to S$.

An R-multilinear map $M^n \to N$ is called *alternate* or *alternating* if its value is 0 whenever two entries of an n-tuple are equal. (This implies that switching two entries negates the value. Making an even permutation of the entries will not change the value, while an odd permutation negates the value.) Let $\bigwedge_R^n(M) = \bigwedge^n(M)$ denote the quotient of $M^{\otimes n}$ by the subspace spanned by all n-tuples two of whose entries are equal. We make the convention that $\bigwedge^0 R \cong R$, and note that we may identify $M \cong \bigwedge^1 M$. Then

$$\bigwedge(M) = \bigoplus_{n=0}^{\infty} \bigwedge^n(M)$$

is an associative $\mathbb{N}$-graded algebra with R in the center, with $\bigwedge^n(M)$ as the component in degree n. $\bigwedge(M)$ is called the *exterior algebra* of M over R, and $\bigwedge^n(M)$ is called the nth *exterior power* of M over R. One can also construct $\bigwedge(M)$ by killing the two-sided ideal of $T(M)$ generated by elements of the form $u \otimes u$, $u \in M$.

The multiplication on $\bigwedge(M)$ is often denoted $\wedge$. If the elements u_j span M, then the elements $u_{j_1} \wedge \cdots \wedge u_{j_i}$ span $\bigwedge^i(M)$. If v has degree m and w has degree n, then one can easily check that $v \wedge w = (-1)^{mn} w \wedge v$. Thus, the even degree elements are all in the center, while any two odd degree elements anti-commute. If G is free with free basis $u_1, \ldots, u_n$, then the elements $u_{j_1} \wedge \cdots \wedge u_{j_i}$, $1 \le j_1 < \cdots < j_i \le n$ form a free basis for $\bigwedge^i(G)$, and $\bigwedge^i(G)$ has rank $\binom{n}{i}$. In particular, $\bigwedge^N(G) = 0$ if $N >$ rank G (or, more generally, if G is not necessarily free but is spanned by fewer than N elements).

Given a linear map $L : M \to N$, there is an induced map $\bigwedge^n(L) : \bigwedge^n(M) \to \bigwedge^n(N)$, and $\bigwedge^n(L' \circ L) = \bigwedge^n(L) \circ \bigwedge^n(L')$ when the composition $L' \circ L$ is defined. Together these maps give a ring homomorphism of $\bigwedge(M) \to \bigwedge(N)$ that preserves degrees. Thus, $\bigwedge$ is a covariant functor from R-modules to graded associative R-algebras with R in the center.

An associative $\mathbb{N}$-graded R-algebra Λ such that R maps into the center of Λ and also into Λ_0 is called *skew-commutative* (or even *commutative* by some authors!) if whenever $u, v \in \Lambda$ are homogeneous,

$$uv = (-1)^{\deg(u)\deg(v)} vu$$

in Λ. Then $\bigwedge(M)$ has the following universal property: if Λ is any skew-commutative R-algebra and $\theta : M \to \Lambda_1$ any R-linear map, θ extends uniquely to a degree-preserving R-homomorphism $\bigwedge(M) \to \Lambda$.

If G is free of rank n with basis $u_1, \ldots, u_n$ and $L : G \to G$ has matrix α, then $\bigwedge^n(L) : \bigwedge^n G \to \bigwedge^n G$ sends $u_1 \wedge \cdots \wedge u_n$ to $\det(\alpha) u_1 \wedge \cdots \wedge u_n$. To see this, note that we have that

$$\bigwedge^n(u_1 \wedge \cdots \wedge u_n) = (a_{11}u_1 + \cdots + u_{n1}v_n) \wedge \cdots \wedge (u_{n1}v_1 + \cdots + a_{nn}u_n).$$

Expanding by the generalized distributive law yields n^n terms each of which has the form $a_{i_1,1} \cdots a_{i_n,n} u_{i_1} \wedge \cdots \wedge u_{i_n}$. If two of the i_t are equal, this term is 0. If they are all distinct, the v_{i_t} constitute all the elements $u_1, \ldots, u_n$ in some order: call the corresponding permutation σ. Rearranging the v_j gives $\operatorname{sgn}(\sigma) a_{i_1,1} \cdots a_{i_n,n} v_1 \wedge \cdots \wedge v_n$. The sum of all of the $n!$ surviving terms is $\det(\alpha) v_1 \wedge \cdots \wedge v_n$, using one of the standard definitions of $\det(\alpha)$. The fact that the determinant of a product of two $n \times n$ matrices is the product of the determinants may be deduced from the fact that $\bigwedge^n$ preserves composition.

Note also that if $M \to N$ is surjective, then $\bigwedge^n M \to \bigwedge^n N$ is surjective for all n. It is straightforward to check that if $R \to S$ is any map of commutative rings, there is an isomorphism

$$S \otimes_R \textstyle\bigwedge_R^n M \to \bigwedge_S^n (S \otimes_R M).$$

The map $M \to S \otimes M$ sending $u \mapsto 1 \otimes u$ induces a degree-preserving map

$$\textstyle\bigwedge_R M \to \bigwedge_S^n (S \otimes_R M),$$

and hence a map

$$S \otimes_R \textstyle\bigwedge_R M \to \bigwedge_S^n (S \otimes_R M).$$

On the other hand $S \otimes \bigwedge_R M$ is $S \otimes_R M$ in degree 1, giving an S-linear map of $S \otimes_R M$ into the degree one part of $S \otimes \bigwedge_R M$, and this yields a map

$$\textstyle\bigwedge_S^n (S \otimes_R M) \to S \otimes_R \bigwedge_R M,$$

using the appropriate universal mapping properties. These maps are easily checked to be mutually inverse degree-preserving S-algebra isomorphisms, under which

$$(s_1 \otimes u_1) \wedge \cdots \wedge (s_n \otimes u_n) \in \textstyle\bigwedge_S^n (S \otimes_R M)$$

corresponds to

$$(s_1 \cdots s_n) \otimes (u_1 \wedge \cdots \wedge u_n) \in S \otimes \textstyle\bigwedge_R M.$$

In particular, localization commutes with the formation of exterior algebras and exterior powers.

We have previously introduced $\mathcal{K}_i(x_1, \ldots, x_n; R)$ with a free R-basis consisting of elements $u_{j_1, \ldots, j_i}$ where $1 \le j_1 < \cdots < j_i \le n$. In particular, $u_1, \ldots, u_n$ is a free basis for $\mathcal{K}_1(x_1, \ldots, x_n; R)$. It turns out to be convenient to think of $\mathcal{K}_i(x_1, \ldots, x_n; R)$ as $\bigwedge^i(G)$,

where $G = \mathcal{K}_1(x_1, \ldots, x_n; R)$ is the free module on n generators, letting $u_{j_1, \ldots, j_i}$ correspond to $u_{j_1} \wedge \cdots \wedge u_{j_i}$. We obviously have isomorphisms of the relevant free R-modules. We still have $d(u_j) = x_j$, $1 \leq j \leq n$. The formula for the differential d is

$$(*) \quad d(u_{j_1} \wedge \cdots \wedge u_{j_i}) = \sum_{t=1}^{i} (-1)^{t-1} x_{j_t} u_{j_1} \wedge \cdots \wedge u_{j_{t-1}} \wedge u_{j_{t+1}} \cdots \wedge u_{j_i}.$$

We shall refer to an R-linear map of a graded skew-commutative R-algebra Λ into itself that lowers degrees of homogeneous elements by one and satisfies

$$(\#) \quad d(uv) = (du)v + (-1)^{\deg(u)} u\, dv$$

when u is a form as an *R-derivation.*

Once we identify $\mathcal{K}(x_1, \ldots, x_n; R)$ with $\bigwedge(G)$, the differential R is a derivation. By the R-bilinearity of both sides in u and v, it suffices to verify $(\#)$ when $u = u_{j_1} \wedge \cdots u_{j_h}$ and $v = u_{k_1} \wedge \cdots u_{k_i}$ with $j_1 < \cdots < j_h$ and $k_1 < \cdots < k_i$. It is easy to see that this reduces to the assertion $(**)$ that the formula $(*)$ above is correct even when the sequence $j_1, \ldots, j_i$ of integers in $\{1, 2, \ldots, n\}$ is allowed to contain repetitions and is not necessarily in ascending order: one then applies $(**)$ to $j_1, \ldots, j_h, k_1, \ldots, k_i$. To prove $(**)$, note that if we switch two consecutive terms in the sequence $j_1, \ldots, j_i$ every term on both sides of $(*)$ changes sign. If the $j_1, \ldots, j_i$ are mutually distinct this reduces the proof to the case where the elements are in the correct order, which we know from the definition of the differential. If the elements are not all distinct, we may reduce to the case where $j_t = j_{t+1}$ for some t. But then $u_{j_1} \wedge \cdots \wedge u_{j_i} = 0$, while all but two terms in the sum on the right contain $u_{j_t} \wedge u_{j_{t+1}} = 0$, and the remaining two terms have opposite sign.

Once we know that d is a derivation, we obtain by a straightforward induction on k that if $v_1, \ldots, v_k$ are forms of degrees $a_1, \ldots, a_k$, then

$$(***) \quad d(v_1 \wedge \cdots \wedge v_i) = \sum_{t=^i} (-1)^{a_1 + \cdots + a_{t-1}} v_{j_1} \wedge \cdots \wedge v_{j_{t-1}} \wedge dv_{j_t} \wedge v_{j_{t+1}} \wedge \cdots \wedge v_{j_i}.$$

Note that the formula $(*)$ is a special case in which all the given forms have degree 1.

It follows that the differential on the Koszul complex is uniquely determined by what it does in degree 1, that is, by the map $G \to R$, where G is the free R-module $\mathcal{K}_1(\underline{x}; R)$, together with the fact that it is a derivation on $\bigwedge(G)$. Any map $G \to R$ extends uniquely to a derivation: we can choose a free basis $u_1, \ldots, u_n$ for G, take the x_i to be the values of the map on the u_i, and then the differential on $\mathcal{K}_\bullet(x_1, \ldots, x_n; R)$ gives the extension we want. Uniqueness follows because the derivation property forces $(***)$ to hold, and hence forces $(*)$ to hold, thereby determining the values of the derivation on an R-free basis.

Thus, instead of thinking of the Koszul complex $\mathcal{K}(x_1, \ldots, x_n; R)$ as arising from a sequence of elements $x_1, \ldots, x_n$ of R, we may think of it as arising from an R-linear map of a free module $\theta : G \to R$ (we might have written d_1 for θ), and we write $\mathcal{K}_\bullet(\theta; R)$ for the

corresponding Koszul complex. The sequence of elements is hidden, but can be recovered by choosing a free basis for G, say $u_1, \ldots, u_n$, and taking $x_i = \theta(u_i)$, $1 \leq i \leq n$. The exterior algebra point of view makes it clear that the Koszul complex does not depend on the choice of the sequence of elements: only on the map of the free module $G \to R$. Different choices of basis produce Koszul complexes that look different from the "sequence of elements" point of view, but are obviously isomorphic.

For example, if the sequence of elements is $x_1, \ldots, x_n$ and we compose the map $R^n \to R$ these elements give with the automorphism of $R^n \to R^n$ with matrix A, where A is an invertible $n \times n$ matrix (this is equivalent to taking a new free basis for R^n), we get the Koszul complex of a new sequence of elements $y_1, \ldots, y_n$, the elements of the row $Y = XA$ where $X = \begin{pmatrix} x_1 & \ldots & x_n \end{pmatrix}$ and $Y = \begin{pmatrix} y_1 & \ldots & y_n \end{pmatrix}$. Since this amounts to using the same map $R^n \to R$ with a new free basis for R^n, the Koszul complex we get from Y is isomorphic to that we get from X, and its homology is the same.

Another, nearly equivalent, point of view is that the isomorphism $A : R^n \to R^n$ extends to an isomorphism $\mathcal{K}_\bullet(y_1, \ldots, y_n; R) \cong \mathcal{K}_\bullet(x_1, \ldots, x_n; R)$: in degree i, we have the map $\bigwedge^i(A) : \bigwedge^i(R^n) \cong \bigwedge^i(R^n)$. The commutativity of the squares is easily checked. Notice that for $i = 0$, 1 we have the diagram:

$$\begin{array}{ccccc} R^n & \xrightarrow{Y} & R & \longrightarrow & 0 \\ {\scriptstyle A}\downarrow & & \downarrow{\scriptstyle \mathrm{id}} & & \downarrow \\ R^n & \xrightarrow[X]{} & R & \longrightarrow & 0 \end{array}$$

In particular, permuting the x_i, multiplying them by units, and adding a multiple of one of the x_i to another are operations that do not change the Koszul complex nor Koszul homology, up to isomorphism. In the local case, any two sets of generators of an ideal such that the two sets have the same cardinality are equivalent via the action of an invertible matrix.

To see this, note that if the set of generators is not minimal we can pick a subset that is minimal and subtract sums of multiples of these from the redundant generators to make them 0. Therefore it suffices to consider the case of two minimal sets of generators $x_1, \ldots, x_n$ and $y_1, \ldots, y_n$. We can choose an $n \times n$ matrices A, B over the local ring (R, m, K) such that $Y = XA$ (since the x_i generate) and such that $X = YB$ (since the y_i generate). Then $X = XAB$, so that $X(I - AB) = 0$. Every column of $I - AB$ is a relation on the x_j, and since these are minimal generators the coefficients in any relation are in m. Thus, $I - AB$ has all entries in m, and working mod m, $I - AB \equiv 0$, so that A is invertible modulo m. This implies that its determinant of A is nonzero mod m, and so is a unit of R. But then A is invertible over R. $\square$

The exterior algebra point of view enables us to define the Koszul complex of a map $\theta : P \to R$, where P is a finitely generated projective module that is locally free of constant rank n. Note that P is a homomorphic image of a finitely generated free module

G, and the map $G \twoheadrightarrow P$ will split, so that P is finitely presented. Recall that projective is equivalent to locally free for finitely presented modules: see the Theorem on the first page of the Math 614 Lecture Notes of November 7. The exterior powers $\bigwedge^i(P)$ of P are likewise projective and locally free of constant rank $\binom{n}{i}$, $0 \leq i \leq n$, since the formation of exterior powers commutes with localization. They are also finitely generated and therefore finitely presented. We need to define a map $\bigwedge^i(P) \to \bigwedge^{i-1}(P)$ for every i, and this map is an element of $\mathrm{Hom}_R(\bigwedge^i(P), \bigwedge^{i-1}(P))$. Note that $\mathrm{Hom}(\bigwedge^i(P), \_)$ commutes with localization here, because $\bigwedge^i(P)$ is finitely presented. We have a unique way of defining these maps if we localize so that P becomes free (this can be achieved on a Zariski open neighborhood of every point: this is the content of problem **5.(a)** in Problem Set #3, and this construction commutes with further localization. Therefore, unique maps exist globally that give a differential for $\mathcal{K}_\bullet(\theta; R)$, by the Theorem on the first page of the Math 614 Lecture Notes of November 26. We note that if $f : P \to P$ is an endomorphism of a finitely generated projective module P, we can use the same idea to define a trace and determinant for f, which will agree with the usual ones coming from a matrix for f once we have localized sufficiently that P becomes free.

We want to develop some further sequences associated with Koszul complexes, and we shall make use of the long exact sequence associated with a *mapping cone*, which we describe next.

Given a map $\phi_\bullet : B_\bullet \to A_\bullet$ of complexes, we can associate with it a double complex with two nonzero rows (thought of as indexed by 1 and 0):

$$\begin{array}{ccccccccc}
\cdots & \longrightarrow & 0 & \longrightarrow & 0 & \longrightarrow & 0 & \longrightarrow & \cdots \\
 & & \downarrow & & \downarrow & & \downarrow & & \\
\cdots & \longrightarrow & B_{n+1} & \longrightarrow & B_n & \longrightarrow & B_{n-1} & \longrightarrow & \cdots \\
 & & {\scriptstyle \phi_{n+1}}\downarrow & & {\scriptstyle \phi_n}\downarrow & & {\scriptstyle \phi_{n-1}}\downarrow & & \\
\cdots & \longrightarrow & A_{n+1} & \longrightarrow & A_n & \longrightarrow & A_{n-1} & \longrightarrow & \cdots \\
 & & \downarrow & & \downarrow & & \downarrow & & \\
\cdots & \longrightarrow & 0 & \longrightarrow & 0 & \longrightarrow & 0 & \longrightarrow & \cdots
\end{array}$$

The total complex is called the *mapping cone* of $\phi_\bullet$. The bottom row $A_\bullet$ is a subcomplex. The quotient complex is the top row $B_\bullet$ with degrees shifted down by one. Thus, if $C_\bullet$ is the mapping cone we have the short exact sequence

$$0 \to A_\bullet \to C_\bullet \to B_{\bullet_{-1}} \to 0$$

and so we get

$$\cdots \to H_n(A_\bullet) \to H_n(C_\bullet) \to H_{n-1}(B_\bullet) \to H_{n-1}(A_\bullet) \to \cdots .$$

The connecting homomorphism is easily checked to be given, up to sign, by

$$\phi_{n-1_*} : H_{n-1}(B_\bullet) \to H_{n-1}(A_\bullet).$$

To see this, we choose a cycle $z \in B_{n-1}$. We lift this to the element $0 \oplus z \in C_n = A_n \oplus B_{n-1}$ that maps to z, and now take the image of $0 \oplus z$ in $A_{n-1} \oplus B_{n-2}$, which is $\pm\phi_{n-1}(z) \oplus 0$, and pull this back to $\pm\phi_{n-1}(z) \in A_{n-1}$, which gives the required result.

We now apply this to the Koszul complex $\mathcal{K}(\underline{x}; M)$, where $\underline{x} = x_1, \ldots, x_n$. Let $\underline{x}^- = x_1, \ldots, x_{n-1}$. Then

$$\mathcal{K}_\bullet(x_1, \ldots, x_n; M) = \mathcal{T}_\bullet\big(\mathcal{K}_\bullet(\underline{x}^-; R) \otimes \mathcal{K}_\bullet(x_n; R)\big) \otimes M \cong \mathcal{T}_\bullet\big((\mathcal{K}_\bullet(\underline{x}^-; M) \otimes \mathcal{K}_\bullet(x_n; R)\big)$$

which is the mapping cone of the map from $\mathcal{K}_\bullet(\underline{x}^-; M)$ to itself induced by multiplication by x_n on every module. The long exact sequence of the mapping cone gives

$$H_n(\underline{x}^-; M) \xrightarrow{\pm x_n} H_n(\underline{x}^-; M) \to H_n(\underline{x}; M) \to H_{n-1}(\underline{x}^-; M) \xrightarrow{\pm x_n} H_{n-1}(\underline{x}^-; M)$$

which in turn implies:

Theorem. *Let M be any R-module and $x_1, \ldots, x_n$ any sequence of elements of R. Let $\underline{x}$ denote $x_1, \ldots, x_n$ and $\underline{x}^-$ denote $x_1, \ldots, x_{n-1}$. Then for every i there is a short exact sequence:*

$$0 \to H_n(\underline{x}^-; M)/xH_n(\underline{x}^-; M) \to H_n(\underline{x}; M) \to \operatorname{Ann}_{H_{n-1}(\underline{x}^-; M)} x_n \to 0.$$

Proof. This is immediate from the long exact sequence above. □

We next note that if R is $\mathbb{N}$ graded and the x_i are homogeneous, then $\mathcal{K}_\bullet(\underline{x}; R)$ can be $\mathbb{N}$-graded with differentials that preserve degree. Moreover, if M is $\mathbb{Z}$-graded but $[M]_k$ is 0 for $k \ll 0$, then $\mathcal{K}_\bullet(\underline{x}; M)$ is $\mathbb{Z}$-graded with differentials that preserve degree, and all of the modules occurring are 0 in all sufficiently low negative degrees. This property will also pass to all graded quotients of their graded submodules, and, in particular, every $H_i(\underline{x}; M)$ will have the property that all modules it is zero in all sufficiently low negative degrees.

To see this, note that if A, B are $\mathbb{Z}$-graded R-modules that are 0 in low degree, we may grade $A \otimes_R B$ by letting $[A \otimes_R B]_k$ be the span of all $a \otimes b$ such that $a \in A_i$ and $b \in B_j$ for some choice of i and j such that $i + j = k$. This gives a $\mathbb{Z}$-grading that vanishes in low degree: if $A_i = 0$ for $i < c$ and $B_j = 0$ for $j < d$, then $[A \otimes_R B]_k = 0$ for $k < c + d$. Next, note that if x_i has degree d_i, $1 \leq i \leq n$, then $\mathcal{K}_\bullet(x_i; R)$ may be thought of as $0 \to R(-d_i) \xrightarrow{x_i} R \to 0$, and this is graded with degree-preserving differentials. The general Koszul complex is constructed by tensoring these together, and then tensoring with M. Note that $R(-d) \otimes_R R(-e) \cong R(-d-e)$ as graded modules, and that $R(-d) \otimes_R M \cong M(-d)$ as graded modules. It follows that $\mathcal{K}_i(\underline{x}; M)$ is the direct sum of all the modules $M\big(-(d_{j_1} + \cdots + d_{j_i})\big)$ for $1 \leq j_1 < \cdots < j_i \leq n$.

Theorem. *Suppose that the R-module $M \neq 0$, and either that (1) M is $\mathbb{Z}$-graded over the $\mathbb{N}$-graded ring R, with all sufficiently small negative graded pieces of M equal to 0, and that $x_1, \ldots, x_n$ are forms of positive degree, or (2) that (R, m, K) is local, M is finitely*

generated, and that $x_1, \ldots, x_n \in m$. *Let* $I = (x_1, \ldots, x_n)R$. *Then the following conditions are equivalent:*
(1) $H_1(\underline{x};\, M) = 0$.
(2) $H_i(\underline{x};\, M) = 0$ *for all* $i \geq 1$.
(3) *In the case where* R *and* M *are Noetherian,* $\operatorname{depth}_I M = n$.
(4) *The elements* $x_1, \ldots, x_n$ *form a regular sequence on* M.

Proof. The hypothesis implies that $IM \neq M$, by the local or graded form of Nakayama's lemma. We know that (2) and (3) are equivalent in the case where the ring and module are Noetherian. We also know that (4) $\Rightarrow$ (2) $\Rightarrow$ (1). It will therefore suffice to show that (1) $\Rightarrow$ (4). We use induction on n. The case $n = 1$ is obvious, since $H_1(x_1;\, M) = \operatorname{Ann}_M x_1$. Suppose that the result is known for $n - 1$ elements, $n \geq 2$.

Taking $i = 1$ in the preceding Theorem we have a short exact sequence

$$0 \to H_1(\underline{x}^-;\, M)/x_n H_1(\underline{x}^-;\, M) \to H_1(\underline{x};\, M) \to \operatorname{Ann}_{H_0(\underline{x}^-;\, M)} x_n \to 0.$$

Assume that the middle term vanishes. Then all three terms vanish, and so

$$H_1(x_1, \ldots, x_{n-1}; M) = x_n H_1(x_1, \ldots, x_{n-1}; M).$$

By Nakayama's lemma, $H_1(x_1, \ldots, x_{n-1}; M) = 0$, which shows, using the induction hypothesis, that $x_1, \ldots, x_{n-1}$ is a regular sequence on M. The vanishing of the rightmost term shows that x_n is not a zerodivisor on

$$H_0(x_1, \ldots, x_{n-1}; M) \cong M/(x_1, \ldots, x_{n-1})M.$$

Therefore, $x_1, \ldots, x_n$ is a regular sequence on M, as required. $\square$

Math 615: Lecture of February 22, 2012

We note two important consequences of the final Theorem of the Lecture of February 20.

Corollary. *Under the same hypothesis as for the preceding Theorem (i.e., in certain graded and local situations) a regular sequence* $x_1, \ldots, x_n$ *on* M *is permutable. In other words, if the elements form a regular sequence in one order, they form a regular sequence in every order.*

Proof. Permuting $x_1, \ldots, x_n$ can be viewed as the result of an action of an invertible matrix — an appropriate permutation matrix. By the results of the preceding lecture, the Koszul homology is not affected by such a permutation. But $x_1, \ldots, x_n$ is a regular sequence on M if and only if $H_1(x_1, \ldots, x_n;\, M) = 0$, by the Theorem cited. $\square$

This result can also be proved by elementary means. It suffices to show that any two consecutive elements in the regular sequence can be switched: every permutation can be

built up this way. One can work modulo the predecessors of the pair being switched, and so we may assume that the elements are the first two, say x_1, x_2. It is easy to see that it suffices to show that x_2, x_1 is a regular sequence, since $M/(x_1,\, x_2)M = M/(x_2, x_1)M$. The only hard step is to show that x_2 is not a zerodivisor on M. This still requires some form of Nakayama's lemma to hold. The statement that if x_1, x_2 is a regular sequence on M then x_1 is not a zerodivisor on M/x_2M always holds.

Corollary. *Let M be a Noetherian R-module and $\underline{x} = x_1, \ldots, x_n \in R$. If $H_i(\underline{x};\, M) = 0$ for some i then $H_j(\underline{x};\, M) = 0$ for all $j \geq i$.*

Proof. We may replace R by $R/\mathrm{Ann}_R M$ without affecting the Koszul complex or its homology. Therefore, we may assume that R is Noetherian. Let $X_1, \ldots, X_n$ be indeterminates over R, and extend the action of R on M to $S = R[X_1, \ldots, X_n]$ by letting X_i act the way x_i does. This is equivalent to taking the R-algebra map $S \to R$ that fixes $R \subseteq S$ and sends X_i to x_i for $1 \leq i \leq n$, and restricting scalars from R to S. Then M is a finitely generated R-module over the Noetherian ring S, and $\mathcal{K}_\bullet(X_1, \ldots, X_n;\, M) \cong \mathcal{K}_\bullet(\underline{x};\, M)$. The X_i form a regular sequence in S. Replacing R by S and $x_1, \ldots, x_n$ by $X_1, \ldots, X_n$, we see that we may assume without loss of generality that $x_1, \ldots, x_n$ is a regular sequence in R. If $H_j(\underline{x};\, M) \neq 0$ we may choose a prime ideal P of the ring R such that $H_j(\underline{x};\, M)_P \neq 0$. We may replace R by R_P and M by M_P, since $H_t(x_1/1, \ldots, x_n/1;\, M_P) \cong H_t(\underline{x};\, M)_P$ for all P. Thus, we may assume that $(R,\, m)$ is local. We may also assume that $x_1, \ldots, x_n \in m$: if not, $(x_1, \ldots, x_n)R = R$ kills all the Koszul homology, and all of it vanishes.

If $i = 1$ we are done by the final Theorem of the Lecture of February 20: the vanishing of $H_1(\underline{x};\, M)$ implies that $x_1, \ldots, x_n$ is a regular sequence on M, and that all the higher Koszul homology vanishes. We can now complete the proof by induction on i. Assume that $i > 1$ and the result is known for smaller integers. Form an exact sequence

$$0 \to M' \to R^h \to M \to 0$$

by mapping a finitely generated free module onto M. Since $x_1, \ldots, x_n$ is a regular sequence on R, it is a regular sequence on R^h, and $H_t(\underline{x};\, R^h) = 0$ for all $t \geq 1$. The long exact sequence for Koszul homology then implies at once that $H_t(\underline{x};\, M) \cong H_{t-1}(\underline{x};\, M')$ for all $t > 1$, and so $H_{i-1}(\underline{x};\, M') = 0$ while $H_{j-1}(\underline{x};\, M') \neq 0$ with $j - 1 \geq i - 1$, contradicting the induction hypothesis. $\square$

We shall eventually use this result to prove that if M, N are finitely generated modules over a regular ring R and $\mathrm{Tor}_i^R(M,\, N) = 0$, then $\mathrm{Tor}_j^R(M,\, N) = 0$ for all $j \geq i$. This was proved by M. Auslander in the equicharacteristic case and by S. Lichtenbaum in general. In the equicharacteristic case, after localization and completion the values of Tor can be interpreted as Koszul homology over an auxiliary ring. This is not true in the mixed characteristic case, where one also needs spectral sequence arguments to make a comparison with the case where one can interpret values of Tor as Koszul homology. Both arguments make use of the structure of complete regular rings.

We shall soon begin our study of spectral sequences, but before doing that we introduce Grothendieck groups and use them to prove that regular local rings are unique factorization domains, following M. P. Murthy.

Let R be a Noetherian ring. Let $\mathcal{M}$ denote the set of modules

$$\{R^n/M : n \in \mathbb{N},\, M \subseteq R^n\}.$$

Every finitely generated R-module is isomorphic to one in $\mathcal{M}$, which is all that we really need about $\mathcal{S}$: we can also start with some other set of modules with this property without affecting the Grothendieck group, but we use this one for definiteness.

Consider the free abelian group with basis $\mathcal{M}$, and kill the subgroup generated by all elements of the form $M - M' - M''$ where

$$0 \to M' \to M \to M'' \to 0$$

is a short exact sequence of elements of $\mathcal{M}$. The quotient group is called the *Grothendieck group* $G_0(R)$ of R. It is an abelian group generated by the elements $[M]$, where $[M]$ denotes the image of $M \in \mathcal{M}$ in $G_0(R)$. Note that if $M' \cong M$ we have a short exact sequence

$$0 \to M' \to M \to 0 \to 0,$$

so that $[M] = [M'] + [0] = [M']$, i.e., isomorphic modules represent the same class in $G_0(R)$.

A map L from $\mathcal{M}$ to an abelian group $(A, +)$ is called *additive* if whenever

$$0 \to M' \to M \to M'' \to 0$$

is exact, then $L(M) = L(M') + L(M'')$. The map γ sending M to $[M] \in G_0(R)$ is additive, and is a universal additive map in the following sense: given any additive map $L : \mathcal{M} \to A$, there is a unique homomorphism $h : G_0(M) \to A$ such that $L = h \circ \gamma$. Since we need $L(M) = h([M])$, if there is such a map it must be induced by the map from the free abelian group with basis $\mathcal{M}$ to A that sends M to $h(M)$. Since h is additive, the elements $M - M' - M''$ coming from short exact sequences

$$0 \to M' \to M \to M'' \to 0$$

are killed, and so there is an induced map $h : G_0(R) \to A$. This is obviously the only possible choice for h.

Over a field K, every finitely generated module is isomorphic with $K^{\oplus n}$ for some $n \in \mathbb{N}$. It follows that $G_0(K)$ is generated by $[K]$, and in fact it is $\mathbb{Z}[K]$, the free abelian group on one generator. The additive map associated with the Grothendieck group sends M to $\dim_K(M)[K]$. If we identify $\mathbb{Z}[K]$ with $\mathbb{Z}$ by sending $[K]$ to 1, this is the dimension map.

If R is a domain with fraction field $\mathcal{F}$, we have an additive map to $\mathbb{Z}$ that sends M to $\dim_{\mathcal{F}} \mathcal{F} \otimes_R M$, which is called the *torsion-free rank* of M. This induces a surjective map $G_0(R) \to \mathbb{Z}$. If R is a domain and $[R]$ generates $G_0(R)$, then $G_0(R) \cong \mathbb{Z}[R] \cong \mathbb{Z}$, with the isomorphism given by the torsion-free rank map.

Notice that if L is additive and

$$0 \to M_n \to \cdots \to M_1 \to M_0 \to 0$$

is exact, then

$$L(M_0) - L(M_1) + \cdots + (-1)^n L(M_n) = 0.$$

If $n \leq 2$, this follows from the definition. We use induction. In the general case note that we have a short exact sequence

$$0 \to N \to M_1 \to M_0 \to 0$$

and an exact sequence

$$0 \to M_n \to \cdots \to M_3 \to M_2 \to N \to 0,$$

since

$$\text{Coker}\,(M_3 \to M_2) \cong \text{Ker}\,(M_1 \to M_0) = N.$$

Then

$$(*) \quad L(M_0) - L(M_1) + L(N) = 0,$$

and

$$(**) \quad L(N) - L(M_2) + \cdots + (-1)^{n-1} L(M_n) = 0$$

by the induction hypothesis. Subtracting $(**)$ from $(*)$ yields the result. $\square$

From these comments and our earlier results on regular local rings we get at once:

Theorem. *If R is a regular local ring, $G_0(R) = \mathbb{Z}[R] \cong \mathbb{Z}$.*

Proof. R is a domain, and we have the map given by torsion-free rank. It will suffice to show that $[R]$ generates $G_0(R)$. But if M is any finitely generated R-module, we know that M has a finite free resolution

$$0 \to R^{b_k} \to \cdots \to R^{b_1} \to R^{b_0} \to M \to 0,$$

and so the element $[M]$ may be expressed as

$$[R^{b_0}] - [R^{b_1}] + \cdots + (-1)^k [R^{b_k}] = b_0[R] - b_1[R] + \cdots + (-1)^k b_k[R] = (b_0 - b_1 + \cdots + (-1)^k b_k)[R]$$

$\square$

Math 615: Lecture of February 24, 2012

Note that given a finite filtration

$$0 = M_0 \subseteq M_1 \subseteq \cdots \subseteq M_{n-1} \subseteq M_n = M$$

of a finitely generated R-module M and an additive map L we have that

$$L(M) = L(M_n/M_{n-1}) + L(M_{n-1}),$$

and, by induction on n, that

$$L(M) = \sum_{j=1}^{n} L(M_j/M_{j-1}).$$

In particular, $[M] \in G_0(R)$ is

$$\sum_{j=1}^{n} [M_j/M_{j-1}].$$

Theorem. *Let R be a Noetherian ring. $G_0(R)$ is generated by the elements $[R/P]$, as P runs through all prime ideals of R. If P is prime and $x \in R - P$, then $[R/(P + xR)] = 0$, and so if $R/Q_1, \ldots, R/Q_k$ are all the factors in a prime filtration of $[R/(P + xR)]$, we have that $[R/Q_1] + \cdots + [R/Q_k] = 0$. The relations of this type are sufficient to generate all relations on the classes of the prime cyclic modules.*

Proof. The first statement follows from the fact that every finitely generated module over a Noetherian ring R has a finite filtration in which the factors are prime cyclic modules. The fact that $[R/(P + xR)] = 0$ follows from the short exact sequence

$$0 \to R/P \xrightarrow{x} R/P \to R/(P + xR) \to 0,$$

which implies $[R/P] = [R/P] + [R/(P + xR)]$ and so $[R/(P + xR)] = 0$ follows.

Now, for every $M \in \mathcal{M}$, fix a prime cyclic filtration of M. We need to see that if we have a short exact sequence

$$0 \to M' \to M \to M'' \to 0$$

that the relation $[M] = [M'] + [M'']$ is deducible from ones of the specified type. We know that M' will be equal to the sum of the classes of the prime cyclic module coming from its chosen prime filtration, and so will M''. These two prime cyclic filtrations together induce a prime cyclic filtration $\mathcal{F}$ of M, so that the information $[M] = [M'] + [M'']$ is conveyed by setting $[M]$ equal to the sum of the classes of the prime cyclic modules in these specified filtrations of $[M]$ and $[M']$. But $\mathcal{F}$ will not typically by the specified filtration of $[M]$, and so we need to set the sum of the prime cyclic modules in the specified filtration of M equal to the sum of all those occurring in the specified filtrations of M' and M''.

Thus, we get all relations needed to span if for all finitely generated modules M and for all pairs of possibly distinct prime cyclic filtrations of M, we set the sum of the classes of the prime cyclic modules coming from one filtration equal to the corresponding sum for the other. But any two filtrations have a common refinement. Take a common refinement, and refine it further until it is a prime cyclic filtration again. Thus, we get all relations

needed to span if for every finitely generated module M and for every pair consisting of a prime cyclic filtration of M and a refinement of it, we set the sum of the classes coming from one filtration to the sum of those in the other. Any two prime cyclic filtrations may then be compared by comaring each two a prime cyclic filtration that refines them both.

In refining a given prime cyclic filtration, each factor R/P is refined. Therefore, we get all relations needed to span if for every R/P and every prime cyclic filtration of R/P, we set $[R/P]$ equal to the sum of the classes in the prime cyclic filtration of R/P. Since $\mathrm{Ass}\,(R/P) = P$, the first submodule of a prime cyclic filtration of R/P will be isomorphic with R/P, and will therefore have the form $x(R/P)$, where $x \in R - P$. If the other factors are $R/Q_1, \ldots, R/Q_k$, then these are the factors of a filtration of $(R/P)/x(R/P) = R/(P + xR)$. Since $[x(R/P)] = [R/P]$, the relation we get is

$$[R/P] = [R/P] + [R/Q_1] + \cdots + [R/Q_k],$$

which is equivalent to

$$[R/Q_1] + \cdots + [R/Q_k] = 0,$$

and so the specified relations suffice to span all relations. □

Corollary. $G_0(R) \cong G_0(R_{\mathrm{red}})$.

Proof. The primes of R_{red} and those of R are in bijective correspondence, and the generators and relations on them given by the preceding Proposition are the same. □

Proposition. *If R and S are Noetherian rings, then $G_0(R \times S) \cong G_0(R) \times G_0(S)$.*

Proof. If M is an $(R \times S)$-module, then with $e = (1, 0)$ and $f = (0, 1)$ we have an isomorphism $M \cong eM \times fM$, where eM is an R-module via $r(em) = (re)(em)$ and fM is an S-module via $s(fm) = (sf)(fm)$. There is an isomorphism $M \cong eM \times fM$. Conversely, given an R-module A and an S-module B, these determine an $R \times S$-module $M = A \times B$, where $(r, s)(a, b) = (ra, sb)$ such that $eM \cong A$ over R and $fM \cong B$ over R. Thus, $(R \times S)$-modules correspond to pairs A, B where A is an R-module and B is an S-module. Moreover, if $h : M \to M'$ then h induces maps $eM \to eM'$ and $fM \to fM'$ that determine h. Said differently, a map from $A \times B \to A' \times B'$ as $(R \times S)$-modules corresponds to a pair of maps $A \to A'$ as R-modules and $B \to B'$ as S-modules. Consequently, a short exact sequence of $(R \times S)$-modules corresponds to a pair consisting of short exact sequences, one of R-modules and the other of S-modules. The stated isomorphism of Grothendieck groups follows at once. □

Proposition. *Let R be an Artin ring.*

(a) *If (R, m, K) is Artin local, $G_0(R) \cong \mathbb{Z} \cdot [K] \cong \mathbb{Z}$, where the additive map $M \mapsto \ell_R(M)$ gives the isomorphism with $\mathbb{Z}$.*

(b) *If R has maximal ideals $m_1, \ldots, m_k$, then $G_0(R)$ is the free abelian group on the $[R/m_j]$.*

Proof. For part (b), notice that the R/m_k are generators by Theorem, and there are no non-trivial relations, since if $x \notin m_j$, $R/(m_j + xR) = 0$. Part (a) follows easily from part (b). We may also deduce part (b) from part (a), using the fact that an Artin ring is a finite product of Artin local rings and the preceding Proposition. □

Proposition. *Let R and S be Noetherian rings.*

(a) *If $R \to S$ is a flat homomorphism, there is a a group homomorphism $G_0(R) \to G_0(S)$ sending $[M]_R \mapsto [S \otimes_R M]_S$. Thus, G_0 is a covariant functor from the category of rings and flat homomorphisms to abelian groups.*

(b) *If $S = W^{-1}R$ is a localization, the map described in (a) is surjective.*

(c) *If P is a minimal prime of R, there is a homomorphism $G_0(R) \to \mathbb{Z}$ given by $[M] \mapsto \ell_{R_P}(M_P)$. Of course, if R is a domain and $P = (0)$, this is the torsion-free rank map.*

(d) *If R is a domain, the map $\mathbb{Z} \to G_0(R)$ that sends 1 to $[R]$ is split by the torsion-free rank map. Thus, $G_0(R) = \mathbb{Z}[R] + \overline{G}_0(R)$, where $\overline{G}_0(R) = G_0(R)/\mathbb{Z} \cdot [R]$, the reduced Grothendieck group of R. When R is a domain, the reduced Grothendieck group may be thought of as the subgroup of $G_0(R)$ spanned by the classes of the torsion R-modules.*

(e) *If S is module-finite over R, there is a group homomorphism $G_0(S) \to G_0(R)$ sending $[M]_S$ to $[{}_RM]_R$, where ${}_RM$ denotes M viewed as an R-module via restriction of scalars. In particular, this holds when S is homomorphic image of I. Thus, G_0 is a contravariant functor from the category of rings and module-finite homomorphisms to abelian groups.*

Proof. (a) is immediate from the fact that $S \otimes_R \_$ preserves exactness.

To prove (b), note that if M is a finitely generated module over $W^{-1}R$, it can be written as the cokernel of a matrix of the form (r_{ij}/w_{ij}), where every $r_{ij} \in R$ and every $w_{ij} \in W$. Let w be the product of all the w_{ij}. Then the entries of the matrix all have the form r'_{ij}/w. If we multiply every entry of the matrix by w, which is a unit in S, the cokernel is unaffected: each column of the matrix is multiplied by a unit. Let $M_0 = \text{Coker } (r'_{ij})$. Then $S \otimes_R M_0 \cong M$. This shows the surjectivity of the map of Grothendieck groups.

Part (c) is immediate from the fact that localization is exact coupled with the fact the length is additive. The statement in (d) is obvious, since the torsion-free rank of R is 1.

One has the map in (e) because restriction of scalars is an exact functor from finitely generated S-modules to finitely generated R-modules. One needs that S is module-finite over R to guarantee that when one restricts scalars, a finitely generated S-module becomes a finitely generated R-module. $\square$

If S is faithfully flat or even free over R, the induced map $[M]_R \to [S \otimes_R M]_S$ need not be injective, not even if $S = L \otimes_K R$ where L is a finite field extension of $K \subseteq R$: an example is given in the sequel (see the last paragraph of today's Lecture Notes).

An R-module M is said to have *finite Tor dimension* or *finite flat dimension* over R at most d if $\text{Tor}_i^R(M,\, N) = 0$ for all $i > d$. If $M = 0$, the Tor dimension is defined to be -1. Otherwise, it is the smallest integer d such that $\text{Tor}_i^R(M,\, N) = 0$ for all $i > d$, if such an integer exists, and $+\infty$ otherwise. We leave it as an exercise to show that M has finite Tor dimension at most d if and only if some (equivalently, every) d th module of syzygies of M is flat. Likewise, M has finite Tor dimension at most d if and only if M has a left resolution by flat modules of length at most d. A nonzero module M has Tor dimension 0 if and only of M is flat over R. Of course, if M has finite projective dimension d, then M has Tor dimension at most d.

Proposition. *If S is a Noetherian R-algebra of finite Tor dimension $\leq d$ over the Noetherian ring R, there is a map $G_0(R) \to G_0(S)$ that sends $[M]_R$ to*

$$\theta(M) = \sum_{i=0}^{d} (-1)^i [\mathrm{Tor}_i^R(S,\, M)]_S.$$

Proof. We simply need to check the additivity of the map. Let $0 \to M' \to M \to M'' \to 0$ be a short exact sequence of finitely generated R-modules. Then we get a long exact sequence of finitely generated S-modules

$$\begin{aligned} 0 \to \mathrm{Tor}_d^R(S,\, M') \to \mathrm{Tor}_d^R(S,\, M) \to \mathrm{Tor}_d^R(S,\, M'') \to \cdots \\ \to \mathrm{Tor}_0^R(S,\, M') \to \mathrm{Tor}_0^R(S,\, M) \to \mathrm{Tor}_0^R(S,\, M'') \to 0 \end{aligned}$$

and so the alternating sum Σ of the classes of these modules in $G_0(S)$ is 0. We think of these $3d$ modules as in positions $3d-1$, $3d-2$, $\cdots$, 2, 1, 0 counting from the left. The terms involving M'' are in positions numbered 0, , 3, 6, $\ldots$, $3(d-1)$. Their signs alternate starting with $+$, and so their contribution to Σ is $\theta(M'')$. The terms involving M are in positions numbered 1, 4, 7, $\ldots$, $3(d-1)+1$. Their signs alternate starting with $-$, and so their contribution to Σ is $-\theta(M)$. Finally, the terms involving M' are in positions numbered 2, 5, 8, $\ldots$, $3(d-1)+2$. Their signs alternate starting with $+$, and so their contribution to Σ is $\theta(M')$. This yields $0 = \Sigma = \theta(M') - \theta(M) + \theta(M'')$, as required. $\square$

Corollary. *If x is not a zerodivisor in the Noetherian ring R, there is a map $G_0(R) \to G_0(R/xR)$ that sends $[M]_R \mapsto [M/xR]_{R/xR} - [\mathrm{Ann}_M\, x]_{R/xR}$.*

Proof. This is the special case of result just above when $S = R/xR$, which has projective dimension at most 1 and, hence, flat dimension at most 1. We have that $\mathrm{Tor}_0^R(R/xR,\, M) \cong (R/xR) \otimes_R M \cong M/xM$, and $\mathrm{Tor}_1^R(R/xR,\, M) \cong \mathrm{Ann}_M x$. An elementary proof of this result may be given by showing that when

$$0 \to M' \to M \to M'' \to 0$$

is exact then so is

$$0 \to \mathrm{Ann}_{M'}\, x \to \mathrm{Ann}_M\, x \to \mathrm{Ann}_{M''}\, x \to M'/xM' \to M/xM \to M''/xM'' \to 0,$$

developing this special case of the long exact sequence for Tor from first principles. $\square$

Corollary. *Let R be Noetherian and let S denote either $R[x]$ or $R[[x]]$, where x is an indeterminate. Since S is flat over R, we have an induced map $G_0(R) \to G_0(S)$. This map is injective.*

Proof. We have that $S/xS \cong R$, where x is not a zerodivisor in S, and so we have a map $G_0(S) \to G_0(R)$. Under the composite map, the class $[M]_R$ of an R-module M maps first to $[M[x]\,]_S$ (respectively, $[M[[x]]\,]_S$), and then to $[M[x]/xM[x]\,]_R$ (respectively, $[M[[x]]/xM[[x]]\,]_R$), since x is not a zerodivisor on $M[x]$ (respectively, $M[[x]]$). In both cases, the quotient is $\cong M$, and so the composite map takes $[M]_R \to [M]_R$. Thus, the composite $G_0(R) \to G_0(S) \to G_0(R)$ is the identity on $G_0(R)$, which implies that $G_0(R) \to G_0(S)$ is injective. $\square$

We next aim to establish the following result, which will imply unique factorization in regular local rings.

Theorem (M. P. Murthy). *Let R be a normal domain and let H be the subgroup of $\overline{G}_0(R)$ spanned by the classes $[R/P]$ for P a prime of height 2 or more. Then*

$$\mathcal{C}\ell\,(R) \cong \overline{G}_0(R)/H.$$

Assuming this for the moment, note the failure of the injectivity of the map from $G_0(R) \to G_0(S)$ where $R = \mathbb{R}[x,\, y]/(x^2+y^2-1)$ and $S = \mathbb{C} \otimes_{\mathbb{R}} R \cong \mathbb{C}[x,\, y]/(x^2+y^2-1)$. We have seen in **6.(b)** of Problem Set #6 from Math 614 that the maximal ideal $P = (x,\, y-1)R$ is not principal in R, from which it will follow that $[P]$ is nonzero in $\mathcal{C}\ell\,(R)$, and so that $[R/P]$ is nonzero in $\overline{G}_0(R)$, and therefore $[R/P]$ is not zero in $G_0(R)$. But P becomes principal when expanded to S. In fact, S is a UFD, for if we let $u = x + yi$ and $v = x - yi$, then $\mathbb{C}[x,\, y] \cong \mathbb{C}[u,\, v]$ (we have made a linear change of variables), and so $S \cong \mathbb{C}[u,\, v]/(uv-1) \cong \mathbb{C}[u][1/u]$. Thus, $[S \otimes R/P]_S = [S/PS]_S = 0$ in $G_0(S)$.

Math 615: Lecture of March 5, 2012

Recall that if R is a normal domain, one defines the *divisor class group* of R, denoted $\mathcal{C}\ell\,(R)$, as follows. First form the the free abelian group on generators in bijective correspondence with the height one prime ideals of R. The elements of this group are called *divisors*. The divisor $\mathrm{div}\,(I)$ of an ideal $I \neq 0$ whose primary decomposition only involves height one primes (I is said to be of *pure height one*) is then obtained from the primary decomposition of I: if the primary decomposition of I is $P_1^{(k_1)} \cap \cdots \cap P_s^{(k_s)}$ where the P_j are mutually distinct, then $\mathrm{div}\,(I) = \sum_{j=1}^{s} k_j P_j$. We regard the unit ideal as having pure height one in a vacuous sense, and define its divisor to be 0. The divisor $\mathrm{div}\,(r)$ of an element $r \in R - \{0\}$ is the divisor of rR, and, hence, 0 if r is a unit. Then $\mathcal{C}\ell\,(R)$ is the quotient of the free abelian group of divisors by the span of the divisors of nonzero principal ideals. The following is part of a Theorem on the third page of the Math 614 Lecture Notes from December 1, to which we refer the reader for the proof.

Theorem. *Let R be a Noetherian normal domain. If I has pure height one, then so does fI for every nonzero element f of R, and* $\mathrm{div}\,(fI) = \mathrm{div}\,(f) + \mathrm{div}\,(I)$. *For any two ideals I and J of pure height one,* $\mathrm{div}\,(I) = \mathrm{div}\,(J)$ *iff $I = J$, while the images of* $\mathrm{div}\,(I)$ *and* $\mathrm{div}\,(J)$ *in $\mathcal{C}\ell\,(R)$ are the same iff there are nonzero elements f, g of R such that $fI = gJ$. This holds iff I and J are isomorphic as R-modules. In particular, I is principal if and only if* $\mathrm{div}\,(I)$ *is 0 in the divisor class group. Hence, R is a UFD if and only if $\mathcal{C}\ell\,(R) = 0$.*

While we are not giving a full proof here, we comment on one point. If $I \cong J$ as an R-module, the isomorphism is given by an element of $\mathrm{Hom}_R(I,\, J)$. If we localize at the prime (0), which is the same as applying $\mathcal{F} \otimes_R \_$, where $\mathcal{F}$ is the fraction field of R, we see that $\mathrm{Hom}_R(I,\, J)$ embeds in $\mathcal{F} \otimes_R \mathrm{Hom}_R(I,\, J) \cong \mathrm{Hom}_{\mathcal{F}}(I\mathcal{F},\, J\mathcal{F}) = \mathrm{Hom}\mathcal{F}(\mathcal{F},\, \mathcal{F}) \cong \mathcal{F}$, that is, every homomorphism from I to J is induced by multiplying by a suitable fraction f/g, $f \in R$, $g \in R - \{0\}$. When this fraction gives an isomorphism we have $(f/g)I = J$ or $fI = gJ$.

Theorem (M. P. Murthy). *Let R be a normal domain and let H be the subgroup of $\overline{G}_0(R)$ spanned by the classes $[R/P]$ for P prime of height 2 or more. Then $\mathcal{C}\ell\,(R) \cong \overline{G}_0(R)/H$ with the map sending $[P] \mapsto [R/P]$ for all height one primes P.*

Before proving this, we note two corollaries. One is that regular local rings have unique factorization. Whether this is true was an open question for many years that was first settled by M. Auslander and D. Buchsbaum by a much more difficult method, utilizing homological methods but based as well on a result of Zariski that showed it suffices to prove the result for regular local rings of dimension 3. Later, I. Kaplansky gave a substantially simpler proof. But I feel that Murthy's argument gives the "right" proof. We have already seen that for a regular local ring R, $\overline{G}_0(R) = 0$. Therefore:

Corollary. *A regular local ring is a UFD.* $\square$

Corollary. *If R is a Dedekind domain, then $\overline{G}_0(R) \cong \mathcal{C}\ell\,(R)$ and $G_0(R) = \mathbb{Z}\cdot[R] \oplus \mathcal{C}\ell\,(R)$.*

Proof. This is clear, since there are no primes of height two or more. $\square$

We now go back and prove Murthy's result.

Proof of the Theorem. We know that $G_0(R)$ is the free group on the classes of the R/P, P prime, modulo relations obtained from prime cyclic filtrations of $R/(P + xR)$, $x \notin P$. We shall show that if we kill $[R]$ and all the $[R/Q]$ for Q of height 2 or more, all relations are also killed except those coming from $P = (0)$, and the image of any relation corresponding to a prime cyclic filtration of R/xR corresponds precisely to $\operatorname{div}(x)$. Clearly, if $P \neq 0$ and $x \notin P$, any prime containing $P + xR$ strictly contains P and so has height two or more. Thus, we need only consider relations on the R/P for P of height one coming from prime cyclic filtrations of R/xR, $x \neq 0$. Clearly, R does not occur, since R/xR is a torsion module, and occurrences of R/Q for Q of height ≥ 2 do not matter. We need only show that for every prime P of height one, the number of occurrences of R/P in any prime cyclic filtration of R/xR is exactly k, where $P^{(k)}$ is the P-primary component of xR. But we can do this calculation after localizing at P: note that all factors corresponding to other primes become 0, since some element in the other prime not in P is inverted. Then $xR_P = P^k R_p$, and we need to show that any prime cyclic filtration of R_P/xR_P has k copies of R_P/PR_P, where we know that $xR_P = P^k R_P$. Notice that $(R_P,\, PR_P)$ is a DVR, say (V, tV), and $xR_P = t^k V$. The number of nonzero factors in any prime cyclic filtration of $V/t^k V$ is the length of $V/t^k V$ over V, which is k, as required: the only prime cyclic filtration without repetitions is

$$0 \subset t^{k-1}V \subset t^{k-2}V \subset \cdots \subset t^2 V \subset tV \subset V. \quad \square$$

Theorem. *$G_0(R) \cong G_0(R[x])$ under the map that sends $[M] \mapsto [M[x]\,]$, where we have written $M[x]$ for $R[x] \otimes_R M$.*

Proof. We have already seen that the map is injective, and even constructed a left inverse for it, which takes

$$[N]_{R[x]} \mapsto [N/xN]_R - [\operatorname{Ann}_N x]_R.$$

However, we shall not make use of this left inverse to prove surjectivity. Instead, we prove that every $[S/Q]$, Q prime, is in the image of $G_0(R) \to G_0(R[x])$ by Noetherian induction

on $R/(Q \cap R)$. There are two sorts of primes lying over $P \in \operatorname{Spec}(R)$. One is $PR[x]$. The other is generated, after localization at $R - P$, by a polynomial $f \in R[x]$ of positive degree with leading coefficient in $R - P$ such that the image of f is irreducible in $\kappa_P[x]$, where $\kappa_P = R_P/PR_P \cong \operatorname{frac}(R/P)$. To see this, note that every prime Q lying over P corresponds, via contraction to $R[x]$, to a prime of the fiber $(R-P)^{-1}(R/P)[x] \cong \kappa_P[x]$. The primes in $\kappa_P[x]$ are of two types: there is the (0) ideal, whose contraction to $R[x]$ is $PR[x]$, and there are the maximal ideals, each of which is generated by an irreducible polynomial of positive degree in $\kappa_P[x]$. We can clear the denominators by multiplying by an element of $R-P$, and then lift the nonzero coefficients to $R-P$, to obtain a polynomial f with leading coefficient in $R - P$ as described previously. Note that Q is recovered from P and f as the set of all elements of $R[x]$ multiplied into $P+fR[x]$ by an element of $R-P$. Briefly, $Q = (PR[x] + fR[x]) :_{R[x]} (R - P)$.

Since $R[x]/PR[x] = (R/P) \otimes_R R[x]$ is evidently in the image, we need only show that the primes Q of the form $(PR[x]+fR[x]) :_{R[x]} (R-P)$ are in the image of $G_0(R) \to G_0(R[x])$. We have exact sequences

$$(*) \quad 0 \to (R/P)[x] \xrightarrow{f} (R/P)[x] \to M \to 0,$$

where $M = R[x]/(PR[x] + fR[x])$, and

$$(**) \quad N \to M \to R[x]/Q \to 0.$$

Because $(R-P)^{-1}M = (R-P)^{-1}R[x]/Q$, we have that N is a finitely generated module that is a torsion module over R/P. Since every generator of N is killed by an element of $R - P$, we can choose $a \in R - P$ that kills N. From $(*)$, $[M] = 0$ in $G_0(S)$. From $(**)$, $[R[x]/Q] = -[N]$ in $G_0(R[x])$. Therefore, it suffices to show that $[N]$ is in the image. In a prime cyclic filtration of N, every factor is killed by $P + aR$, and therefore for every $R[x]/Q'$ that occurs, Q' lies over a prime strictly containing P. But then every $[R[x]/Q']$ is in the image by the hypothesis of Noetherian induction. $\square$

Theorem. *Let R be a ring and S a multiplicative system. Then the kernel of $G_0(R) \to G_0(S^{-1}R)$ is spanned by the set of classes $\{[R/P] : P \cap S \neq \emptyset\}$. Hence, for any $x \in R$ there is an exact sequence*

$$G_0(R/xR) \to G_0(R) \to G_0(R_x) \to 0.$$

Proof. The final statement is immediate from the general statement about localization at S, since $G_0(R/xR)$ is spanned by classes $[R/P]_{R/xR}$ such that $x \in P$ and $x \in P$ iff P meets $\{x^n : n \geq 1\}$, and so the image of $G_0(R/xR)$ in $G_0(R)$ is spanned by the classes $[R/P]_R$ for $x \in P$.

To prove the general statement about localization, first note that the specified classes are clearly in the kernel. To show that these span the entire kernel, it suffices to show that all the spanning relations on the classes $[S^{-1}R/QS^{-1}R_Q]$ hold in the quotient of $G_0(R)$ by the span Γ of the classes $[R/P]$ for $P \cap S \neq \emptyset$. Consider a prime cyclic filtration of

$S^{-1}R/(PS^{-1}R + (x))$, where x may be chosen in R. We may contract (i.e., take inverse images of) the submodules in this filtration to get a filtration of R/P. Each factor N_i contains an element u_i such that, after localization at S, u_i generates $S^{-1}N_i \cong S^{-1}R/Q_i$. Thus, for each i, we have short exact sequences

$$0 \to Ru_i \to N_i \to C_i \to 0 \qquad \text{and} \qquad 0 \to D_i \to Ru_i \to R/Q_i \to 0,$$

where C_i and D_i vanish after localization at S and so have prime cyclic filtrations with factors $R/\mathcal{Q}_j$ such that $\mathcal{Q}_j$ meets S. Here, we have that $Q_1 = P$. We must show that the relation $\sum_{i>1}[S^{-1}R/S^{-1}Q_i] = 0$ comes from a relation on the $[R/Q_i]$ in $G_0(R)/\Gamma$. But $[R/P] = N_1 + \sum_{i>1}[N_i]$, and for every i,

$$[N_i] = [Ru_i] + [C_i] = [R/Q_i] + [C_i] + [D_i].$$

Since $Q_1 = P$, we have

$$0 = [C_1] + [D_1] + \sum_{i>1}[R/Q_i] + [C_i] + [D_i]$$

in $G_0(R)$, and the conclusion we want follows: as aleady observed, every C_i and every D_i is killed by an element of S, and so has a prime cyclic filtration in which each prime cyclic module has a class in Γ. $\square$

We next define the *Grothendieck group of projective modules* over a Noetherian ring R by forming the free abelian group on generators P in $\mathcal{M}$ (one can work with any set of finitely generated projective modules containing a representative of every isomorphism class) and killing the subgroup spanned by elements $P - P' - P''$, where $0 \to P' \to P \to P'' \to 0$ is exact. In this situation the short exact sequence of projectives is split (this only uses that P'' is projective), and so $P \cong P' \oplus P''$. Thus, the elements that we kill to construct $K_0(R)$ have the form $(P' \oplus P'') - P' - P''$. Note that isomorphic projectives represent the same class in $K_0(R)$.

There is obviously a canonical map $K_0(R) \to G_0(R)$ that takes $[P]$ in $K_0(R)$ to $[P]$ in $G_0(R)$ for every finitely generated projective module over R.

Theorem. *If R is regular, the map $K_0(R) \cong G_0(R)$ is an ismorphism.*

Proof. We want to define a map from $G_0(R)$ to $K_0(R)$. Given a finitely generated R-module M, we can choose a finite projective resolution of M by finitely generated projective modules, say $P_\bullet$, and suppose that the length of this resolution is d. The obvious way to define an inverse map is to send $[M]$ to

$$[P_0] - [P_1] + \cdots + (-1)^d[P_d] \in K_0(R).$$

We must check that this is independent of the choice of the projective resolution. Given another such projective resolution $Q_\bullet$ of M we must show that the two alternating sums are the same in $K_0(R)$ (this is obvious in $G_0(R)$, since both equal $[M]$, but M is not

"available" in $K_0(R)$). To prove this, choose a map of complexes $\phi_\bullet : P_\bullet \to Q_\bullet$ such that the induced map of augmentations $M = H_0(P_\bullet) \to H_0(Q_\bullet) = M$ is the identity. Form $C_\bullet$, the mapping cone of ϕ, which is a complex of projective modules. Then $C_n = P_n \oplus Q_{n-1}$. We claim that $C_\bullet$ is exact (not just acyclic): *all* the homology vanishes. To see this, consider the long exact sequence of the mapping cone:

$$\cdots \to H_n(Q_\bullet) \to H_n(C_\bullet) \to H_{n-1}(P_\bullet) \to H_{n-1}(Q_\bullet) \to \cdots .$$

If $n \geq 2$, $H_n(C_\bullet) = 0$ since $H_n(Q_\bullet)$ and $H_{n-1}(P_\bullet)$ both vanish. If $n = 1$, $H_1(C_\bullet)$ vanishes because $H_1(Q_\bullet) = 0$ and the connecting homomorphism $H_0(P_\bullet) \to H_0(Q_\bullet)$ is an isomorphism. If $n = 0$, $H_0(C_\bullet) = 0$ because $H_0(Q_\bullet)$ and $H_{-1}(P_\bullet)$ both vanish.

Thus, the alternating sum of the classes in $C_\bullet$ is 0 in $K_0(R)$, and this is exactly what we want.

Additivity follows because given a short exact sequence of finitely generated modules $0 \to M' \to M \to M'' \to 0$ and projective resolutions $P'_\bullet$ of M' and $P''_\bullet$ of M'' by finitely generated projective modules, one can construct such a resolution for M whose j th term is $P'_j \oplus P''_j$: cf. the middle of page 4 of the Lecture Notes of February 6. $\square$

Math 615: Lecture of March 7, 2012

Note that K_0 is a functor on all maps of Noetherian rings (not just flat maps) because short exact sequences of projectives are split and remain exact no matter what algebra one tensors with. Restriction of scalars from S to R will not induce a map on K_0 unless S is module-finite and *projective* over R.

Observe also that $K_0(R)$ has a commutative ring structure induced by $\_ \otimes_R \_$, with $[R]$ as the multiplicative identity, since the tensor product of two finitely generated projective modules is a projective module, and tensor distributes over direct sum.

Proposition. *Let P and Q be finitely generated projective modules over a Noetherian ring R. Then $[P] = [Q]$ in $K_0(R)$ if and only there is a free module G such that $P \oplus G \cong Q \oplus G$.*

Proof. $[P] = [Q]$ if and only if $[P] - [Q]$ is in the span of the standard relations used to define $K_0(R)$, in which case, for suitable integers h, k,

$$P - Q = \sum_{i=1}^{h} \big((P_i \oplus Q_i) - P_i - Q_i\big) + \sum_{j=1}^{k} \big(P'_j + Q'_j - (P'_j \oplus Q'_j)\big)$$

and so

$$P + \sum_{i=1}^{h} (P_i + Q_i) + \sum_{j=1}^{k} (P'_j \oplus Q'_j) = Q + \sum_{i=1}^{h} (P_i \oplus Q_i) + \sum_{j=1}^{k} (P'_j + Q'_j).$$

The fact that this equation holds implies that the number of occurrences of any given projective module on the left hand side is equal to the number of occurrences of that projective module on the right hand side. Therefore, if we change every plus sign (+) to a direct sum sign ($\oplus$), the two sides of the equation are isomorphic modules: the terms occurring in the direct sum on either side are the same except for order. Therefore:

$$P \oplus \bigoplus_{i=1}^{h}(P_i + Q_i) \oplus \bigoplus_{j=1}^{k}(P'_j \oplus Q'_j) = Q \oplus \bigoplus_{i=1}^{h}(P_i \oplus Q_i) \oplus \bigoplus_{j=1}^{k}(P'_j \oplus Q'_j).$$

In other words, if we let

$$N = \bigoplus_{i=1}^{h}(P_i \oplus Q_i) \oplus \bigoplus_{j=1}^{k}(P'_j \oplus Q'_j),$$

then $P \oplus N = Q \oplus N$. But N is projective, and so we can choose N' such that $N \oplus N' \cong G$ is a finitely generated free module. But then

$$P \oplus N \oplus N' \cong Q \oplus N \oplus N',$$

i.e., $P \oplus G \cong Q \oplus G$. $\square$

Corollary. *let R be Noetherian. $K_0(R)$ is generated by $[R]$ if and only if every projective module P has a finitely generated free complement, i.e., if and only if for every finitely generated projective module M there exist integers h and k in $\mathbb{N}$ such that $P \oplus R^h \cong R^k$.* $\square$

We know that

$$K_0(K[x_1, \ldots, x_n]) \cong G_0(K[x_1, \ldots, x_n]) \cong G_0(K) \cong \mathbb{Z}$$

is generated by the class of R. Therefore, every finitely generated projective module over $R = K[x_1, \ldots, x_n]$ has a finitely generated free complement. To prove that every projective module over a R is free, it suffices to show that if $P \oplus R \cong R^n$ then $P \cong R^{n-1}$. The hypothesis implies precisely that P is the kernel of a map $R^n \twoheadrightarrow R$. Such a map is given by a $1 \times n$ matrix $(r_1 \ \ldots \ r_n)$. The surjectivity of the map corresponds to the condition that the r_j generate the unit ideal of R. If $\sum_{j=1}^{n} r_j s_j = 1$, then the $n \times 1$ column matrix whose entries are $s_1, \ldots, s_n$ mapping $R \to R^n$ gives a splitting. $P \cong R^{n-1}$ implies that this column vector v can be extended to a free basis for R^n, since $R^n = P \oplus Rv$. Since $P \cong R^n/Rv$, P will be free if and only if it has $n-1$ generators, and so P will be free if only if v can be extended to a free basis for R^n. This led to the following question: if one is given one column of a matrix consisting of polynomials over K that generate the unit ideal, can one "complete" the matrix so that it has determinant which is a unit in the polynomial ring? This is equivalent to completing the matrix so that its determinant is 1 if $n \geq 2$: the unit can be absorbed into one of the columns other than the first. This is known as the "unimodular column" problem. However, some authors, who use matrices that act on the right, study the equivalent "unimodular row" problem.

The question was raised by Serre in the mid 1950s and was open until 1976, when it was settled in the affirmative, independently, by D. Quillen and A. Suslin. A bit later, Vaserstein gave another proof which is very short, albeit very tricky. It is true that projective modules over a polynomial ring over a field are free, but it is certainly a non-trivial theorem.

We next want to develop the theory of spectral sequences. Fix a ring R. We work in the category of R-modules, so that all maps are R-linear. But R will play almost no role here. The entire theory works without changes in any abelian category. We shall talk a bit about the notion of an abelian category later. In the sequel, it is understood that the given objects are R-modules and the maps are R-linear.

Spectral sequences arise when a complex has a filtration, that is, a sequential chain of subcomplexes. This may be ascending or descending, and one may also consider filtrations indexed by $\mathbb{Z}$. For simplicity, for the moment, we shall only consider descending filtrations.

We need to choose whether the complex is homological or cohomological, i.e., whether the differential raises degree or lowers degree. This has virtually no effect on the theory, except for whether one writes subscripts or superscripts. For definiteness, we shall assume that the differential lowers degrees by 1. Thus, we assume that we have a complex $\mathcal{K}_\bullet$ with a differential $d_\bullet$ that lowers degrees: $d_n : \mathcal{K}_n \to \mathcal{K}_{n-1}$. (In this section $\mathcal{K}_\bullet$ has, in general, no particular relation to the Koszul complex.) We allow n to take on negative values here, so that the case of cohomology is covered simply by renumbering.

We also assume that we have a descending sequence of subcomplexes, which we write as $\langle \mathcal{K}_\bullet \rangle_p$. Thus:

$$\mathcal{K}_\bullet = \langle \mathcal{K}_\bullet \rangle_0 \supseteq \langle \mathcal{K}_\bullet \rangle_1 \supseteq \langle \mathcal{K}_\bullet \rangle_2 \supseteq \cdots \supseteq \langle \mathcal{K}_\bullet \rangle_p \supseteq \cdots \supseteq \langle \mathcal{K}_\bullet \rangle_\infty = 0.$$

Thus, for each $n \in \mathbb{Z}$ we have

$$\mathcal{K}_n = \langle \mathcal{K} \rangle_0 \supseteq \langle \mathcal{K}_n \rangle_1 \supseteq \langle \mathcal{K}_n \rangle_2 \supseteq \cdots \supseteq \langle \mathcal{K}_n \rangle_p \supseteq \cdots \supseteq \langle \mathcal{K}_n \rangle_\infty = 0.$$

In discussing this material we shall, rather rigidly, reserve n to keep track of where we are in the complex and p for where we are in the filtration.

It will be convenient to make the convention that

$$\langle \mathcal{K}_n \rangle_{-1} = \langle \mathcal{K}_n \rangle_{-2} = \cdots \langle \mathcal{K}_n \rangle_{-\infty} = \mathcal{K}_n.$$

That is, as we move up in the filtration from $\langle \mathcal{K}_n \rangle_p$ we eventually reach $\mathcal{K}_n = \langle \mathcal{K}_n \rangle_0$ and then are "stuck" there.

One can form from the filtered complex $\langle \mathcal{K}_\bullet \rangle_\bullet$ an associated graded complex whose term in degree n is

$$\bigoplus_p \langle \mathcal{K}_n \rangle_p / \langle \mathcal{K}_n \rangle_{p+1}.$$

We denote this complex $E^0_\bullet$. This associated graded complex is a function of the filtered complex $\langle \mathcal{K}_\bullet \rangle_\bullet$: we are omitting the argument from the notation. We shall write $E^1_\bullet$ for the homology of $E^0_\bullet$. On the other hand, we can take the homology of the original complex $H_\bullet(\mathcal{K}_\bullet)$ and give it a filtration by letting $\langle H_\bullet(\mathcal{K}_\bullet)\rangle_p$ be the image of $H_\bullet(\langle \mathcal{K}_\bullet \rangle_p)$. Our objective is to compare the homology of the associated graded complex with the associated graded of the homology of the original complex. There turns out to be a mildly complicated way of making this comparison.

Let us return to $E^1_\bullet$ for a moment. Ordinarily, when one takes homology, the new complex has no differential on it other than 0. But it turns out that there is a (typically) non-trivial differential on $E^1_\bullet$. The homology of $E^1_\bullet$ is a new complex, $E^2_\bullet$, and this likewise has a non-trivial differential on it defined by looking at the original filtered complex. One can continue in this way to define a sequence of complexes $E^r_\bullet$, each of which is the homology of the preceding one. Under certain hypotheses on the original filtration, for each n, E^r_n becomes stable for sufficiently large $r \gg 0$ (in the sense that the incoming and outgoing differentials are both 0, and so taking homology again produces the same object), and is the same as the associated graded of the homology of the original complex, for which we write E^∞_n.

We now give the definitions. Keep in mind that E^r_n will be graded, and we will use p to indicate graded pieces, so that we write

$$E^r_n = \bigoplus_{p=0}^{\infty} E^{r,p}_n$$

When no limits are indicated for p, it is understood that p ranges over all of $\mathbb{N}$. The spectral sequence is the sequence of complexes $\{E^r_\bullet\}_r$ and, again, we shall be rigid in our use of r, which is tracking which term of the sequence of complexes we are considering.

We note that in doing the cohomological theory, where n becomes a superscript, one converts r and p to subscripts, and writes $E^n_{r,p}$ instead of $E^{r,p}_n$.

We build the theory by defining all the modules $E^{r,p}_n$ at once, as well as some auxiliary modules. We define

$$Z^{r,p}_n = \mathrm{Ker}\left(\langle \mathcal{K}_n \rangle_p \xrightarrow{d_n} \mathcal{K}^{n-1}/\langle \mathcal{K}_{n-1}\rangle_{p+r}\right)$$

and

$$B^{r,p}_n = \langle \mathcal{K}_n \rangle_p \cap d_{n+1}(\langle \mathcal{K}_{n+1}\rangle_{p-r}),$$

where $-1 \leq r \leq \infty$. The elements of $Z^{r,p}_n$ are approximately cycles for large r in the sense that they are getting pushed r spots further down in the filtration from where they are by the differential. $B^{r,p}_n$ does not contain all boundaries: only those elements that are values of the differential on elements at most r steps further up in the filtration.

Note that $Z^{0,p}_n = \langle \mathcal{K}_n \rangle_p$, and that if $r = -1$, then $Z^{-1,p+1}_n = \langle \mathcal{K}^n \rangle_{p+1}$ as well.

Observe that

$$B^{-1,p}_n = \langle \mathcal{K}_n \rangle_p \cap d_{n+1}(\langle \mathcal{K}_{n+1}\rangle_{p+1}).$$

Note that

$$Z_n^{\infty,p} = \mathrm{Ker}\,(d_n) \cap \langle \mathcal{K}_n \rangle_p,$$

actual cycles, while

$$B_n^{\infty,p} = \mathrm{Im}\,(d_{n+1}) \cap \langle \mathcal{K}_n \rangle_p.$$

Let

$$E_n^{r,p} = Z_n^{r,p}/(B_n^{r-1,p} + Z_n^{r-1,p+1}).$$

Let

$$E_n^r = \bigoplus_p E_n^{r,p},$$

which is graded. Now let

$$d_n^{r,p} : E_n^{r,p} \to E_{n-1}^{r,p+r}.$$

Let

$$d_n^r = \bigoplus_p d_n^{r,p}.$$

Note that $d_n^r : E_n^r \to E_{n-1}^r$ is a map that shifts the p-grading by r. Then, with respect to these maps, $E_\bullet^r$ with maps $d_\bullet^r$ is a complex of graded modules in which the maps lower degree, but shift the p-grading by r. For every r, $H_\bullet(E_\bullet^r) = E_\bullet^{r+1}$.

Note also that $E_\bullet^0$ is the associated graded complex of $\mathcal{K}_\bullet$, while $E_\bullet^\infty$ is the associated graded complex of $H_\bullet(\mathcal{K}_\bullet)$.

Math 615: Lecture of March 9, 2012

Verification of the basic assertions about spectral sequences. To see that $E_\bullet^0$ is the associated graded complex of $\mathcal{K}_\bullet$, note that

$$E_n^{0,p} = Z_n^{0,p}/(B_n^{-1,p} + Z_n^{-1,p+1}) = \langle \mathcal{K}_n \rangle_p / \big(\langle \mathcal{K}_n \rangle_p \cap d_{n+1}(\langle \mathcal{K}_{n+1} \rangle_{p+1}) + \langle \mathcal{K}_n \rangle_{p+1} \big).$$

Since $d_{n+1}(\langle \mathcal{K}_{n+1} \rangle_{p+1}) \subseteq \langle \mathcal{K}_n \rangle_{p+1}$, the denominator is simply $\langle \mathcal{K}_n \rangle_{p+1}$, and

$$E_n^{0,p} = \langle \mathcal{K}_n \rangle_p / \langle \mathcal{K}_n \rangle_{p+1},$$

as claimed.

To see that $E_\bullet^\infty$ is the associated graded complex of $H_\bullet(\mathcal{K}_\bullet)$, note that

$$E_n^{\infty,p} = Z_n^{\infty,p}/(B_n^{\infty,p} + Z_n^{\infty,p+1}) =$$

$$(\mathrm{Ker}\,(d_n) \cap \langle \mathcal{K}_n \rangle_p)/(\mathrm{Im}\,(d_{n+1}) \cap \langle \mathcal{K}_n \rangle_p + \mathrm{Ker}\,(d_n) \cap \langle \mathcal{K}_n \rangle_{p+1}).$$

Here,

$$(\mathrm{Ker}\,(d_n) \cap \langle \mathcal{K}_n \rangle_p)/(\mathrm{Im}\,(d_{n+1}) \cap \langle \mathcal{K}_n \rangle_p$$

is the image of $H_n(\langle \mathcal{K}_\bullet \rangle_p)$ in $H_n(\mathcal{K}_\bullet)$, while killing the image of $\mathrm{Ker}\,(d_n) \cap \langle \mathcal{K}_n \rangle_{p+1}$ has the effect of passing to the associated graded complex.

Recall that

$$E_n^{r,p} = Z_n^{r,p}/(B_n^{r-1,p} + Z_n^{r-1,p+1}),$$

where

$$Z_n^{r,p} = \mathrm{Ker}\,(\langle \mathcal{K}_n \rangle_p \xrightarrow{d_n} \mathcal{K}^{n-1}/\langle \mathcal{K}_{n-1} \rangle_{p+r})$$

and

$$B_n^{r,p} = \langle \mathcal{K}_n \rangle_p \cap d_{n+1}(\langle \mathcal{K}_{n+1} \rangle_{p-r}).$$

Note quite generally that one has the alternative formula

$$(*_{n,r,p}) \quad d_{n+1}(Z_{n+1}^{r,p-r}) = B_n^{r,p}.$$

It is clear that d_n induces a map $E_n^{r,p} \to E_n^{r,p+r}$, that is,

$$Z_n^{r,p}/(B_n^{r-1,p} + Z_n^{r-1,p+1}) \to Z_n^{r,p+r}/(B_n^{r-1,p+r} + Z_n^{r-1,p+r+1})$$

since $d_n(Z_n^{r,p}) \subseteq Z_{n-1}^{r,p+r}$ (the image of d_n in fact consists of true cycles), the image of $B_n^{r-1,p}$ is 0, while, by $(*_{n-1,r-1,p+r})$ above, the image of $Z_n r - 1, p + 1$ is $B_{n-1}^{r-1,p+r}$.

Finally, we verify that the homology of $E_\bullet^r$ is $E_\bullet^{r+1}$. Notice that $u \in Z_n^{r,p}$ represents a cycle for the map $E_n^{r,p} \to E_{n-1}^{r,p+r}$ precisely if $d_n(u) \in B_{n-1}^{r-1,p+r} + Z_{n-1}^{r-1,p+r+1}$. Now, $B_{n-1}^{r-1,p+r} = d_n(Z_n^{r-1,p+1})$ by $(*_{n-1,r-1,p+r})$ and $Z_n^{r-1,p+1} \subseteq Z_n^{r,p}$. Thus, the cycles are represented precisely by the elements of $Z_n^{r-1,p+1} + V$, where V is the set of elements in $Z_n^{r,p}$ that are mapped to $Z_{n-1}^{r-1,p+r+1}$. Since any element of $d_n(Z_n^{r,p})$ is a cycle, V is the same as the set of elements of $Z_n^{r,p}$ that map in into $\langle \mathcal{K}_{n-1} \rangle_{p+r+1}$, which is precisely $Z_n^{r+1,p}$. Thus, the cycles can be described as the image of $Z_n^{r+1,p} + Z_n^{r-1,p+1}$ in $Z_n^{r,p}/(B_n^{r-1,p} + Z_n^{r-1,p+1})$, which is

$$(B_n^{r-1,p} + Z_n^{r+1,p} + Z_n^{r-1,p+1})/(B_n^{r-1,p} + Z_n^{r-1,p+1}).$$

The image of $E_{n+1}^{r,p-r}$ within this module is the same as the image of the numerator of $E_{n+1}^{r,p-r}$, and the numerator is $Z_{n+1}^{r,p-r}$, whose image is represented by $d_{n+1}(Z_{n+1}^{r,p-r}) = B_n^{r,p}$, and this contains $B_n^{r-1,p}$. Thus, the homology is

$$(B_n^{r-1,p} + Z_n^{r+1,p} + Z_n^{r-1,p+1})/(B_n^{r,p} + Z_n^{r-1,p+1}) \cong Z_n^{r+1,p}/\big(Z_n^{r+1,p} \cap (B_n^{r,p} + Z_n^{r-1,p+1})\big).$$

We are now done provided that we can show that $Z_n^{r+1,p} \cap (B_n^{r,p} + Z_n^{r-1,p+1}) = B_n^{r,p} + Z_n^{r,p+1}$. This follows from the elementary observation that $Y \cap (B + Z) = B + (Y \cap Z)$ for R-modules Y, B, and Z such that $B \subseteq Y$, along with the observations that $B = B_n^{r,p} \subseteq Z_n^{r+1,p} = Y$ and $Z_n^{r+1,p} \cap Z_n^{r-1,p+1} = Z_n r, p + 1$. $\square$

We next observe that if the filtrations begins with a term indexed by $-p_0 < 0$, we have the same theory without essential change. We note two cases in which convergence is obvious. One is the case where the filtration is finite, i.e., all terms are eventually 0. The

second is the case where for every n, the filtration of $\mathcal{K}_n$ is finite: we shall say that the filtration is *locally finite* in this case. In fact, the behavior of the E_n^r only depends on the filtrations for $\mathcal{K}_{n+1}$, $\mathcal{K}_n$, and $\mathcal{K}_{n-1}$.

In particular, we do not need to develop a separate theory for ascending filtrations provide that they are finite or locally finite.

Before proceeding further with the general theory of spectral sequences (in particular, a more precise criterion for convergence), we want to consider two examples of filtered complexes.

Let M be a Noetherian module over a Noetherian ring R, let $\underline{x} = x_1, \ldots, x_d \in R$ and let $I = (x_1, \ldots, x_d)R$. We put a staggered I-adic filtration on the Koszul complex as follows: we let $\langle \mathcal{K}_n(\underline{x};\, M)\rangle_p = I^{p-n}\mathcal{K}_n(\underline{x};\, M)$, where I^t is defined to be R if $t \leq 0$. The fact that these are subcomplexes is a consequence of the fact that the entries of the matrices for the Koszul complex are elements of I.

The associated graded complex is the $E_\bullet^0$ term for a spectral sequence. It is easy to see that it may be identified with the Koszul complex of the associated graded module $\mathrm{gr}_I(M)$ over the associated graded ring $\mathrm{gr}_I(R)$ with respect to the sequence of elements $X_1, \ldots, X_d$, where X_i is the image of x_i in I/I^2. We shall show soon that this Koszul complex converges. The $E_\bullet^\infty$ term is an associated graded complex of the the Koszul homology $H_\bullet(\underline{x};\, M)$.

Our second example is for a cohomological double complex $A^{\bullet\bullet}$ where we assume that $A^{i,j} = 0$ if either $i < 0$ or $j < 0$, with differentials $d^{i,j} : A^{i,j} \to A^{i,j+1}$ and $e^{i,j} : A^{i,j} \to A^{i+1,j}$. Let $H_{\mathrm{I}}(A^{\bullet\bullet})$ denote the result of taking cohomology with respect to columns (i.e., with respect to the maps e): it is a new double complex in which the the vertical maps are 0 and the horizontal maps are induced by d. Likewise, let $H_{\mathrm{II}}(A^{\bullet\bullet})$ denote the result of taking cohomology with respect to rows (i.e., with respect to the maps d): it is a new double complex in which the the horizontal maps are 0 and the vertical maps are induced by e. Thus, we can take iterated cohomology $H_{\mathrm{I}}H_{\mathrm{II}}(A^{\bullet\bullet})$. We can do this in the other order as well and consider $H_{\mathrm{II}}H_{\mathrm{I}}(A^{\bullet\bullet})$. It is frequently of interest to compare what one gets from each of these double complexes of *iterated cohomology* with the cohomology of the total complex $H^\bullet(T^\bullet(A^{\bullet\bullet})$.

The comparison is done using spectral sequences. There is a spectral sequence such that the $E_2^\bullet$ term is $H_{\mathrm{II}}H_{\mathrm{I}}(A^{\bullet\bullet})$ and such that the $E_\infty^\bullet$ term is an associated graded of $H^\bullet\big(\mathcal{T}^\bullet(A^{\bullet\bullet})\big)$. Similarly, there is a spectral sequence whose $E_2^\bullet$ term is $H_{\mathrm{I}}H_{\mathrm{II}}(A^{\bullet\bullet})$ and whose $E_\infty^\bullet$ term is an associated graded of $H^\bullet\big(\mathcal{T}^\bullet(A^{\bullet\bullet})\big)$. *In general, the two filtrations used on $\mathcal{T}^\bullet(A^{\bullet\bullet})$,and hence, on $H^\bullet\big(\mathcal{T}^\bullet(A^{\bullet\bullet})\big)$, are different.* Nonetheless, there are many situations where the information that comes out of this analysis is useful.

To see that one gets a spectral sequence whose $E_2^\bullet$ term is $H_{\mathrm{II}}H_{\mathrm{I}}(A^{\bullet\bullet})$, we filter the total complex as follows. The double complex $A^{\bullet\bullet}$ has a double subcomplex $\langle A^{\bullet\bullet}\rangle_p$ obtained by replacing all the A^{ij} by 0 for $i < p$ by their 0 subobjects by while leaving the A^{ij} unchanged for $i \geq p$. The total complex $\mathcal{T}^\bullet(\langle A^{\bullet\bullet}\rangle_p)$ is then a subcomplex $\mathcal{T}^\bullet(\langle A^{\bullet\bullet}\rangle)_p$ of $\mathcal{T}^\bullet(A^{\bullet\bullet})$ for all p. This gives a locally finite filtration, and so a convergent spectral sequence. The $E_0^\bullet$

term, the associated graded complex, consists of the direct sum of the rows. The $E_1^\bullet$ term is $H_{\mathrm{I}}(A^{\bullet\bullet})$. The $E_2^\bullet$ term is $H_{\mathrm{II}}H_{\mathrm{I}}(A^{\bullet\bullet})$, although this description does not explain the differential, d^2.

Suppose that one has a cohomological double complex in which every row is exact except at the 0 spot and every column is exact except at the 0 spot. The row cohomology is a double complex with all 0 entries except for the 0 th column, which consists of the augmentations of the rows. Then $H_{\mathrm{II}}H_{\mathrm{I}}$ is the cohomology of this single column. In this case, the spectral sequence has already converged: the $E_\infty^\bullet$ term is the same as the $E_2^\bullet$ term. The same is true, quite similarly, for $H_{\mathrm{I}}H_{\mathrm{II}}$. In this instance, the filtrations on the cohomology of the total complex do turn out to agree, and one recovers a cohomological version of the double complex lemma that we proved earlier: the cohomology of the column of row augmentations, the cohomology of the row of column augmentations, and the cohomology of the total complex all agree. The theory of spectral sequences gives a similar result whenever one has that the rows of a double complex are all exact except in the j_0 spot and the columns are all exact except at the i_0 spot. The cohomology of the total complex in degree n is the same as H^{n-j_0} of the of the column formed by taking row cohomology at each j_0 spot, or H^{n-i_0} of the row formed by taking column cohomology at each i_0 spot.

Math 615: Lecture of March 12, 2012

There is an alternative convention for describing the terms of a spectral sequence that is used a great deal, particularly in dealing with the spectral sequence of a double complex. One lets $q = n - p$, and then $E_n^{r,p} = E_{p,q}^r$ in the homological case and $E_{r,p}^n = E_r^{p,q}$ in the cohomological case. The integer p is referred to as the *filtration degree* (or *index*) and the integer q is referred to as the *complementary degree* (or *index*). Then $n = p + q$ is called the *total degree*.

With these notations

$$E_n^r = \bigoplus_{p+q=n} E_{p,q}^r \qquad \text{and} \qquad E_r^n = \bigoplus_{p+q=n} E_r^{p,q}.$$

Note that

$$d^r : E_r^{p,q} \to E_r^{p+r,q-r+1}$$

and

$$d_r : E_{p,q}^r \to E_{p+r,q-r-1}^r$$

in the homological case.

Our theory applies without essential change to a locally finite ascending filtration (we can think of it as descending instead), but because it is numbered "backward," so to speak, the sign of r is reversed, so that

$$d^r : E_r^{p,q} \to E_r^{p-r,q+r+1}$$

and

$$d_r : E^r_{p,q} \to E^r_{p-r,q-r-1}.$$

Notice that if you think of p as negative its absolute value increases by r.

Observe that in the spectral sequence of a cohomological double complex whose E_2 term is $H_{\mathrm{II}}H_{\mathrm{I}}(A^{\bullet\bullet})$, the d^2 map sends $E_2^{p,q} \to E_2^{p+2,q-1}$. If we picture the objects $E_2^{p,q}$ in a double array, the map is making a knight's move, as in chess, from its domain to its target. Then $d_3 : E_3^{p,q} \to E_3^{p+3,q-2}$, as well as the maps $d_r : E_r^{p,q} \to E_r^{p+r,q-r+1}$ for larger r, may be thought of similarly as involving a sort of generalized knight's move.

Consider a homological double complex $A_{\bullet\bullet}$ in which the objects are 0 if either index is negative. Again we can filter by rows, taking the subcomplex $\langle A_{\bullet\bullet}\rangle_p$ in which every A_{ij} is replaced by 0 for $i > p$. (This is really the same filtration as in the cohomological case if we index by $-p$ instead of p.) This is an ascending filtration, but that is harmless since it is locally finite. The total complex $\mathcal{T}_\bullet(A_{\bullet\bullet})$ is likewise filtered, taking $\langle \mathcal{T}_\bullet(A_{\bullet\bullet})\rangle_p = \mathcal{T}_\bullet(\langle A_{\bullet\bullet}\rangle_p)$. The associated graded complex is the direct sum of the rows: this is E^0. E^1 is the homology of the rows, and E^2 is the iterated homology $H_{\mathrm{II}}H_{\mathrm{I}}(A_{\bullet\bullet})$. We get a spectral sequence converging to an associated graded complex of $H_\bullet\big(\mathcal{T}_\bullet(A_{\bullet\bullet})\big)$: this associated graded is the E^∞ term, and there is similarly a spectral sequence from $H_{\mathrm{I}}H_{\mathrm{II}}(A_{\bullet\bullet})$: the E^∞ term is the associated graded complex of $H_\bullet\big(\mathcal{T}_\bullet(A_{\bullet\bullet})\big)$ *with respect to a different grading.*

In dealing with the spectral sequence of a double complex, suppose that one has a formula $F_{p,q}$ for $E^2_{p,q}$ and that the total complex has homology $\mathcal{H}_n$. One sometimes writes $F_{p,q} \underset{p}{\Longrightarrow} \mathcal{H}_n$ to mean that $F_{p,q}$ is the E^2 term of a spectral sequence that converges to an associated graded complex of $\mathcal{H}_n$. The presence of p under the arrow means that p is the filtration degree.

We now give a characterization of convergence.

Theorem. *The following two conditions are equivalent:*

(1) *For every n there exists $r(n) < \infty$ such that*

$$E_n^{r(n)} \cong E_n^{r(n)+1} \cong \cdots \cong E_n^s \cong \cdots \cong E_n^\infty,$$

where this holds in the sense that for $s \geq r(n)$ we have (i) the incoming and outgoing differentials d^s_{n+1} and d^s_n for E^s_n are both 0 and (ii) the inclusion $Z_n^{\infty,p} \subseteq Z_n^{s,p}$ induces an isomorphism of $E_n^{\infty,p} \cong E_n^{s,p}$ for all p.

(2) *For every integer n there exists an integer $s(n)$ such that*

$$(*) \quad \langle \mathcal{K}_{n-1}\rangle_{p+s(n)} \cap d_n(\langle \mathcal{K}_n\rangle) \subseteq d_n(\langle \mathcal{K}_n\rangle_{p+1},$$

$0 \leq p$.

We have already defined a spectral sequence to converge precisely when condition (1) holds, and we have noted that convergence is automatic for locally finite filtrations.

The second condition is sometimes referred to as a *condition of Artin-Rees type*. It compares two filtrations on the module of boundaries $d_n(\langle \mathcal{K}_n \rangle)$, the quotient filtration coming from the filtration on $\mathcal{K}_n$, and the inherited filtration from $\mathcal{K}_{n-1}$. It holds when we use staggered I-adic filtrations on a Koszul complex: it is an immediate consequence of the Artin-Rees lemma (see the Math 614 Lecture Notes of December 10, and the final Theorem of these Lecture Notes from January 18). In fact, suppose that we have a map $N \to M$ of finitely generated modules over a Noetherian ring R that carries an I-stable filtration on N into a given I-stable filtration on M. Then the image B of N has an I-stable filtration $\langle B \rangle_p$ using the images of the submodules in the filtration of N, while the inherited filtration $B \cap \langle M \rangle_p$ on B is also I-stable, by the Artin-Rees Lemma. The existence of s such that $B \cap \langle M \rangle_{p+s} \subseteq B_{p+1}$ is then clear: for s sufficiently large we will have $B \cap \langle M \rangle_{p+s} \subseteq I^{p+1}B \subseteq B_{p+1}$ for all p.

Proof of the Theorem. To see that (1) $\Rightarrow$ (2), fix n and choose $r(n)$ so that one has the isomorphisms described in (1). We want to show that for all p,

$$\langle \mathcal{K}_{n-1} \rangle_{p+r(n)} \cap d_n(\mathcal{K}_n) \subseteq d_n(\langle \mathcal{K}_n \rangle_{p+1}).$$

Suppose that w is in the intersection on the left but not in $d_n(\langle \mathcal{K}_n \rangle_{p+1})$. For all choices of $z \in \mathcal{K}_n$ such that $d_n(z) = w$, choose z so that it lies in $\langle K_n \rangle_{p'}$ for p' as large as possible. We must have $p' \leq p$, or else $w = d_n(z) \in d_n(\langle \mathcal{K}_n \rangle_{p+1})$. Then $z \in Z_n^{r(n)+p-p',p'}$, and represents an element of $E_n^{r(n)+p-p',p'}$. This element must be in the image of $Z_n^{\infty,p'}$, and so we have that $z \in Z_n^{\infty,p'} + B_n^{r(n)+p-p'-1,p'} + Z_n^{r(n)+p-p'-1,p'+1}$, where the sum of the second and third terms give the denominator for $E_n^{r(n)+p-p',p'}$. Since the second term is contained in the first term, this is $Z_n^{\infty,p'} + Z_n^{r(n)+p-p'-1,p'+1}$. Modifying z by subtracting an element of $Z_n^{\infty,p'}$, which does not change $d_n(z)$, we obtain an element of $\langle K_n \rangle_{p'+1}$ with the same image, which contradicts the choice of p'.

Now assume condition (2): we want to prove that (1) holds. First observe that the differential $d_n^{r,p} : E_n^{r,p} \to E_{n-1}^{r,p+r}$ is 0 precisely when

$$d_n(Z_n^{r,p}) \subseteq B_{n-1}^{r-1,p+r} + Z_{n-1}^{r-1,p+r+1}$$

Now if $s \geq s(n)$ and $(*)$ holds then any element of $d_n(Z_n^{s,p})$ is in

$$\langle \mathcal{K}_{n-1} \rangle_{p+s} \cap d_n(\mathcal{K}_n) \subseteq d_n(\langle \mathcal{K}_n \rangle_{p+s-s(n)+1}) \subseteq d_n(\langle \mathcal{K}_n \rangle_{p+1}).$$

However, an element of $\langle \mathcal{K}_n \rangle_{p+1}$ that maps into $\langle \mathcal{K}_{n-1} \rangle_{p+s}$ is automatically in $Z_n^{s-1,p+1}$, so that when (2) holds we actually have

$$d_n(Z_n^{s,p}) \subseteq d_n(Z_n^{s-1,p+1}) = B_n^{s-1,p+s}$$

for all $s \geq s(n)$. This shows that $d_n^{s,p} = 0$ for all $s \geq s(n)$ and all p, and so $d_n^s = 0$ for all $s \geq s(n)$. It remains only to check isomorphism with the term at infinity.

Still assuming (2), note that for all $s \geq s(n+1)$ we have

$$B_n^{s-1,p} = d_{n+1}(\langle K_{n+1}\rangle_{p-(s-1)}) \cap \langle \mathcal{K}_n\rangle_p = d_{n+1}(\mathcal{K}_{n+1}) \cap \langle \mathcal{K}_n\rangle_p = B_n^{\infty,p}.$$

The second equality follows because we have that

$$d_{n+1}(\mathcal{K}_{n+1}) \cap \langle \mathcal{K}_n\rangle_p \subseteq d_{n+1}(\langle K_{n+1}\rangle_{p-(s-1)}),$$

which is an instance of $(*)$ with $n+1$ replacing n and $p-s$ replacing p. Thus, we have a map

$$E_n^{\infty,p} = Z_n^{\infty,p}/(B_n^{\infty,p} + Z_n^{\infty,p+1}) \qquad \text{to} \qquad E_n^{s,p} = Z_n^{s,p}/(B_n^{s-1,p} + Z_n^{s-1,p+1})$$

by virtue of the inclusions $Z_n^{\infty,p} \subseteq Z_n^{s,p}$, $Z_n^{\infty,p+1} \subseteq Z_n^{s-1,p+1}$ and the fact that $B_n^{\infty,p} = B_n^{s-1,p}$. We simply want to see that this map is an isomorphism for large s. But for $s \geq s(n)$, $d_n(Z_n^{s,p}) \subseteq d_n(Z_n^{s-1,p+1})$, which implies that $Z_n^{s,p} \subseteq Z_n^{s-1,p+1} + Z_n^{\infty,p}$, and surjectivity follows.

Finally, suppose that some element of $E_n^{\infty,p}$ maps to 0. Then it is represented by $z \in Z_n^{\infty,p}$ and is also in $B_n^{s-1,p} + Z_n^{s-1,p+1} = B_n^{\infty,p} + Z_n^{s-1,p+1}$. But then

$$z \in Z_n^{\infty,p} \cap (B_n^{\infty,p} + Z_n^{s-1,p+1}) = B_n^{\infty,p} + (Z_n^{\infty,p} \cap Z_n^{s-1,p+1}),$$

using the fact that $Y \cap (B+Z) = B + (Y \cap Z)$ when $B \subseteq Y$, and this is $B_n^{\infty,p} + Z_n^{\infty,p+1})$, as required. This completes the argument that condition (2) is sufficient for convergence. $\square$

Let $A_\bullet$ be a complex with only finitely many nonzero homology modules and let L be an additive function defined on these homology modules with values in an abelian group G. By the *Euler characteristic of $A_\bullet$ with respect to L*, which we denote $\chi_L(A_\bullet)$ or, simply, $\chi(A_\bullet)$, we mean $\sum_{i\in\mathbb{Z}}(-1)^i L\big(H_i(A_\bullet)\big) \in G$. Note that we take homology *before* computing the Euler characteristic: in fact, L need not, in general, be defined on the original modules A_n.

The most important example for us will be the case where $L = \ell$ is length, so that for $\chi(A_\bullet)$ to be defined, $A_\bullet$ must be a complex with only finitely many nonzero homology modules, each of finite length.

An important use of spectral sequences is the comparison of Euler characteristics. Suppose that $A_\bullet$ is a complex with only finitely many nonzero modules in it, and that L is an additive function defined on these modules, on the modules of cycles $Z_i = \operatorname{Ker}(A_i \to A_{i-1})$, on the modules of boundaries $B_i = \operatorname{Im}(A_{i+1} \to A_i)$, and on the homology modules $H_i = Z_i/B_i$. A key observation is that

$$\sum_{i\in\mathbb{Z}}(-1)^i L(A_i) = \sum_{i\in\mathbb{Z}}(-1)^i L(H_i).$$

The point is that we have short exact sequences

$$0 \to Z_i \to A_i \to B_{i-1} \to 0$$

and

$$0 \to B_i \to Z_i \to H_i \to 0$$

for all i, so that

$$\sum_{i\in\mathbb{Z}}(-1)^i L(H_i) = \sum_{i\in\mathbb{Z}}(-1)^i\big(L(Z_i) - L(B_i)\big) = \sum_{i\in\mathbb{Z}}(-1)^i L(Z_i) + \sum_{i\in\mathbb{Z}}(-1)^{i+1} L(B_i) =$$

$$\sum_{i\in\mathbb{Z}}(-1)^i L(Z_i) + \sum_{i\in\mathbb{Z}}(-1)^i L(B_{i-1}) = \sum_{i\in\mathbb{Z}}(-1)^i\big(L(Z_i) + L(B_{i-1})\big) = \sum_{i\in\mathbb{Z}}(-1)^i L(A_i),$$

as claimed.

Because each term in a spectral sequence is the homology of the preceding term, we may apply this in the case where L is length to obtain the following:

Proposition. *Let $\mathcal{K}_\bullet$ be a complex with a descending filtration that has a convergent spectral sequence. Assume (#) that the intersection of the submodules in the induced filtration on $H_\bullet(\mathcal{K}_\bullet)$ is 0. Suppose that the associated graded complex* $\mathrm{gr}(\mathcal{K}_\bullet)$ *has only finitely many nonvanishing homology modules and that these are of finite length. Then $\mathcal{K}_\bullet$ itself has only finitely many nonvanishing homology modules, these are of finite length, and* $\chi(\mathcal{K}_\bullet) = \chi(\mathrm{gr}(\mathcal{K}_\bullet)$.

Proof. $\mathrm{gr}(\mathcal{K}_\bullet)$ is the $E^0_\bullet$ term of the spectral sequence, and its homology is $E^1_\bullet$, which has only finitely many nonzero modules, and these are of finite length. It follows that $E^r_\bullet$ has nonzero terms at most in the spots where $E^1_\bullet$ does, and that all the terms of every $E^r_\bullet$ have finite length. Moreover, since each is the homology of the preceding, it follows by induction on r that the $E^r_\bullet$ all have the same Euler characteristic as $E^0_\bullet$, $r \geq 0$. Since there are only finitely many spots with nonzero terms, the spectral sequence stabilizes at the $E^\infty_\bullet$ term after finitely many steps. Thus, $E^\infty_\bullet$ has only finitely many nonzero terms, each of finite length, and the alternating sum of those lengths is $\chi(E^0_\bullet)$. If the intersection of the submodules in a descending filtration is 0, passing to an associated graded module does not affect whether it is 0, nor whether it has finite length, nor what that length is. Since $E^\infty_\bullet$ is an associated graded complex of $H_\bullet(\mathcal{K}_\bullet)$, it follows that $\mathcal{K}_\bullet$ has only finitely many nonzero homology modules, that they have finite lengths, and that $\chi(\mathcal{K}_\bullet) = \chi(E^0_\bullet)$. $\square$

Note that the condition (#) is automatic for locally finite filtrations, and also for I-stable filtrations on finitely generated modules over a local ring (R, m) with $I \subseteq m$. If z_p representing a cycle is in $I^p\mathcal{K}_n$, then z_p is in $I^{p-c}d_n(\mathcal{K}_{n+1})$ by the Artin-Rees Lemma, and for c independent of p, and so the common image of z_p in homology is in $I^{p-c}H_n(\mathcal{K}_\bullet)$ for all p, and is therefore 0.

If R is Noetherian $x_1, \ldots, x_d \in R$ are such that $M/(x_1, \ldots, x_d)M$ has finite length, with M finitely generated, we denote by $\chi(x_1, \ldots, x_d; M)$ the Euler characteristic of $\mathcal{K}(x_1, \ldots, x_d; M)$. The hypothesis that $M/(x_1, \ldots, x_d)M$ has finite length is equivalent to the assumption that $(x_1, \ldots, x_d)R + \mathrm{Ann}_R M$ is contained only in maximal ideals.

Corollary. *If (R, m) is local, M is finitely generated, and $x_1, \ldots, x_d \in m$ generate an ideal I such that M/IM has finite length, then*

$$\chi(x_1, \ldots, x_d; M) = \chi\big(X_1, \ldots, X_d; gr_I(M)\big)$$

where X_j is in the image of x_j in I/I^2, the degree one graded component of $\mathrm{gr}_I(R)$, and the second Koszul complex is taken over $\mathrm{gr}_I(R)$. $\square$

Math 615: Lecture of March 14, 2012

In connection with problem **3.** of Problem Set #4: if one does not assume a local or graded situation, the result is false. Let $R = K[x, y_1, \ldots, y_n]$ where K is a field, say, and let $I = \big((1-x)y_1, \ldots, (1-x)y_n\big)R \subseteq (1-x)R$. Then $\mathrm{depth}_I R \leq \mathrm{depth}_{(1-x)R} R$. But the depth on a principal ideal is at most 1, and in this case it is exactly one, since any nonzero element of I is a nonzerodivisor on R. On the other hand $J = I + xR = (x, y_1, \ldots, y_n)$, and $\mathrm{depth}_J R = n + 1$.

We are now ready to prove a result stated much earlier, related to the notion of the multiplicity of an ideal generated by a system of parameters. If I is any m-primary ideal of the local ring (R, m) and $M \neq 0$ is a finitely generated R-module, we may consider the Hilbert function

$$H_{I,M}(p) = \ell(M/I^{p+1}M),$$

which we know agrees with a polynomial in p of degree equal to the Krull dimension of M for $p \gg 0$. (We may also do this when the image of I is primary to $m/\mathrm{Ann}_R M$ in $R/\mathrm{Ann}_R M$, but since we may typically replace R by $R/\mathrm{Ann}_R M$, we shall stick to the case where I is actually m-primary.) The leading term of this polynomial has the form $\dfrac{e}{d!}p^d$ where d is the Krull dimension of M and e is a positive integer, called the *multiplicity* of M with respect to I. The multiplicity e can also be obtained as

$$d! \lim_{p\to\infty} \frac{\ell(M/I^{p+1}M)}{p^d}.$$

See the Lecture Notes of January 27.

If $\dim(R) = d$ but we allow M to be of Krull dimension $\leq d$, when the Krull dimension of M is $< d$ there will still be a term of the form $\dfrac{e}{d!}p^d$: now, $e = 0$ iff the dimension of M is less than d: when $\dim(M) = d$, we have that $e > 0$. The theorem that we want to prove next asserts that the Euler characteristic of M with respect to a system of parameters for R is the same as the multiplicity of M with respect to the ideal generated by the parameters if $\dim(M) = \dim(R)$. If $\dim(M) < \dim(R)$, the Euler characteristic is 0. In any case, it is $d!$ times the coefficient of p^d in the Hilbert polynomial of M.

Before proving this result, we note the following. If Q is a polynomial in p, we have defined ΔQ to be the polynomial given by the formula

$$\Delta Q(p) = Q(p) - Q(p-1).$$

See the second page of the Lecture Notes of January 23. If Q is constant, ΔQ is identically 0. Otherwise ΔQ has degree exactly one less than the degree of Q, and its leading coefficient is the degree of Q times the leading coefficient of Q. If d is the degree of Q and a is its leading coefficient, then $\Delta^d Q$ is the constant polynomial $d!\,a$. It is also true that, by a straightforward induction on $k \geq 1$,

$$\Delta^k Q(p) = \sum_{n=0}^{k} (-1)^n \binom{k}{n} Q(p-n).$$

Here, the exponent on Δ indicates iterated composition of the operator Δ. Note that when $k = 1$ this is just the same as the definition: $\Delta Q(p) = Q(p) - Q(p-1)$. When $k = 2$, we can verify the formula as follows:

$\Delta^2 Q(p) = \Delta Q(p) - \Delta Q(p-1) = \big(Q(p) - Q(p-1)\big) - \big(Q(p-1) - Q(p-2)\big) =$
$Q(p) - 2Q(p-1) + Q(p-2)$.

The detailed induction is left to the reader.

Theorem. *Let (R, m, K) be a local ring of Krull dimension d, let $\underline{x} = x_1, \ldots, x_d$ be a system of parameters for R, and let M be a nonzero finitely generated R-module. Let $\dfrac{e}{d!}$ be the coefficient of p^d in the Hilbert polynomial $H(p)$ of M with respect to $I = (x_1, \ldots, x_d)R$, (thus, $H(p) = \ell(M/I^{p+1}M)$ for all $p \gg 0$). Then the Euler characteristic $\chi(\underline{x}; M)$ of the Koszul complex $\mathcal{K}(\underline{x}; M)$ is equal to e, and therefore is 0 if $\dim(M) < d$ and is positive and equal to the multiplicity of M with respect to I if $\dim(M) = d$.*

Proof. We already know that because of the spectral sequence using the staggered I-adic filtration of $\mathcal{K}_\bullet(\underline{x};\, M)$ (where $\langle \mathcal{K}_n(\underline{x};\, M)\rangle_p = I^{p-n}\mathcal{K}_n(\underline{x};\, M)$, with $I^{-t} = R$ for $t \geq 0$) that there is a spectral sequence whose $E_\bullet^0$ term is the associated graded complex of this filtered complex, and whose $E_\bullet^\infty$ term is an associated graded complex of the Koszul homology. The $E_\bullet^0$ term may be identified with $\mathcal{K}\big(X_1, \ldots, X_d; \mathrm{gr}_I(M)\big)$, the Koszul complex of the graded module $\mathrm{gr}_I(M)$ with respect to $\underline{X} = X_1, \ldots, X_d$, where X_j is the image of x_j in I/I^2, the first graded component of $\mathrm{gr}_I(R)$: this is a Koszul complex over $\mathrm{gr}_I(R)$. In particular, $\chi(\underline{x};\, M) = \chi\big(\underline{X};\, \mathrm{gr}_I(M)\big)$.

To calculate the latter, first note that, when we keep track of the grading, we see that $\mathcal{K}_n\big(\underline{X};\, \mathrm{gr}_I(M)\big)$ is the direct sum of $\binom{d}{n}$ copies of $\mathrm{gr}_I(M)(-n)$: the matrix of each map has entries that are either 0 or else $\pm X_j$ for some j, and so the maps increase degree by 1. With this grading, the maps preserve degree, and so for every degree one may take homogeneous components in that degree and get an exact sequence in that degree. In each degree all the homogeneous components are finitely generated modules over the Artin local ring R/I (which is the degree 0 homogeneous component of $\mathrm{gr}_I(R)$) , and all have finite

length. The whole complex is the direct sum of these subcomplexes coming from the various choices of degree, and its homology is therefore the direct sum of the homology of these subcomplexes. Since the homology of the whole complex has finite length, it follows that for all but finitely many degrees the complex is exact in that degree. Therefore we may choose a fixed integer $p > 0$ such that the complex is exact in every degree that exceeds p. Enlarging p if necessary, we may also assume that $p \geq d$ and that $p \geq p_0 + d$, where p_0 is so large that $\ell(M/I^{p'+1}M)$ is given by $H(p')$ for all $p' \geq p_0$ (recall that H is the Hilbert polynomial of M with respect to I).

We may form a subcomplex $\mathcal{G}_\bullet$ that is a direct summand of $\mathcal{K}_\bullet(\underline{X};\, \mathrm{gr}_I(M))$ over $R/(\underline{x})R$ by taking the direct sum of the subcomplexes corresponding to degrees that are $\leq p$. The complementary direct summand has homology 0. Therefore, $\mathcal{G}_\bullet$ is a complex consisting of finite length modules over $R/(\underline{x})R$ that has the same homology as $\mathcal{K}_\bullet(\underline{X};\, \mathrm{gr}_I(M))$. The Euler characteristic of $\mathcal{K}_\bullet(\underline{X};\, \mathrm{gr}_I(M))$ is therefore the same as the Euler characteristic of $\mathcal{G}_\bullet$. But since the modules in $\mathcal{G}_\bullet$ have finite length already, this Euler characteristic can be calculated as the alternating sum of the lengths of the modules in $\mathcal{G}_\bullet$.

Notice that $\mathcal{G}_n$ is actually an associated graded module of $M^{\binom{d}{n}}/I^{p-n}M^{\binom{d}{n}}$, and so has the same length as this module. But that length is

$$\binom{d}{n}\ell(M/I^{p-n}M) = \binom{d}{n}H(p-n).$$

Thus, the alternating sum of the lengths of the modules in $\mathcal{G}_\bullet$ is $\sum_{n=0}^{d}(-1)^n\binom{d}{n}H(p-n)$ for any $p \gg 0$, and this is the same as $(\Delta^d H)(p)$, by the discussion preceding the statement of the Theorem. But if the degree d term of H is $\dfrac{e}{d!}p^d$, we know that this dth difference is $d!\dfrac{e}{d!} = e$, which shows that the multiplicity e is the Euler characteristic of $\mathcal{K}_\bullet\big(\underline{X};\, \mathrm{gr}_I(M)\big)$ and, hence, of the original Koszul complex $\mathcal{K}_\bullet(\underline{x};\, M)$, as claimed. $\square$

We next want to discuss what is sometimes referred to as the *associativity* of Tor. Let A, B, and C be R-modules. We want to relate the modules $\mathrm{Tor}_i^R\big(\mathrm{Tor}_j(A,\, B),\, C\big)$ and the R-modules $\mathrm{Tor}_i^R\big(A,\, \mathrm{Tor}_j^R(B,\, C)\big)$. The general situation is complicated, but a relationship can be given using two spectral sequences which converge to associated graded complexes (with respect to two different gradings) of a new sequence of homology modules.

To carry this through we need to introduce the notion of *triple Tor*: we define

$$\mathrm{Tor}_n^R(A,\, B,\, C) = H_n\big(\mathcal{T}_\bullet(N_\bullet \otimes_R P_\bullet \otimes_R Q_\bullet)\big),$$

where $N_\bullet$, $P_\bullet$, and $Q_\bullet$ are projective resolutions over the ring R of A, B, and C, respectively. To remove ambiguity, we can use the canonical free resolutions of the three modules described in our treatment of Tor, but the values are independent of the projective resolutions used up to canonical isomorphism. For example, if one chooses a different projective resolution $N'_\bullet$ of A, each of the resolutions $N_\bullet$, $N'_\bullet$ maps to the other so as to lift the identity map on A, and these maps of complexes are determined up to homotopy. When

one forms the total total tensor product complex, one still has maps each way unique up to homotopy, and so there is a canonical identification of the homology using $N_\bullet$ and the homology using $N'_\bullet$. Precisely the same comment applies to each of the resolutions $P_\bullet$ and $Q_\bullet$. As in the case of ordinary Tor, one may use a flat resolution instead of a projective resolution.

Consider the complex $\mathcal{D}_\bullet = \mathcal{T}_\bullet(N_\bullet \otimes_R P_\bullet)$. The homology of this complex is $\operatorname{Tor}^R_\bullet(A,\, B)$. Now consider the double complex $\mathcal{D}_\bullet \otimes Q_\bullet$: at the i, j spot we have $\mathcal{D}_j \otimes_R Q_i$. Suppose we fix $i = p$ and take the homology of the pth row, which is $\mathcal{D}_\bullet \otimes_R P_p$. Since P_p is projective, the functor $\_ \otimes_R P_p$ commutes with taking homology, and so this homology is $\operatorname{Tor}^R_\bullet(A,\, B) \otimes_R P_p$. If we fix $j = q$ and take the homology of the qth column we get, from the spectral sequence for $H_{\mathrm{I}} H_{\mathrm{II}}$,

$$\operatorname{Tor}^R_p\big(\operatorname{Tor}^R_q(A,\, B),\, C\big) \underset{p}{\Longrightarrow} \operatorname{Tor}^R_n(A,\, B,\, C).$$

On the other hand, we may consider the double complex $N_\bullet \otimes \mathcal{E}_\bullet$, where we let $\mathcal{E}_\bullet = \mathcal{T}_\bullet(P_\bullet \otimes_R Q_\bullet)$, so that at the i, j spot we have $N_j \otimes_R \mathcal{E}_i$. If we filter by columns, so that we first take homology of columns and then of rows, we first get that the homology of the qth column is $N_q \otimes_R \operatorname{Tor}^R_\bullet(B,\, C)$. Next taking homology of rows, we see that the spectral sequence for $H_{\mathrm{II}} H_{\mathrm{I}}$ gives

$$\operatorname{Tor}^R_q\big(A,\, \operatorname{Tor}^R_p(B,\, C)\big) \underset{q}{\Longrightarrow} \operatorname{Tor}^R_n(A,\, B,\, C).$$

This gives a rather complicated comparison of the iterated Tors, but it does yield useful information in many cases.

Math 615: Lecture of March 16, 2012

Example. Let $\mathcal{K}$ be a filtered complex with a descending filtration

$$\mathcal{K} = \langle \mathcal{K}_\bullet \rangle_0 \supseteq \langle \mathcal{K}_\bullet \rangle_1 \supseteq \langle \mathcal{K}_\bullet \rangle_0 = 0.$$

Consider the spectral sequence of this filtered complex. The associated graded complex is $\mathcal{K}_\bullet / \langle \mathcal{K}_\bullet \rangle_1 \oplus \langle \mathcal{K}_\bullet \rangle_1$: this is $E^0_\bullet$. The $E^1_\bullet$ term is its homology. Let us write $\mathcal{Q}_\bullet$ for the quotient complex $\mathcal{K}_\bullet / \langle \mathcal{K}_\bullet \rangle_1$. Note that what we have is precisely a short exact sequence of complexes:

$$0 \to \langle \mathcal{K}_\bullet \rangle_1 \to \mathcal{K}_\bullet \to \mathcal{Q}_\bullet \to 0.$$

Thus, the $E^1_\bullet$ term is $H_\bullet(\mathcal{Q}_\bullet) \oplus H_\bullet(\langle \mathcal{K}_\bullet \rangle_1)$. The $E^2_\bullet$ is the $E^\infty_\bullet$ term, since of any two objects whose degrees differ by two or more, at least one is 0, and so the $E^2_\bullet$ term is an associated graded of $H_\bullet(\mathcal{K}_\bullet)$. Thus, $E^2_\bullet = H_n(E^1_\bullet)$ will be an associated graded complex of $H_\bullet(\mathcal{K}_\bullet)$. Note that

$$d^{1,0}_n : H_n(\mathcal{Q}_\bullet) \to H_{n-1}(\langle \mathcal{K}_\bullet \rangle_1).$$

This is the connecting homomorphism in the snake lemma. Observe also that all of the maps $d_n^{1,1}$ are 0. Thus, $E_n^{2,0}$ is the kernel of $d_n^{1,0}$, and is also a quotient of $H_n(\mathcal{K}_\bullet)$ by $E_n^{2,1}$, which is $E_n^{\infty,1}$, and is the image of $H_n(\langle\mathcal{K}_\bullet\rangle_1)$ in $H_n(\mathcal{K}_\bullet)$. On the other hand, $E_n^{2,1}$ is the homology at $E_n^{1,1}$, which is $H_n(\langle\mathcal{K}_\bullet\rangle_1$ mod the image of

$$d_{n+1}^{1,0} : H_{n+1}(\mathcal{Q}_\bullet) \to H_n(\langle\mathcal{K}_\bullet\rangle_1).$$

This tells us that

$$H_{n+1}(\mathcal{Q}_\bullet) \to H_n(\langle\mathcal{K}_\bullet\rangle_1) \to H_n(\mathcal{K}_\bullet)$$

is exact, while the isomorphism of the cokernel of $H_n(\langle\mathcal{K}_\bullet\rangle_1) \to H_n(\mathcal{K}_\bullet)$ with the kernel of $d_n^{1,0} : H_n(\mathcal{Q}_\bullet) \to H_{n-1}(\langle\mathcal{K}_\bullet\rangle_1)$ says precisely that

$$H_n(\langle\mathcal{K}_\bullet\rangle_1) \to H_n(\mathcal{K}_\bullet) \to H_n(\mathcal{Q}_\bullet) \to H_{n-1}(\langle\mathcal{K}_\bullet\rangle_1)$$

is exact. These exact sequences, as n varies, fit together into the long exact sequence given by the snake lemma. Thus, the spectral sequence is providing the same information as the snake lemma.

We next want to discuss the functor Ext: in order to do so, we need to discuss some facts about injective modules.

If $0 \to M \to N \to Q \to 0$ is an exact sequence of R-modules, we know that for any R-module N the sequence

$$0 \to \mathrm{Hom}_R(Q,\, N) \to \mathrm{Hom}_R(M,\, N) \to \mathrm{Hom}_R(M,\, N)$$

is exact. An R-module E is called *injective* if, equivalently, (1) $\mathrm{Hom}_R(\_\,, E)$ is an exact functor or (2) for any injection $M \hookrightarrow N$, the map $\mathrm{Hom}_R(N, E) \to \mathrm{Hom}_R(M, E)$ is surjective. In other words, every R-linear map from a submodule M of N to E can be extended to a map of all of N to E.

Proposition. *An R-module E is injective if and only if for every I ideal I of R and R-linear map $\phi : I \to E$, ϕ extends to a map $R \to E$.*

Proof. "Only if" is clear, since the condition stated is a particular case of the definition of injective module when $N = R$ and $M = I$. We need to see that the condition is sufficient for injectivity. Let $M \subseteq N$ and $f : M \to E$ be given. We want to extend f to all of N. Define a partial ordering of maps of submodules M' of N to E as follows: $g \leq g'$ means that the domain of g is contained in the domain of g' and that g is a restriction of g' (thus, g and g' agree on the smaller domain, where they are both defined). The set of maps that are $\geq f$ (i.e., extensions of f to a submodule $M' \subseteq N$ with $M \subseteq M'$) has the property that every chain has an upper bound: given a chain of maps, the domains form a chain of submodules, and we can define a map from the union to E by letting is value on an element of the union be the value of any map in the chain that is defined on that element: they all agree. It is easy to see that this gives an R-linear map that is an upper bound for the chain of maps. By Zorn's lemma, there is a maximal extension. Let $f' : M' \to N$

be this maximal extension. If $M' = N$, we are done. Suppose not. We shall obtain a contradiction by extending f' further.

If $M' \neq N$, choose $x \in N - M'$. It will suffice to extend f' to $M' + Rx$. Let $I = \{i \in R : ix \in M'\}$, which is an ideal of R. Let $\phi : I \to E$ be defined by $\phi(i) = f'(ix)$ for all $i \in I$. This makes sense since every $ix \in M'$. By hypothesis, we can choose an R-linear map $\psi : R \to E$ such that $\psi(i) = \phi(i)$ for all $i \in I$. We have a map $\gamma : M \oplus R \to E$ defined by the rule $\gamma(u \oplus r) = f'(u) + \psi(r)$. We also have a surjection $M \oplus R \to M + Rx$ that sends $u \oplus r \mapsto u + rx$. We claim that γ kills the kernel of this surjection, and therefore induces a map $M' + Rx \to E$ that extends f'. To see this, note that if $u \oplus r \mapsto 0$ the $u = -rx$, and then $\gamma(u \oplus r) = f'(u) + \psi(r)$. Since $-u = rx$, $r \in I$, and so $\psi(r) = \phi(rx) = f'(-u) = -f'(u)$, and the result follows. $\square$

Recall that a module E over a domain R is *divisible* if, equivalently,

(1) $rE = E$ for all $r \in R - \{0\}$ or

(2) for all $e \in E$ and $r \in R - \{0\}$ there exists $e' \in E$ such that $re' = e$.

Corollary. *Over a domain R, every injective module is divisible. Over a principal ideal domain R, a module is injective if and only if it is divisible.*

Proof. Consider the problem of extending a map of a principal ideal $aR \to E$ to all of R. If $a = 0$ the map is 0 and the 0 map can be used as the required extension. If $a \neq 0$, then since $aR \cong R$ is free on the generator a, the map to be extended might take any value $e \in E$ on a. To extend the map, we must specify the value e' of the extended map on 1 in such a way that the extended maps takes a to e: the condition that e' must satisfy is precisely that $ae' = e$. Thus, E is divisible if and only if every map of a principal ideal of R to E extends to a map of R to E. The result is now obvious, considering that in a principal ideal domain every ideal is principal. $\square$

It is obvious that a homomorphic image of a divisible module is divisible. In particular, $W = \mathbb{Q}/\mathbb{Z}$ is divisible $\mathbb{Z}$-module and therefore injective as a $\mathbb{Z}$-module. We shall use the fact that W is injective to construct many injective modules over many other rings. We need several preliminary results.

First note that if C is any ring and V is any C-module, we have a map

$$M \to \mathrm{Hom}_C(\mathrm{Hom}_C(M, V), V)$$

for every R-module M. If $u \in M$, this maps sends u to

$$\theta_u \in \mathrm{Hom}_C\big(\mathrm{Hom}_C(M, V), V\big),$$

define by the rule that $\theta_u(f) = f(u)$ for all $f \in \mathrm{Hom}_C(M, V)$.

Now let $\_^\vee$ denote the contravariant exact functor $\mathrm{Hom}_{\mathbb{Z}}(\_, W)$, where $W = \mathbb{Q}/\mathbb{Z}$ as above. As noted in the preceding paragraph, for every $\mathbb{Z}$-module A we have a map $A \to A^{\vee\vee}$, the double dual into W.

Lemma. *With notation in the preceding paragraph, for every $\mathbb{Z}$-module A, A the homomorphism $\theta_A = \theta : A \to A^{\vee\vee}$ is injective.*

If A happens to be an R-module then the map $A \to A^{\vee\vee}$ is R-linear, and for every R-linear map $f : A_1 \to A_2$ we have a commutative diagram of R-linear maps

$$\begin{array}{ccc} A_1^{\vee\vee} & \xrightarrow{f^{\vee\vee}} & A_2^{\vee\vee} \\ {\scriptstyle\theta_{A_1}}\uparrow & & \uparrow{\scriptstyle\theta_{A_2}} \\ A_1 & \xrightarrow[f]{} & A_2 \end{array}$$

Proof. Given a nonzero element $a \in A$, we must show that there exists $f \in \mathrm{Hom}_{\mathbb{Z}}(A, W)$ such that the image of f under θ_a, is not 0, i.e., such that $f(a) \neq 0$. The $\mathbb{Z}$-submodule D of A generated by a is either $\mathbb{Z}$ or else a nonzero finite cyclic module, which will be isomorphic to $\mathbb{Z}/n\mathbb{Z}$ for some $n > 1$. In either case, there will exist a surjection $D \twoheadrightarrow \mathbb{Z}/n\mathbb{Z}$ for some $n > 1$, and $\mathbb{Z}/n\mathbb{Z}$ embeds in W: it is isomorphic to the span of the class of $1/n$ in $\mathbb{Q}/\mathbb{Z}$. Thus, we have a nonzero map $D \to W$, namely $D \twoheadrightarrow \mathbb{Z}/n\mathbb{Z} \hookrightarrow W$. Since $D \subseteq A$ and W is injective as a $\mathbb{Z}$-module, this map extends to a map of $f : A \to W$. Evidently, $f(a) \neq 0$.

The verifications of the remaining statements are straightforward and are left to the reader. $\square$

Before proving the next result we observe the following. Let R be a C-algebra, let M and N be R-modules, let Q be a C-module, and suppose that we are given a C-bilinear map $B : M \times N \to Q$ such that $B(ru, v) = B(u, rv)$ for all $r \in R$. Then there is a unique C-linear map $f : M \otimes_R N \to Q$ such that $f(u \otimes v) = B(u, v)$ for all $u \in M$ and $v \in N$. This is a consequence of the easily verified fact that $M \otimes_R N$ is the quotient of $M \otimes_C N$ by the span of all elements of the form $ru \otimes v - u \otimes rv$ for $r \in R$, $u \in M$ and $v \in N$. We are now ready to establish the following easy but very important result:

Theorem (adjointness of tensor and Hom). *Let $C \to R$ be a ring homomorphism, let M be and N be R-modules, and let Q be a C-module. Then there is a natural isomorphism $\mathrm{Hom}_C(M \otimes_R N, Q) \to \mathrm{Hom}_R(M, \mathrm{Hom}_C(N, Q)$ as R-modules: the two sides are isomorphic as functors of the three variables M, N, and Q.*

Proof. We define mutually inverse maps explicitly. Given $f : M \otimes_R N \to Q$ as C-modules, let $\Theta(f)$ be the map $M \to \mathrm{Hom}_C(N, Q)$ whose value on $u \in M$ is $\beta_{f,u}$, where $\beta_{f,u}(v) = f(u \otimes v)$. Note that the value of $\Theta(rf)$ on u for $r \in R$ is $\beta_{rf,u}$, where $\beta_{rf,u}(v) = (rf)(u \otimes v) = f\big(r(u \otimes v)\big) = f\big((ru) \otimes v)\big)$, while the value of $r\Theta(f)$ on u is $\Theta(f)(ru)$, and the value of that map on $v \in N$ is $\beta_{f,ru}(v) = f\big((ru) \otimes v\big)$. The R-linearity of Θ follows.

On the other hand, given $g : M \to \mathrm{Hom}_C(N, Q)$, we can define a C-bilinear map $B_g : M \times N \to Q$ by letting $B_g(u, v) = g(u)(v)$. Note that $B_g(ru, v) = g(ru)(v) = \big(rg(u)\big)(v) = g(u)(rv) = B_g(u, rv)$. Let

$$\Lambda : \mathrm{Hom}_R(M, \mathrm{Hom}_C(N, Q) \to \mathrm{Hom}_C(M \otimes_R N, Q)$$

be such that $\Lambda(g)$ is the linear map corresponding to B_g. The check that Λ and Θ are mutually inverse is straightforward, as is the check of naturality: further details are left to the reader. $\square$

Corollary. *Let R be a C-algebra, let F be a flat R-module, and let W be an injective C-module. Then* $\mathrm{Hom}_C(F, W)$ *is an injective R-module.*

Proof. Because of the natural isomorphism

$$\mathrm{Hom}_R(M, \mathrm{Hom}_C(F, W)) \cong \mathrm{Hom}_C(M \otimes_R F, W)$$

we may view the functor

$$\mathrm{Hom}_R(\_, \mathrm{Hom}_C(F, W))$$

as the composition of two functors: $\_ \otimes_R F$ followed by $\mathrm{Hom}_C(\_, W)$. Since F is R-flat, the first is exact, while since W is C-injective, the second is exact. Therefore, the composition is exact. $\square$

We can now put things together:

Theorem. *Over every commutative ring R, every R-module embeds in an injective R-module. In fact, this embedding can be achieved canonically, that is, without making any arbitrary choices.*

Proof. Let M be any R-module. In this construction, $\mathbb{Z}$ will play the role of C above. We can map a free R-module F onto $\mathrm{Hom}_{\mathbb{Z}}(M, W)$, were $W = \mathbb{Q}/\mathbb{Z}$ is injective over $\mathbb{Z}$. We can do this canonically, as in the construction of Tor, by taking one free generator of F for every element of $\mathrm{Hom}_{\mathbb{Z}}(M, W)$. By the Corollary above, $F^\vee = \mathrm{Hom}_Z(F, W)$ is R-injective. Since we have a surjection $F \twoheadrightarrow M^\vee$, we may apply $\mathrm{Hom}_{\mathbb{Z}}(\_, W)$ to get an injection $M^{\vee\vee} \hookrightarrow F^\vee$. But we have injection $M \hookrightarrow M^{\vee\vee}$, and so the composite $M \hookrightarrow M^{\vee\vee} \hookrightarrow F^\vee$ embeds M in an injective R-module canonically. $\square$

While the embedding does not involve the axiom of choice, the proof that it is an embedding and the proof that $F^\vee$ is injective do: both use that W is injective. The argument for that used that divisible $\mathbb{Z}$-modules are injective, and the proof of that depended on the Proposition at the top of page 2, whose demonstration used Zorn's lemma.

Math 615: Lecture of March 19, 2012

Note that if $E \subseteq M$ are R-modules and E is injective, then the identity map $E \to E$ extends to a map from all of M to E that is the identity on E. This means that $E \subseteq M$ splits, and so $M \cong E \oplus_R (M/E)$. This is dual to the fact a surjection $M \twoheadrightarrow P$, with P projective, splits.

If M is a module, we refer to the cokernel of an embedding $M \hookrightarrow E$, where E is injective, as a *first module of cosyzygies* of M. Given $0 \to M \to E^0 \to C^1 \to 0$ exact, where E^0 is injective, we can repeat the process: embed $C^1 \hookrightarrow E^1$ and then we get a cokernel C^2,

a second module of cosyzygies of M. Recursively, we can define a $j+1$ st module of cosyzygies to be a first module of cosyzygies of a j th module of cosyzygies. We have the analogue of Schanuel's lemma on syzygies: given two n th modules of cosyzygies, C_n and C'_n, there are injectives E and E' such that $C_n \oplus E \cong C_n \oplus E'$. The main point is to see this for first modules of syzygies. But if we have

$$0 \to M \xrightarrow{\iota} E \xrightarrow{\pi} C \to 0$$

and

$$0 \to M \xrightarrow{\iota'} E' \xrightarrow{\pi'} C' \to 0$$

then we also have

$$0 \to M \xrightarrow{\iota \oplus \iota'} E \oplus E' \to C'' \to 0.$$

The image of M does not meet $E \oplus 0 \cong E$, and so E injects into C''. The quotient is easily seen to be isomorphic with $E'/\mathrm{Im}\,(M) \cong C'$, i.e., there is an exact sequence

$$0 \to E \to C'' \to C' \to 0,$$

and so $C'' \cong E \oplus C'$. Similarly, $C'' \cong E' \oplus C$, and so $C \oplus E' \cong C' \oplus E$.

Constructing a sequence of modules of cosyzygies of M is equivalent to giving a right injective resolution of M, i.e., a right complex $E^\bullet$, say

$$0 \to E^0 \to E^1 \to E^2 \to \cdots \to E^n \to \cdots,$$

such that all of the E^n are injective, $n \geq 0$, and which is exact except possibly at the 0 spot, while $M \cong H^0(E^\bullet)$, which is $\mathrm{Ker}\,(E^0 \to E^1)$. An n th module of cosyzygies for M is recovered from the injective resolution for every $n \geq 1$ as $\mathrm{Im}\,(E_{n-1} \to E_n)$, or as $\mathrm{Ker}\,(E_n \to E_{n+1})$.

We can define the *injective dimension* $\mathrm{id}_R M$ of an R-module M as follows. If $M = 0$ it is -1. Otherwise, it is finite if and only if M has a finite injective resolution, and it is the length of the shortest such resolution. Then $\mathrm{id}_R M \leq n$, where $n \geq 0$, if and only if M has an injective resolution of length at most n. If M has no finite injective resolution we define $\mathrm{id}_R M = +\infty$. We note that the following are equivalent conditions on a nonzero module M and nonnegative integer n :

(1) M has injective resolution of length at most n.
(2) Some n th module of cosyzygies of M is injective.
(3) Every n th module of cosyzygies of M is injective.

The reader may also check easily that if M is not injective then the injective dimension of any module of cosyzygies of M is $\mathrm{id}_R M - 1$. More generally, if M has injective dimension $\geq n \geq 1$ then any n th module of cosyzygies has injective dimension $\mathrm{id}_R M - n$.

Given a projective resolution $P_\bullet$ of M and an injective resolution $E^\bullet$ of N, we can form a cohomological double complex $\mathrm{Hom}_R(P_j,\, E_i)$ of which a typical square is

$$\begin{array}{ccc} \mathrm{Hom}_R(P_j,\, E^{i+1}) & \longrightarrow & \mathrm{Hom}_R(P_{j+1},\, E^{i+1}) \\ \uparrow & & \uparrow \\ \mathrm{Hom}_R(P_j,\, E^i) & \longrightarrow & \mathrm{Hom}_R(P_{j+1},\, E^i) \end{array}$$

Every row and every column is exact except at the 0 spot. The homology of the total complex is denoted $\mathrm{Ext}^\bullet_R(M,\, N)$. This is the same as the homology of the complex $\mathrm{Hom}_R(M,\, E^\bullet)$ or of the complex $\mathrm{Hom}_R(P_\bullet,\, N)$. Notice that the arrows are reversed, so that the maps raise the index: a typical map is

$$\mathrm{Hom}_R(P_j,\, N) \to \mathrm{Hom}_R(P_{j+1},\, N).$$

To remove the ambiguity from this definition, one may use the canonical free resolution of M, as in the definition of Tor, for $P_\bullet$, and the canonical injective resolution of N, that comes from embedding each successive module of cosyzygies C of N in an injective by mapping a free module F onto $C\vee$ with one element of the free basis for every element of $C\vee$, and then using the embedding $C \hookrightarrow C^{\vee\vee} \hookrightarrow F^\vee$. However, the value of Ext is independent of the resolutions chosen up to canonical isomorphism. One way to see this is to fix the projective resolution and let the injective resolution vary. No matter how the injective resolution is chosen, the cohomology of the total complex is $H^\bullet(\mathrm{Hom}_R(P_\bullet,\, N)$. Similarly, if we fix the injective resolution and vary the projective resolution the cohomology of the total complex is $H^\bullet(\mathrm{Hom}_R(M,\, E^\bullet)$, and so does not change.

One may also see independence of the projective resolution more directly, using the theory of homotopy of maps of complexes. Given two different projective resolutions $P_\bullet$, $Q_\bullet$ of M, there are maps in each direction that lift the identity map on M, and these are unique up to homotopy. It follows that the composition in either order is homotopic to the identity map on the relevant complex, $P_\bullet$ or $Q_\bullet$. After applying $\mathrm{Hom}_R(\_,\, N)$ we still have the maps induced by the homotopy, although, like the maps of complexes, they have reversed direction. This is a homotopy in the cohomological sense: h^n maps the n th term of one complex to the $n-1$ st in the other.

If we develop the theory of Ext purely using injective resolutions, we find that given the following set-up:

$$\begin{array}{ccccccccccc} 0 & \longrightarrow & N & \longrightarrow & E^0 & \longrightarrow & E^1 & \longrightarrow & E^2 & \longrightarrow & \cdots \\ & & {\scriptstyle f}\uparrow & & & & & & & & \\ 0 & \longrightarrow & M & \longrightarrow & Q_0 & \longrightarrow & Q_1 & \longrightarrow & Q_2 & \longrightarrow & \cdots \end{array}$$

where each row is a complex, the bottom row is exact, and the E_j are injective, one can fill in the vertical arrows, i.e., one can give a map of complexes

$$\begin{array}{ccccccccccc} 0 & \longrightarrow & N & \longrightarrow & E^0 & \longrightarrow & E^1 & \longrightarrow & E^2 & \longrightarrow & \cdots \\ & & {\scriptstyle f}\uparrow & & {\scriptstyle \phi^0}\uparrow & & {\scriptstyle \phi^1}\uparrow & & {\scriptstyle \phi^2}\uparrow & & \\ 0 & \longrightarrow & M & \longrightarrow & Q_0 & \longrightarrow & Q_1 & \longrightarrow & Q_2 & \longrightarrow & \cdots \end{array}$$

which is unique up to homotopy. The homotopy is given by R-linear maps $h^n : Q_n \to E_{n-1}$, and if $\phi^\bullet$, $\psi^\bullet$ are two different liftings of f, then

$$\phi^n - \psi^n = e^{n-1}h^n + h^{n+1}d^n$$

for all n for a suitably chosen homotopy $h^\bullet$.

This theory can be used to check the independence of the values of Ext from the choice of injective resolution, just as in the case of Tor.

It is easy to verify that $\operatorname{Ext}^n_R(M,\, N)$ is a functor of the two variables M, N, contravariant in M (when N is held fixed) and covariant in N (when M is held fixed). Given a map $M \to M'$, the map on Ext is induced by lifting it to a map of projective resolutions, unique up to homotopy. (Note that applying $\operatorname{Hom}_R(\_,\, N)$ reverses the arrows.) Likewise, given a map $N \to N'$ the map on Ext is induced by lifting it to a map of injective resolutions, unique up to homotopy. The following result gives a number of basic properties of Ext:

Proposition. *Let R be a ring, and let M, M_i, N,and N_j be R-modules.*

(a) $\operatorname{Ext}^n_R(M,\, N) = 0$ *if* $n < 0$.

(b) $\operatorname{Ext}^0_R(M,\, N) \cong \operatorname{Hom}_R(M,\, N)$ *canonically, as functors of two variables.*

(c) $\operatorname{Ext}^n_R(M,\, N) = 0$ *for all* N *and all* $n \geq 1$ *iff* $Ext^1_R(M,\, N) = 0$ *for all* N *iff* M *is projective.*

(d) $\operatorname{Ext}^n_R(M,\, N) = 0$ *for all* M *and all* $n \geq 1$ *iff* $Ext^1_R(M,\, N) = 0$ *for all* M *iff* N *is injective.*

(e) *Given a short exact sequence* $0 \to M_2 \to M_1 \to M_0 \to 0$ *there is a functorial long exact sequence for Ext, namely*

$$0 \to \operatorname{Hom}_R(M_0,\, N) \to \operatorname{Hom}_R(M_1,\, N) \to \operatorname{Hom}_R(M_2,\, N) \to \operatorname{Ext}^1_R(M_0,\, N) \to \cdots$$

$$\to \operatorname{Ext}^n_R(M_0,\, N) \to \operatorname{Ext}^n_R(M_1,\, N) \to \operatorname{Ext}^n_R(M_2,\, N) \to \operatorname{Ext}^{n+1}_R(M_0,\, N) \to \cdots .$$

(f) *Given a short exact sequence* $0 \to N_0 \to N_1 \to N_2 \to 0$ *there is a functorial long exact sequence for Ext, namely*

$$0 \to \operatorname{Hom}_R(M,\, N_0) \to \operatorname{Hom}_R(M,\, N_1) \to \operatorname{Hom}_R(M,\, N_2) \to \operatorname{Ext}^1_R(M,\, N_0) \to \cdots$$

$$\to \operatorname{Ext}^n_R(M,\, N_0) \to \operatorname{Ext}^n_R(M,\, N_1) \to \operatorname{Ext}^n_R(M,\, N_2) \to \operatorname{Ext}^{n+1}_R(M,\, N_0) \to \cdots .$$

(g) *The map given by multiplication by $r \in R$, acting on the R-module M, induces the map given by multiplication by r on* $\operatorname{Ext}^n_R(M,\, N)$ *for all n. The same is true for the map given by multiplication by r on N.*

Proof. Part (a) is immediate from the definition. Part (b) follows because the exactness of $\cdots \to P_1 \to P_0 \to M \to 0$ implies the exactness of

$$0 \to \operatorname{Hom}_R(M,\, N) \to \operatorname{Hom}_R(P_0,\, N) \to \operatorname{Hom}_R(P_1,\, N),$$

so that $\operatorname{Hom}_R(M,\, N)$ may be identified with

$$H^0\big(\operatorname{Hom}_R(P_\bullet,\, N)\big) = \operatorname{Ker}\big(\operatorname{Hom}_R(P_0,\, N) \to \operatorname{Hom}_R(P_1,\, N)\big).$$

If $M = P_0$ is projective it has the very short projective resolution $0 \to P_0 \to 0$, from which it is clear that all the higher $\mathrm{Ext}^n(M, N)$ vanish, $n \geq 1$. On the other hand, if all $\mathrm{Ext}^1(M,\, N)$ vanish, then map a free module P onto M, and consider

$$0 \to N \to F \to P \to 0.$$

When we apply $\mathrm{Hom}_R(P,\, \_)$ we get

$$0 \to \mathrm{Hom}_R(P,\, N) \to \mathrm{Hom}_R(P,\, F) \to \mathrm{Hom}_R(P,\, P) \to \mathrm{Ext}^1_R(P,\, N),$$

from the long exact sequence for Ext, and the last term, $\mathrm{Ext}^1_R(P,\, N)$, is 0 by hypothesis. It follows that $\mathrm{Hom}_R(P,\, F) \to \mathrm{Hom}_R(P,\, P)$ is surjective, and so the identity map on P is the image of some map $g : P \to F$. But then g is a splitting of $F \twoheadrightarrow P$, and so P is a direct summand of F and therefore projective. The proof of (d) is entirely similar, and the details are left to the reader. (At the last step, one shows that N is a direct summand of an injective module in which it is embedded, and therefore injective.)

To prove (e) one may Hom the short exact sequence $0 \to M_2 \to M_1 \to M_0 \to 0$ into an injective resolution $E^\bullet$ for N and apply the snake lemma, while for (f) one may hom a projective resolution $P_\bullet$ for M into the short exact sequence $0 \to N_0 \to N_1 \to N_2 \to 0$ and apply the snake lemma. Finally, (g) follows because the map given by multiplication by r on every projective (respectively, injective) module of the resolution lifts multiplication by r on M (respectively, on N) to a map of the projective (respectively, injective) resolution. $\square$

An easy but important fact is that if M and N are finitely generated modules over a Noetherian ring R, all of the modules $\mathrm{Ext}^n_R(M,\, N)$ are finitely generated. The point is the one may compute Ext using a projective resolution $P_\bullet$ of M by finitely generated free modules over R. Then $\mathrm{Hom}(P_\bullet,\, N)$ has terms each of which consists of a direct sum of finitely many copies of N, and so every term is a Noetherian module (although there may be infinitely many terms). It follows that the cohomology is Noetherian. We record this explicitly:

Proposition. *Let R be Noetherian and let M and N be finitely generated R-modules. Then the modules $\mathrm{Ext}^n_R(M,\, N)$ are all Noetherian.* $\square$

The following two results use the behavior of Ext to characterize injective dimension and projective dimension.

Proposition. *Let R be a ring, and $n \geq 0$ an integer. The following conditions on the R-module M are equivalent:*
(1) $\mathrm{pd}_R M \leq n$.
(2) $\mathrm{Ext}^{n+1}_R(M,\, N) = 0$ *for every R-module N.*
(3) $\mathrm{Ext}^j_R(M,\, N) = 0$ *for all $j > n$ and every R-module N.*

Proof. It is clear that (1) $\Rightarrow$ (3) since we may use a projective resolution of M of length at most n to compute $\mathrm{Ext}^j(M,\, N)$, and (3) $\Rightarrow$ (2) is obvious. We prove that (2) $\Rightarrow$ (1) by induction on n. The case $n = 0$ is (c) of the preceding Proposition. If $n > 0$, form a short exact sequence $0 \to M_1 \to P \to M \to 0$. The long exact sequence for Ext shows that $\mathrm{Ext}^{n+1}(M, N) \cong \mathrm{Ext}^n(M_1, N) = 0$ for all N, and so M_1 a first module of syzygies of M has projective dimension $\leq n - 1$ by the induction hypothesis. It follows that $\mathrm{pd}_R M \leq n$, as required. $\square$

Proposition. *Let R be a ring. Then N is injective if and only if $\operatorname{Ext}^1_R(R/I,\, N) = 0$ for every ideal I of R.*

Moreover, for every integer $n \geq 0$ the following conditions on the R-module N are equivalent:
(1) $\operatorname{id}_R N \leq n$.
(2) $\operatorname{Ext}^{n+1}_R(R/I,\, N) = 0$ *for every ideal* $I \subseteq R$.
(3) $\operatorname{Ext}^j_R(M,\, N) = 0$ *for all* $j > n$ *and every* R*-module* M.

Proof. Given an ideal $I \subseteq R$ we have a short exact sequence $0 \to I \subseteq R \to R/I \to 0$ yielding that the following is exact from the long exact sequence for Ext:

$$0 \to \operatorname{Hom}_R(R/I,\, N) \to \operatorname{Hom}_R(R,\, N) \to \operatorname{Hom}_R(I,\, N) \to \operatorname{Ext}^1_R(R/I,\, N).$$

If the rightmost term vanishes, then the map $\operatorname{Hom}_R(R,\, N) \to \operatorname{Hom}_R(I,\, N)$ is surjective, which means that every linear map $I \to N$ extends to a map $R \to N$. This is sufficient for N to be injective by the Proposition at the top of page 2 in the Lecture Notes from March 16.

It remains to show the equivalence of (1), (2), and (3), which is quite similar to the proof of the preceding result. First, (1) $\Rightarrow$ (3) because an injective resolution of N of length at most n may be use to compute $\operatorname{Ext}^j(M,\, N)$, and (3) $\Rightarrow$ (2) is obvious. We prove that (2) $\Rightarrow$ (1) by induction on n. The case $n = 0$ is the statement we proved in the preceding paragraph. If $n > 0$ we form a short exact sequence $0 \to N \to E \to N' \to 0$ where E is injective. The long exact sequence for Ext shows that $\operatorname{Ext}^{n+1}(R/I, N) \cong \operatorname{Ext}^n(R/I, N') = 0$ for all R/I, and so N', a first module of cosyzygies of N, has injective dimension $\leq n-1$ by the induction hypothesis. It follows that $\operatorname{id}_R N \leq n$, as required. $\square$

We can now show that over a Noetherian regular ring R of Krull dimension d, the projective dimension of *every* module is at most d. We already know this for finitely generated modules. The argument is almost magically simple.

Corollary (J.-P. Serre). *Let R be a Noetherian regular ring of Krull dimension d. Then the projective dimension of every module, whether finitely generated or not, is at most d. Thus, every d th module of syzygies is projective.*

Proof. We know that for every ideal I of R, $\operatorname{pd}_R(R/I) \leq d$, since R/I is finitely generated. Thus, for all I and all N, $\operatorname{Ext}^j_R(R/I,\, N) = 0$ for $j > d$, and this implies that for all N, $\operatorname{id}_R N \leq d$. But then, for every R-module M, and every R-module N, $\operatorname{Ext}^j_R(M,\, N) = 0$ for $j > d$, and since this holds for all N, it follows that $\operatorname{pd}_R M \leq d$, as claimed. $\square$

Math 615: Lecture of March 21, 2012

If R is a ring, M an R-module, and $\underline{x} = x_1, \ldots, x_n \in R$ the *cohomological Koszul complex* $\mathcal{K}^\bullet(\underline{x};\, M)$ is defined as $\operatorname{Hom}_R\big(\mathcal{K}_\bullet(\underline{x};\, R),\, M\big)$, and its cohomology, called *Koszul cohomology*, is denoted $H^\bullet(\underline{x};\, M)$. The cohomological Koszul complex of R (and, it easily follows, of M) is isomorphic with the homological Koszul complex numbered "backward,"

but this is not quite obvious: one needs to make sign changes on the obvious choices of bases to get the isomorphism. To see this, take the elements

$$u_{j_1,\dots,j_i} = u_{j_1} \wedge \cdots \wedge u_{j_i}$$

with $1 \le j_1 < \cdots < j_i \le n$ as a basis for $\mathcal{K}_i = \mathcal{K}_i(\underline{x}; R)$. Let $\_^*$ indicate the functor $\mathrm{Hom}_R(\_, R)$. We want to set up isomorphisms $\mathcal{K}^*_{n-i} \cong \mathcal{K}_i$ that commute with the differentials.

Note that there is a bijection between the two free bases for $\mathcal{K}_i$ and $\mathcal{K}_{n-i}$ as follows: given $1 \le j_1 < \cdots < j_i \le n$, let $k_1, \dots, k_{n-i}$ be the elements of the set $\{1, 2, \dots, n\} - \{j_1, \dots, j_i\}$ arranged in increasing order, and let $u_{j_1,\dots,j_i}$ correspond to $u_{k_1,\dots,k_{n-i}}$ which we shall also denote as $v_{j_1,\dots,j_i}$.

When a free R-module G has free basis $b_1, \dots, b_t$, this determines what is called a *dual basis* $b'_1, \dots, b'_t$ for G^*, where b'_j is the map $G \to R$ that sends b_j to 1 and kills the other elements in the free basis. Thus, $\mathcal{K}^*_{n-i}$ has basis $v'_{j_1,\dots,j_i}$. However, when we compute the value of the differential d^*_{n-i+1} on $v'_{j_1,\dots,j_i}$, while the coefficient of $v'_{h_1,\dots,h_{i-1}}$ does turn out to be zero unless the elements $h_1 < \cdots < h_{i-1}$ are included among the j_i, if the omitted element is j_t then the coefficient of $v'_{h_1,\dots,h_{i-1}}$ is

$$d^*_{n-i+1}(v'_{j_1,\dots,j_i})(v_{h_1,\dots,h_{i-1}}) = v'_{j_1,\dots,j_i}\big(d_{n-i+1}(v_{h_1,\dots,h_{i-1}})\big),$$

which is the coefficient of $v_{j_1,\dots,j_i}$ in $d_{n-i+1}(v_{h_1,\dots,h_{i-1}})$.

Note that the complement of $j_1, \dots, j_i$ in $\{1, 2, \dots, n\}$ is the same as the complement of $\{h_1, \dots, h_{i-1}\}$ in $\{1, 2, \dots, n\}$, except that one additional element, j_t, is included in the latter. Thus, the coefficient needed is $(-1)^{s-1}x_{j_t}$, where $s-1$ is the number of elements in the complement of $\{h_1, \dots, h_{i-1}\}$ that precede j_t. The signs don't match what we get from the differential in $\mathcal{K}_\bullet(\underline{x}; R)$: we need a factor of $(-1)^{(s-1)-(t-1)}$ to correct (note that $t-1$ is the number of elements in $j_1, \dots, j_i$ that precede j_t). This sign correction may be written as $(-1)^{(s-1)+(t-1)}$, and the exponent is $j_t - 1$, the total number of elements preceding j_t in $\{1, 2, \dots, n\}$. This sign implies that the signs will match the ones in the homological Koszul complex if we replace every v'_{j_i} by $(-1)^{\Sigma}v'_{j_i}$, where $\Sigma = \sum_{t=1}^{i}(j_t - 1)$.

We next want to note that, as was the case for Tor, if we have an exact sequence $0 \to M_1 \to P \to M \to 0$, so that M_1 is a first module of syzygies of M over R, the long exact sequence for Ext yields both

$$0 \to \mathrm{Hom}_R(M, N) \to \mathrm{Hom}_R(P, N) \to \mathrm{Hom}_R(M_1, N) \to \mathrm{Ext}^1_R(M, N) \to 0$$

and isomoorphisms

$$\mathrm{Ext}^i_R(M_1, N) \to \mathrm{Ext}^{i+1}_R(M, N)$$

for $i > 0$.

Thus, every element of $\mathrm{Ext}^1_R(M,\,N)$ is represented by a map from a first module of syzygies of M to N, and the element of $\mathrm{Ext}^1_R(M,\,N)$ represents the obstruction to extending that map from M_1 to all of P. By induction, if M_i is an i th module of syzygies of M, $i \geq 1$, then

$$\mathrm{Ext}^{i+j}_R(M, N) \cong \mathrm{Ext}^j_R(M_i,\, N),$$

$j \geq 1$. In particular, for $i \geq 1$, we have that $\mathrm{Ext}^i_R(M, N) \cong \mathrm{Ext}^1_R(M_{i-1}, N)$, and an element of $\mathrm{Ext}^i_R(M,\,N)$ will be represented by a map $M_i \to N$, giving the obstruction to extending the map to P_{i-1}, where $0 \to M_i \to P_{i-1} \to M_{i-1} \to 0$ is exact.

This can be seen more directly. Let $P_\bullet$ be a projective resolution of M, and let

$$M_i = \mathrm{Ker}\,(P_{i-1} \to P_{i-2}) = \mathrm{Im}\,(P_i \to P_{i-1})$$

for all $i \geq 1$, so that M_i is an i th module of syzygies of M. An element of $\mathrm{Ext}^i(M,\,N)$ is represented by a cycle in $\mathrm{Hom}_R(P_i,\,N)$, that is, a map $P_i \to N$ that kills the image of P_{i+1}. But this is the same thing as a map of $P_i/\mathrm{Im}\,(P_{i+1}) \cong M_i$ to N. The boundaries are the maps $P_i \to N$ that arise by composing $P_i \to P_{i-1}$ with a map $P_{i-1} \to N$. The corresponding maps $M_i \to N$ are the ones that extend to P_{i-1}.

Entirely similar marks apply to cosyzygies: one can form $0 \to N \to E \to N^1 \to 0$, where E is injective and N^1 is a first module of cosyzygies of N, and the long exact sequence for Ext yields:

$$0 \to \mathrm{Hom}_R(M,\,N) \to \mathrm{Hom}_R(M,\,E) \to \mathrm{Hom}_R(M,\,N^1) \to \mathrm{Ext}^1_R(M,\,N) \to 0$$

and isomorphisms

$$\mathrm{Ext}^i_R(M,\,N^1) \to \mathrm{Ext}^{i+1}_R(M,\,N)$$

for $i \geq 1$. Likewise, one has isomorphisms

$$\mathrm{Ext}^{i+j}_R(M, N^j) \cong \mathrm{Ext}^j_R(M,\,N^i)$$

when N_i is an i th module of cosyzygies for N.

Proposition (flat base change in the Noetherian case). *Let R be Noetherian, let S be a flat R-algebra, and let M, N be R-modules. There is a natural isomorphism*

$$S \otimes_R \mathrm{Ext}^j(M,\,N) \to \mathrm{Ext}^j_S(S \otimes_R M,\, S \otimes_R N).$$

Proof. Let $P_\bullet$ be a projective resolution of M by finitely generated (hence, finitely presented) projective modules. Then

$$S \otimes_R \mathrm{Ext}^\bullet_R(M,\,N) \cong S \otimes_R H^\bullet\big(\mathrm{Hom}_R(P_\bullet,\,N)\big) \cong H^\bullet\big(S \otimes_R \mathrm{Hom}_R(P_\bullet,\,N)\big)$$

since S is flat, and since every P_j is finitely presented, this is

$$\cong H^\bullet\big(\mathrm{Hom}_S(S \otimes_R P_\bullet,\, S \otimes_R N)\big) \cong \mathrm{Ext}^\bullet_S(S \otimes_R M,\, S \otimes_R N),$$

since $S \otimes_R P_\bullet$ is a projective resolution of $S \otimes_R M$ over S. It is straightforward to verify that these isomorphisms are independent of the choice of the resolution $P_\bullet$. $\square$

In particular, when R, M, N are Noetherian, Ext commutes with localization and completion.

We briefly describe an alternative approach to the construction of Ext in the category of R-modules which does not use projective or injective modules in the definition. This definition can be adapted to contexts in which there are not enough projective objects and not enough injective objects. We shall not give a complete treatment here: these remarks are only intended to introduce the reader to this circle of ideas. However, we do give examples that show that this point of view leads to new insights about Ext.

We begin with Ext^1. Notice that given a short exact sequence $0 \to A \to B \to C \to 0$ (an extension of C by A) the long exact sequence for exact yields an exact sequence

$$\mathrm{Hom}_R(A,\, A) \to \mathrm{Hom}_R(B,\, A) \to \mathrm{Hom}_R(A,\, A) \to \mathrm{Ext}^1_R(C,\, A),$$

and the identity map on A has an image in $\epsilon \in \mathrm{Ext}^1_R(C,\, A)$.

This element ϵ classifies the extension of C by A in the following sense. Call two such exact sequences $0 \to A \to B \to C \to 0$ and $0 \to A \to B' \to C \to 0$ *equivalent* if there is a map from one to other as follows:

$$\begin{array}{ccccccccc}
0 & \longrightarrow & A & \longrightarrow & B' & \longrightarrow & C & \longrightarrow & 0 \\
 & & \uparrow{\scriptstyle 1_A} & & \uparrow{\scriptstyle f} & & \uparrow{\scriptstyle 1_C} & & \\
0 & \longrightarrow & A & \longrightarrow & B & \longrightarrow & C & \longrightarrow & 0
\end{array}$$

If there is such a map, f is forced to be an isomorphism, and so in this case there is a map the other way. (When we consider higher Ext, there may be a map in one direction but not the other.)

It turns out that two extensions of C by A are equivalent if and only if they give rise to the same element in $\mathrm{Ext}^1_R(C,\, A)$. In fact, suppose that we have such an extension. Write $C = P/C_1$, where P is projective and C_1 is a first module of syzygies of C. Then the map $P \twoheadrightarrow C$ will lift to a map $P \to B$. Then $A \oplus P$ will will map onto B (sending A to B via the given injection $A \hookrightarrow B$), and the map $P \to B$ will map C_1 to A. This map $h : C_1 \to A$ is represents an element of $\mathrm{Ext}^1(C,\, A)$. Conversely, given any element of $\mathrm{Ext}^1_R(C,\, A)$, it is represented by a map $h : C_1 \to A$, and we can construct an extension $A \to B \to C \to 0$ by taking $B = (A \oplus P)/N$, where $N = \{-h(u) \oplus u : u \in C_1\}$, so that every element of C_1 is identified in the quotient with its image in A. Notice that if we kill the image of A in B, $C_1 \subseteq P$ is also killed, and the quotient is C. This explains the map from $\mathrm{Ext}^1_R(C,\, A)$ to equivalence classes of extensions. The remaining details of the proof that $\mathrm{Ext}^1_R(C,\, A)$ classifies extensions are reasonably straightforward.

In describing higher Ext, there is a set-theoretic problem, which we ignore for the moment. Consider exact sequences of length $n + 2$, where $n \geq 1$, of the form

$$0 \to A \to B_{n-1} \to \cdots \to B_0 \to C \to 0.$$

We define two such sequences to be *immediately equivalent* (not standard terminology) if there is a map between them that is the identity on A and on C. The intermediate maps need not be isomorphsims when $n \geq 1$. Immediate equivalence generates an equivalence relation. We claim that the equivalence classes are in bijective correspondence with the elements of $\mathrm{Ext}^n_R(C,\, A)$, and we can define $\mathrm{Ext}^n_R(C,\, A)$ in terms of these equivalence classes.

We first give the map in one direction: fix a projective resolution $P_\bullet$ of C. Then the identity map on C lifts to map of the resolution to the exact sequence, and thus proivdes a map $P_n \to A$ that kills the image of P_{n+1}. This map represents an element of $\mathrm{Ext}^n_R(C,\, A)$. In the other direction, given a map of an n th module of syzygies C_n of C to A, call it h, we construct an exact sequence simply by modifying the last two terms of

$$0 \to C_n \to P_{n-1} \to \cdots \to P_0 \to C \to 0.$$

We replace C_n by A, and P_{n-1} by $(A \oplus P_{n-1})/N$ where $N = \{-h(u) \oplus u : u \in C_n\}$.

Here are four insights that come from this point of view.

Given

$$0 \to A \to B_{n-1} \to \cdots \to B_0 \xrightarrow{\alpha} C \to 0$$

representing an element of $\mathrm{Ext}^n_R(C,\, A)$ and

$$0 \to C \xrightarrow{\beta} D_{m-1} \to \cdots \to D_0 \to E \to 0$$

representing an element of $\mathrm{Ext}^m_R(E, C)$, one can form an exact sequence that "merges" them, dropping C, namely

$$0 \to A \to B_{n-1} \to \cdots \to B_0 \xrightarrow{\beta\circ\alpha} D_{m-1} \to \cdots \to D_0 \to E \to 0.$$

This gives a map $\mathrm{Ext}^m_R(E,\, C) \times \mathrm{Ext}^n_R(C,\, A) \to \mathrm{Ext}^{m+n}_R(E,\, A)$ that turns out to be bilinear. It is called the *Yoneda pairing*.

Second, given a ring homorphism $R \to S$ and S-modules A, C, an exact sequence

$$0 \to A \to B_0 \to \cdots \to B_{n-1} \to C \to 0$$

is obviously an exact sequence of R-modules as well. This gives a very understandable map $\mathrm{Ext}^n_S(M,\, N) \to \mathrm{Ext}^n_R(M,\, N)$.

Third, given an exact sequence

$$0 \to A \to B_0 \to \cdots \to B_{n-1} \to C \to 0$$

of R-modules, if S is R-flat we get an exact sequence

$$0 \to S \otimes_R A \to S \otimes_R B_0 \to \cdots \to S \otimes_R B_{n-1} \to S \otimes_R C \to 0.$$

This gives a rather obvious map $\mathrm{Ext}^n_R(C,\, A) \to \mathrm{Ext}^n_S(S \otimes_R C, S \otimes_R A)$ and hence a map

$$S \otimes_R \mathrm{Ext}^n_R(C,\, A) \to \mathrm{Ext}^n_S(S \otimes_R C, S \otimes_R A)$$

which is always defined when S is R-flat. We proved earlier that it is an isomorphism under additional hypotheses (if R, C and A are Noetherian).

Fourth, given an exact sequence

$$0 \to A \to B_0 \to \cdots \to B_{n-1} \to C \to 0$$

of R-modules, representing an element of $\mathrm{Ext}^n_R(C,\, A)$, if E is injective over R and $\_^\vee$ denotes $\mathrm{Hom}_R(\_,\, E)$, we get an exact sequence

$$0 \to C^\vee \to B^\vee_{n-1} \to \cdots \to B^\vee_0 \to A^\vee \to 0$$

representing an element of $\mathrm{Ext}^n_R(A^\vee,\, C^\vee)$, and so we get a transparently defined map

$$\mathrm{Ext}^n_R(C,\, A) \to \mathrm{Ext}^n_R(A^\vee,\, C^\vee).$$

Math 615: Lecture of March 23, 2012

There is a set-theoretic difficulty with the Yoneda definition of Ext: when $n > 1$ the cardinalities of the modules that can occur are not bounded, and so, even if the isomorphism classes of the modules allowed are restricted, the possible exact sequences form a class rather than a set. This is not an essential difficulty. We have given a construction that provides at least one exact sequence for every element of $\mathrm{Ext}^n_R(C,\, A)$. If one chooses an infinite cardinal that is at least as large as the cardinalities of R, C, and A, one can represent any element of $\mathrm{Ext}^n_R(C,\, A)$ by an exact sequence, of length $n+2$, whose modules are at most of that cardinality. Thus, for any sufficiently large cardinal, one can choose a set of modules that include all isomorphism classes of modules of at most that cardinality, and then consider the equivalence classes of exact sequences from A to C consisting of modules of at most that cardinality. This set will be in bijective correspondence with the elements of $\mathrm{Ext}^n_R(C,\, A)$. If the ring is Noetherian and one wants to work exclusively with finitely generated modules, one can also do that.

It is not difficult to describe the functorial behavior of Ext from the Yoneda point of view. Suppose that we are given R-modules A and C and a map $f : A \to A'$. Given an exact sequence

$$0 \to A \xrightarrow{\alpha} B_n \xrightarrow{\beta} B_{n-1} \to \cdots \to B_1 \xrightarrow{\delta} B_0 \xrightarrow{\gamma} C \to 0$$

representing an element of $\mathrm{Ext}^n_R(C,\, A)$, we expect to be able to construct an exact sequence corresponding to the image of that element in $\mathrm{Ext}^n_R(C,\, A')$. We replace B_n by

$$\frac{A' \oplus B_n}{\{-f(a) \oplus \alpha(a) : a \in A\}}$$

and A by A'. α is replaced by the map α' induced by the map $A' \to A' \oplus B_n$, which is easily seen to be injective, while β is replaced by the homomorphism induced by the map $A' \oplus B \to B_{n-1}$ that kills A' and agrees with β on B.

Similarly, given a map $g : C' \to C$ and an exact sequence representing an element of $\mathrm{Ext}^n_R(C,\, A)$ one expects to be able to construct an exact sequence representing an element of $\mathrm{Ext}^n_R(C',\, A)$. One replaces B_0 by

$$B'_0 = \{(b,\, c') \in B \times C' : \gamma(b) = g(c')\}$$

and C by C'. γ is replaced by the restriction of the product projection of $B \times C' \twoheadrightarrow C'$ to B'_0: it is still surjective. δ is replaced by the map $\delta' : b_1 \mapsto (\delta(b_1),\, 0)$.

The multiplication by elements of R acting on $\mathrm{Ext}^n_R(C,\, A)$ is recovered by using one of these two constructions either for $f : A \xrightarrow{r} A$ or $g : C \xrightarrow{r} C$, which turn out to give the same result.

Addition in $\mathrm{Ext}^1_R(C, \mathbb{A})$ can be described as follows. Suppose that

$$0 \to A \xrightarrow{\alpha} B \xrightarrow{\gamma}\to C \to 0$$

and

$$0 \to A \xrightarrow{\alpha'} B' \xrightarrow{\gamma'}\to C \to 0$$

are exact. Let

$$B'' = \frac{\{(u,\, u'\} \in B \times B' : \gamma(u) = \gamma(u')\}}{\{(-\alpha(a),\, \alpha'(a)) : a \in A\}}$$

Notice that we have a map $\gamma'' : B'' \twoheadrightarrow C$ whose value on the class of $(u,\, u')$ is $\gamma(u)$, which is the same as $\gamma'(u')$, and a map $\alpha'' : A \to b''$ whose value on A is the class of $(\alpha(a), 0)$, which is the same as the class of $(0,\, \alpha'(a))$. It is not difficult to verify that

$$0 \to A \xrightarrow{\alpha''} B'' \xrightarrow{\gamma''} C \to 0$$

is exact, and represents the sum of the elements corresponding to the two exact sequences initially given.

Of great importance is that the 0 element in $\mathrm{Ext}^1_R(C,\, A)$ corresponds to the split exact sequence

$$0 \to C \to C \oplus A \to A \to 0.$$

In particular, $\mathrm{Ext}^1_R(C,\, A) = 0$ if and only if every exact sequence

$$0 \to A \to B \to C \to 0$$

is split.

The Yoneda point of view gives a transparent interpretation of the connecting homomorphism in the long exact sequence for Ext. Suppose that

$$0 \to A \to B \to C \to 0$$

is exact, and we apply $\mathrm{Hom}_R(\_, N)$. The connecting homomorphisms in the long exact sequence for Ext are maps

$$\mathrm{Ext}^n_R(A, N) \to \mathrm{Ext}^{n+1}_R(C, N).$$

These are obtained, up to sign, from the Yoneda pairing: given an element of $\mathrm{Ext}^n_R(A, N)$ represented by an exact sequence:

$$0 \to N \to W_{n-1} \to \cdots \to W_0 \to A \to 0,$$

because $A \cong \mathrm{Ker}\,(B \to C)$ we also have an exact sequence

$$0 \to N \to W_{n-1} \to \cdots \to W_0 \to B \to C \to 0.$$

Similarly, if we apply $\mathrm{Hom}_R(M, \_)$ the connecting homomorphisms map

$$\mathrm{Ext}^n_R(M, C) \to \mathrm{Ext}^{n+1}_R(M, A).$$

Again, up to sign, they turn out to be given by the Yoneda pairing: the element represented by

$$0 \to C \to V_{n-1} \to \cdots \to V_0 \to M \to 0$$

maps to the element represented by

$$0 \to A \to B \to V_{n-1} \to \cdots \to V_0 \to M \to 0.$$

We want to discuss a bit further the problem of showing that when x_n is not a zerodivisor on M, there is an isomorphism $H_\bullet(\underline{x}; M) \cong H_\bullet(\underline{x}^-; M/x_nM)$, where $\underline{x} = x_1, \ldots, x_n$ in R and $\underline{x}^- = x_1, \ldots, x_{n-1}$. This is problem **6.** in Problem Set #4. One method is to use the fact that $\mathcal{K}(\underline{x}; M)$ is the mapping cone of the injection induced by multiplication by x_n acting on $\mathcal{K}(\underline{x}^-; M)$. The quotient complex $\mathcal{Q}_\bullet$ may be identified with $\mathcal{K}(\underline{x}^-; M/x_nM)$. Thus, it suffices to check that the homology of the total complex (or mapping cone) is the same as the homology of the quotient complex, which is done *ad hoc* in the solutions to Problem Set #4. We want to point out three other ways to do this problem, all of which are closely related.

One is to view the mapping cone as a double complex in which the rows are both $\mathcal{K}_\bullet(\underline{x}^-; M)$ and use a spectral sequence argument, taking iterated homology first of columns and then of rows. Each column has only one nonzero homology module, and the resulting row is $\mathcal{Q}_\bullet$. Thus, $H_{\mathrm{II}}H_{\mathrm{I}}$ is $H_\bullet(\mathcal{Q}_\bullet)$, and so this is the same as the homology of the

total complex. This argument is valid for any mapping cone arising from an injection of complexes.

The second is to view Koszul homology as a Tor, and apply the spectral sequence that express the associativity of Tor. If we consider any ring Λ, such as $\mathbb{Z}$ or R, that maps to R, and introduce the auxiliary ring $A = \Lambda[X_1, \ldots, X_n]$, making R into an algebra over this ring by letting $X_j \mapsto x_j$, $1 \le j \le n$, then with $\underline{X} = X_1, \ldots, X_n$ and $\underline{X}^- = X_1, \ldots, X_{n-1}$, we have that

$$H_\bullet(\underline{x};\, M) = \operatorname{Tor}^A_\bullet(A/(\underline{X}),\, M)$$

and

$$H_\bullet(\underline{x}^-;\, M/x_nM) \cong \operatorname{Tor}^A_\bullet(A/(\underline{X}^-),\, M/X_nM).$$

Consider the three A-modules $A/(\underline{X}^-)$, A/X_nA, and M, The tensor product over A of the first two is $A/(\underline{X})$, while all higher Tors vanish because X_n is not a zerodivisor on $A/(\underline{X}^-)$. Then tensor product of the last two is M/X_nM, while all higher Tors vanish because x_n (and, therefore, X_n) is not a zerodivisor on M. But then

$$\operatorname{Tor}^A_\bullet(A/(\underline{X}^-) \otimes_A A/x_nA,\, M) \cong \operatorname{Tor}^A_\bullet(A/(\underline{X}^-),\, A/x_nA \otimes_A M),$$

from which the result follows.

The third method involves developing spectral sequences for iterated Koszul homology. It is possible to view these as a particular case of the spectral sequences expressing the associativity of Tor, but they are very easy to derive directly.

Let $x_1, \ldots, x_n \in R$ and $y_1, \ldots, y_m \in R$. The $\mathcal{K}(\underline{x},\, \underline{y};\, M)$ may be viewed as the total complex of the double complex

$$\mathcal{K}(\underline{x};\, R) \otimes_R \mathcal{K}_\bullet(\underline{y};\, M).$$

A typical column has the form $\mathcal{K}_p(\underline{x};\, R) \otimes_R \mathcal{K}_\bullet(\underline{y};\, M)$ and so the homology of the columns is

$$\mathcal{K}_p(\underline{x};\, R) \otimes_R H_q(\underline{y};\, M) \cong \mathcal{K}_p\big(\underline{x};\, H_q(\underline{y};\, M)\big).$$

The q th row is therefore

$$\mathcal{K}_\bullet\big(\underline{x};\, H_q(\underline{y};\, M)\big),$$

and $H_{\mathrm{I}}H_{\mathrm{II}}$ is

$$H_p\big(\underline{x}; H_q(\underline{y}; M)\big),$$

the iterated Koszul homology. Thus,

$$H_p\big(\underline{x}; H_q(\underline{y}; M)\big) \underset{p}{\Longrightarrow} H_{p+q}(\underline{x},\, \underline{y};\, M).$$

We may similarly consider

$$\mathcal{K}_\bullet(\underline{x};\, M) \otimes \mathcal{K}(\underline{y};\, R)$$

and take $H_{\rm II}H_{\rm I}$ to get

$$H_q(\underline{y};\, H_p(\underline{x};\, M) \underset{q}{\Longrightarrow} H_{p+q}(\underline{x},\, \underline{y};\, M).$$

We may apply this in the context of problem **6.** to the sequences $\underline{x}^-$ and x_n. Since $H_q(x_n;\, M) = 0$ except when $q = 0$, the E^2 term has a single nonzero row, consisting of $H_\bullet(\mathcal{K}(\underline{x}^-;\, M/x_nM)$, which is then the same as the E^∞ term $H_\bullet(\underline{x};\, M)$.

The following result is of great utility, although quite easy to prove. It is similar in spirit to several results that we have already established. It illustrates the fact that when modules have large depth on an ideal, certain homology or cohomology is forced to vanish.

Theorem (Ext characterization of depth). *Let $R \to S$ be a homomorphism of Noetherian rings, let I be an ideal of S, let N be a finitely generated R-module with annihilator I, and let M be a finitely generated S-module. The modules* $\operatorname{Ext}^j_R(N,\, M)$ *are Noetherian S-modules. If $IM = M$ then all of the modules* $\operatorname{Ext}^j_R(N,\, M)$ *vanish. If $IM \neq M$, and* $\operatorname{depth}_I M = d$, *then* $\operatorname{Ext}^j_R(N,\, M) = 0$ *for $j < d$, and* $\operatorname{Ext}^d_R(N,\, M) \neq 0$.

Proof. To see that these Ext modules are Noetherian over S, compute them using a projective resolution $P_\bullet$ of N over R by finitely generated free R-modules. Then $\operatorname{Hom}_R(P_\bullet;\, M)$ consists of finite direct sums of copies of M, and so this complex and its homology consist of Noetherian S-modules.

Next note that $M/IM = 0$ iff $S/IS \otimes_S M = 0$ iff $IS + \operatorname{Ann}_S M = S$. In this case, since the annihilator J of every $\operatorname{Ext}^j_R(N,\, M)$ in S contains IS (because I kills $\operatorname{Ext}^j_R(N,\, M)$ and J is an ideal of S) and contains $\operatorname{Ann}_S M$, we have that $J = S$, so that, for every j, $\operatorname{Ext}^j_R(N,\, M) = 0$.

Now assume that $M \neq IM$, so that $d = \operatorname{depth}_I M$ is finite. We prove the result by induction on d. First suppose that $d = 0$. Let $Q_1, \ldots, Q_h$ be the associated primes of M in S. Let P_j be the contraction of Q_j to R for $1 \leq j \leq h$. The fact that $\operatorname{depth}_I M = 0$ means that I consists entirely of zerodivisors on M, and so I maps into the union of the Q_j. This means that I is contained in the union of the P_j, and so I is contained in one of the P_j: called it $P_{j_0} = P$. Choose $u \in M$ whose annihilator in S is Q_{j_0}, and whose annihilator in R is therefore P. It will suffice to show that $\operatorname{Hom}_R(N,\, M) \neq 0$, and therefore to show that its localization at P is not 0, i.e., that $\operatorname{Hom}_{R_P}(N_P, M_P) \neq 0$. Since P contains $I = \operatorname{Ann}_R N$, we have that $N_P \neq 0$. Therefore, by Nakayama's lemma, we can conclude that $N_P/PN_P \neq 0$. This module is then a nonzero finite dimensional vector space over $\kappa_P = R_P/PR_P$, and we have a surjection $N_P/PN_P \twoheadrightarrow \kappa_P$ and therefore a composite surjection $N_P \twoheadrightarrow \kappa_P$. Consider the image of $u \in M$ in M_P. Since $\operatorname{Ann}_R u = P$, the image v of $u \in M_P$ is nonzero, and it is killed by P. Thus, $\operatorname{Ann}_{R_P} v = PR_P$, and it follows that v generates a copy of κ_P in M_P, i.e., we have an injection $\kappa_P \hookrightarrow M_P$. The composite map $N_P \twoheadrightarrow \kappa_P \hookrightarrow M_P$ gives a nonzero map $N_P \to M_P$, as required.

Finally, suppose that $d > 0$. Then we can choose a nonzerodivisor $x \in I$ on M, and we have that x kills N. The short exact sequence $0 \to M \to M \to M/xM \to 0$ gives a long exact sequence for Ext when we apply $\operatorname{Hom}_R(N,\, \_)$. Because x kills N, it kills all of the

Ext modules in this sequence, and thus the maps induced by multiplication by x are all 0. This implies that the long exact sequence breaks up into short exact sequences

$$(*_j) \quad 0 \to \mathrm{Ext}^j_R(N,\, M) \to \mathrm{Ext}^j_R(N,\, M/xM) \to \mathrm{Ext}^{j+1}_R(N,\, M) \to 0$$

Since M/xM has depth $d-1$ on N, we have from the induction hypothesis that the modules $\mathrm{Ext}^j_R(N,\, M/xM) = 0$ for $j < d-1$, and the exact sequence above shows that $\mathrm{Ext}^j_R(N,\, M) = 0$ for $j < d$. Moreover, $\mathrm{Ext}^{d-1}_R(N,\, M/xM) \neq 0$, and $(*_{d-1})$ shows that $\mathrm{Ext}^{d-1}_R(N,\, M/xM)$ is isomorphic with $\mathrm{Ext}^d_R(N,\, M)$. $\square$

Math 615: Lecture of March 26, 2012

Let $\_^*$ denote the functor $\mathrm{Hom}_R(\_,\, R)$. An R-module is called *reflexive* if the map $\theta_M : M \to M^{**}$ is an isomorphism. Observe also that the value of θ_M on $u \in M$ is the map that sends $f \in M^*$ to $f(u)$. Note that $\theta_{M\oplus N} = \theta_M \oplus \theta_N$ once we identify $(M \oplus N)^{**}$ with $M^{**} \oplus N^{**}$. Thus, $M \oplus N$ is reflexive if and only if both M and N are reflexive. R itself is reflexive, and, hence, so is every finitely generated free module. It follows as well that every finitely generated projective module is reflexive. If R and M are Noetherian, reflexivity is preserved by localization at every multiplicative system, and may be tested locally at maximal ideals, i.e., M is reflexive iff M_m is reflexive over R_m for every maximal ideal m of R.

If R is a domain, reflexive modules are torsion-free: any module of the form M^* is torsion-free. If M is a finitely generated torsion-free module over a Noetherian domain R, the map $M \to M^{**}$ is injective, and becomes an isomorphism if we tensor with the fraction field $\mathcal{F} = \mathrm{frac}\,(R)$. Thus, $M \subseteq M^{**} \subseteq \mathcal{F} \otimes_R M$. We may think of M^{**} as obtained from M by the adjunction of certain fractional elements u/r, where $u \in M$ and $r \in R - \{0\}$.

A Noetherian module M over a Noetherian ring R is said to satisfy the *Serre condition* S_i if for every prime P of R of height h, $\mathrm{depth}_{PR_P} M_P \geq \min\{\mathrm{height}\,(P),\, i\}$. The condition may be limited to primes in $\mathrm{Supp}\,(M)$: it holds when $M_P = 0$ because, by our conventions, the depth is $+\infty$ in that case.

We record the following facts, which will be helpful in understanding reflexive modules over normal Noetherian domains.

Proposition. *Let R be a Noetherian ring and let M, M' be finitely generated R-modules.*

(a) *If M satisfies the Serre condition S_i and I is an ideal of R of height at least i, then* $\mathrm{depth}_I M \geq i$.

(b) *If R is a domain, $M \subseteq M'$ are torsion-free R-modules, $I = \mathrm{Ann}_R(M'/M)$ and* $\mathrm{depth}_I M \geq 2$, *then $M = M'$.*

(c) *If R is a normal domain and M is a torsion-free module, then the height of the annihilator of M^{**}/M is at least 2.*

(d) *If R is normal and I is an ideal of height at least two, then* $\mathrm{depth}_I R \geq 2$.

(e) *If x, y is an improper regular sequence in R then x, y is an improper regular sequence on M^*. (This holds even when R and M are not Noetherian.)*

Proof. (a) By part (b) of the Proposition on the second page of the Lecture Notes from February 17, $\mathrm{depth}_I M$ is the infimum of $\mathrm{depth}_{I_P} M_P$ for $P \in \mathrm{Spec}\,(R)$, and we need only consider primes in $\mathrm{Supp}\,(M)$ that contain I. Once we have localized at $P \supseteq I$, we have $\mathrm{height}\,(P) \geq i$, and the result is immediate from the definition of S_i.

(b) We have a short exact sequence

$$0 \to M \to M' \to M'/M \to 0.$$

Let $N = M'/M$. This short exact sequence represents an element of $\mathrm{Ext}^1_R(N, M)$, The condition $\mathrm{depth}_I M \geq 2$ with $I = \mathrm{Ann}_R N$ implies that $\mathrm{Ext}^1_R(N, M) = 0$ by the final Theorem of the Lecture Notes of March 23. Therefore, the displayed exact sequence is split, and $M' \cong M \oplus M'/M$. But M' is torsion-free, while M'/M has nonzero annihilator. This is only possible if $M'/M = 0$, i.e., $M' = M$, as required.

(c) If the result fails, we can find a prime P of R of height 0 or 1 that contains $I = \mathrm{Ann}(RM^{**}/M)$. It follows that $(M^{**}/M)_P \neq 0$, and this means that M_P is not reflexive over R_P. But R_P is a discrete valuation ring or field, since R is normal, and M_P is torsion-free and, therefore, free, so that it is reflexive.

(d) I cannot be 0. If $I = R$ the depth is $+\infty$, and we are done. Assume that $I \neq 0$ is proper. Let $x \in I - \{0\}$. Since R is normal, principal ideals are unmixed, and so every associated prime of xR as an ideal (these are the associated primes of R/xR as a module) has height one. It follows that I is not contained in the union of these associated primes, or it would be contained in one of them, and then could not have height ≥ 2. This implies that there is an element $y \in I$ not in an associated prime of R/xR, and so y is not a zerodivisor on R/xR. Thus, x, y is a regular sequence in I.

(e) If x kills $f \in \mathrm{Hom}_R(M, R)$ then x kills every value of f. This implies that all the values of f are 0, and so $f = 0$. Now suppose that $f, g \in \mathrm{Hom}_R(M, R)$ and $yg = xf$. For every $u \in M$, we have that $yg(u) = xf(u)$ in with $g(u)$, $f(u) \in R$. It follows that $g(u) = h(u)x$ for some choice of $h(u) \in R$, and $h(u)$ is unique because x is not a zerodivisor on R. It is quite straightforward to verify that $h : M \to R$ is R-linear, since g is linear and x is not a zerodivisor on R. Thus, $g \in x\mathrm{Hom}_R(M, R)$, as required. $\square$

Since $M \subseteq M^{**} \subseteq \mathcal{F} \otimes_R M$ when M is torsion-free and R is a Noetherian domain, it is natural to try to characterize the fractional elements in $\mathcal{F} \otimes_R M$ that are in M^{**}. The following result achieves this when R is normal, and also gives a useful characterization of reflexive modules. If M is torsion-free over a domain R with fraction field $\mathcal{F}$, and $v \in \mathcal{F} \otimes_R M$, we write $M :_R v$ for $\{r \in R : rv \in M\}$. This ideal is called the *denominator ideal* for v. A nonzero element $r \in R$ is in $M :_R v$ if and only if v can written as u/r for some $u \in M$.

Theorem. *Let M be a finitely generated torsion-free module over a Noetherian ring normal domain R. Then M is reflexive if and only if M satisfies the Serre condition S_2. For any finitely generated R-module M, M^* and M^{**} are reflexive, and, if M is torsion-free, M^{**}, the reflexivization of M, may be identified with $\{v \in \mathcal{F} \otimes_R M : \mathrm{height}\,(M :_R v) \geq 2\}$.*

Proof. We first check that if M is S_2 the M is reflexive. By part (c) of the preceding Proposition, the annihilator I of M^{**}/M has height 2. By part (a) of the Proposition, $\operatorname{depth}_I M \geq 2$. Finally, by part (b), $M^{**} = M$.

We next check that M^* is S_2 for any finitely generated R-module M. Note that if T is the torsion submodule of M, $M^* \cong (M/T)^*$, since any homomorphism from M to R must kill T. If $M = 0$ the result is vacuously true. Therefore assume that $M \neq 0$ is torsion-free. Suppose that P is a prime in the support of M. If the height of P is one or zero then $(M^*)_P$ is free over R_P and there is nothing to check. If the height of P is two or more, then then PR_P contains a regular sequence on R_P of length two. By part (e) of the preceding Proposition, this will be a regular sequence on M_P (Nakayama's lemma implies that it is a regular sequence, not just an improper regular sequence).

This implies that M^* and M^{**} are reflexive. Moreover, since every reflexive module has the form M^{**}, every reflexive module is S_2.

Finally, by part (c) of the preceding Proposition, the denominator ideal of every element of $M^{**} \subseteq \mathcal{F} \otimes_R M$ has height at least 2, since the denominator ideal contains $\operatorname{Ann}_R(M^{**}/M)$. On the other hand, if $v \in \mathcal{F} \otimes_R M$ has denominator ideal J of height at least two, we have an exact sequence

$$0 \to M \to M + Rv \to R/J \to 0,$$

because $(M + Rv)/M \cong R/\{r \in R : rv \in M\} = R/J$. When we apply $\operatorname{Hom}_R(\_, R)$, we get

$$0 \to 0 \to \operatorname{Hom}_R(M + Rv, R) \to \operatorname{Hom}_R(M, R) \to \operatorname{Ext}^1_R(R/J, R) \to 0.$$

By part (d) of the preceding Proposition, since the height of J is at least two, $\operatorname{depth}_I R \geq 2$, and so $\operatorname{Ext}^1_R(R/J, R) = 0$ by the final result of the Lecture of March 23. Thus, $M \to M + Rv$ induces an isomorphism $(M + Rv)^* \to M^*$ and, hence, an isomorphism

$$M^{**} \to (M + Rv)^{**}.$$

The injection

$$M + Rv \hookrightarrow (M + Rv)^{**} \cong M^{**}$$

together with the compatibility of all of these maps with $\mathcal{F} \otimes_R \_$ shows that

$$v \in M^{**} \subseteq \mathcal{F} \otimes_R M.$$

□

Math 615: Lecture of March 28, 2012

Given an ideal I in a Noetherian domain R we may choose to think of it simply as a torsion-free R-module of torsion-free rank one. In fact, any finitely generated torsion-free

module M of torsion-free rank one is isomorphic with an ideal: we know that if $\mathcal{F}$ is the fraction field of R, then $\mathcal{F} \otimes_R M \cong \mathcal{F}$. If the images of a finite set of generators for M are $r_1/s, \ldots, r_h/s \in \mathcal{F}$ where $r_1, \ldots, r_h \in R$ and $s \in R - \{0\}$ (we may use, for example, the product of the denominators as a common denominator), then M is isomorphic with the R-span of $r_1/s, \ldots, r_h/s \in \mathcal{F}$, and multiplication by s gives an isomorphism of M with $I = (r_1, \ldots, r_h)R \subseteq R$.

If R is a domain, and I is an ideal, then $I^{**} \subseteq R^{**} = R$ is also an ideal. When R is normal Noetherian we can characterize I^{**} in terms of the primary decomposition of I. The ideal (0) is reflexive and we assume $I \neq 0$.

Let R be a normal Noetherian domain, and let $I \neq 0$ be an ideal of R. Suppose that the associated primes of I are $P_1, \ldots, P_h$ and $Q_1, \ldots, Q_k$, where $P_1, \ldots, P_h$ have height one and $Q_1, \ldots, Q_k$ have height > 1. Fix a primary decomposition

$$P_1^{(n_1)} \cap \cdots \cap P_h^{(n_h)} \cap \mathfrak{A}_1 \cap \cdots \cap \mathfrak{A}_k$$

for I, where each $\mathfrak{A}_j$ is Q_j-primary. The n_j are unique, since the P_j must be minimal primes of I (all ideals primary to height one primes of a normal Noetherian domain are symbolic powers, since R_P is a DVR).

Theorem. *With hypotheses and notation as in the preceding paragraph,*

$$I^{**} = P_1^{(n_1)} \cap \cdots \cap P_h^{(n_h)},$$

the "height one part" of a primary decomposition of I. If I is not contained in any height one primes, the intersection on the right is taken over the empty set and is defined to be R.

Proof. Let $J = P_1^{(n_1)} \cap \cdots \cap P_h^{(n_h)}$ or let $J = R$ of I is not contained in any height one prime. Note that $I \subseteq J \Rightarrow I^{**} \subseteq J^{**} \subseteq \mathcal{F}$. We first want to prove that J is reflexive. If $u \in R$ is in J^{**}, it suffices to show that $u \in P_j^{(n_j)} = Q_j$ for all j, and $u \in Q^{**}$ since $J^{**} \subseteq Q_j^{**}$. After localization at P_j, P_j and Q_j become principal, $Q_j^{**}R_{P_j} = Q_jR_{P_j}$ is reflexive, and so $u \in Q_jR_{P_j} \cap R = Q_j$, since primary ideals are contracted with respect to localization at the corresponding prime ideal. It follows that $u \in J$. Thus, $I^{**} \subseteq J$. To complete the proof, it will suffice to show that $J \subseteq I^{**}$, and for this is suffices to show that J/I has a height two annihilator, by the characterization of reflexivization given in the Lecture Notes of March 26. Let $J' = \mathfrak{A}_1 \cap \cdots \cap \mathfrak{A}_k$. Then J' has height at least two, and $I = J \cap J'$, so that $J'J \subseteq I$, and this shows that J' annihilates J/I, as required. $\square$

Before beginning our study of abelian categories, we want to mention another application of the theory of spectral sequences: one can extend the result on the adjointness of tensor and Hom to a relationship on Tor and Ext. Given three modules A, B, C take projective resolution $P_\bullet$ and $Q_\bullet$ of A and B and an injective resolution $E_\bullet$ of C. Let $\mathcal{D}_\bullet = \mathcal{T}_\bullet(P_\bullet \otimes_R Q_\bullet)$ and $T^\bullet = \mathcal{T}^\bullet\big(\mathrm{Hom}_R(\mathcal{D}_\bullet, E^\bullet)\big)$, a cohomological complex. Then the cohomology of a row of $\mathrm{Hom}_R(\mathcal{D}_\bullet, E^\bullet)$ has the form $\mathrm{Hom}_R(\mathrm{Tor}_p^R(A,B), E^q)$, and the iterated cohomology is $\mathrm{Ext}_R^q(\mathrm{Tor}_p^R(A,B),\, C)$. Thus,

$$\mathrm{Ext}_R^q(\mathrm{Tor}_p^R(A,B),\, C) \underset{p}{\Longrightarrow} H^{p+q}(T^\bullet).$$

On the other hand, let $\mathcal{G}^\bullet = \mathcal{T}^\bullet\big(\mathrm{Hom}_R(Q_\bullet, E^\bullet)\big)$, a cohomological complex. By the adjointness of tensor and Hom, $\mathcal{T}^\bullet\big(\mathrm{Hom}_R(P_\bullet, \mathcal{G}^\bullet)\big)$ may be identified with $T^\bullet$. Fixing first columns and then rows in $\mathrm{Hom}_R(P_\bullet, \mathcal{G}^\bullet)$ we get a spectral sequence

$$\mathrm{Ext}_R^p\big(A,\, \mathrm{Ext}_R^q(B,\, C)\big) \underset{q}{\Longrightarrow} H^{p+q}(T^\bullet).$$

The gradings on $H^\bullet(T^\bullet)$ are different.

We next want to discuss the definitions and some basic properties of additive and abelian categories. We first review some category-theoretic notions.

In this discussion of categories, we shall write $\mathrm{Hom}_{\mathcal{A}}(X,\, Y)$ for the set of morphisms from $X \to Y$ in the category $\mathcal{A}$, instead of $\mathrm{Mor}_{\mathcal{A}}(X,\, Y)$, since Hom is often the notation used for the morphisms in an abelian category. The subscript $\mathcal{A}$ is frequently omitted.

A morphism $f : A \to B$ in a category $\mathcal{A}$ is called a *monomorphism* if for any two morphisms $g : X \to A$ and $h : X \to A$, whenever $fg = fh$ then $g = h$. The composition of two monomorphisms is a monomorphism. In the categories of sets, topological spaces, groups and R-modules, monomorphisms correspond to morphisms that are injective on the underlying sets.

Example. Consider the category whose objects are the subsets of the integers and whose morphisms are functions $f : X \to Y$ such that are either (1) $X = Y$ and f is the identity map or (2) $f(X)$ is a proper subset of the odd integers in Y. It is easy to verify that the composition of two such functions is again such a function, and we get a subcategory of the category of sets. In this category, a monomorphism need not be injective. A function from X is a monomorphism if and only if it is injective when restricted to the odd integers in X.

A morphism $f : A \to B$ in a category $\mathcal{A}$ is called an *epimorphism* if for any two morphisms $g : A \to Y$ and $h : A \to Y$, whenever $gf = hf$ then $g = h$. In the categories of sets, groups and R-modules, epimorphisms correspond to morphisms that are surjective on the underlying sets. In the category of Hausdorff topological spaces, an epimorphism is a continuous map whose image is dense: it need not be surjective. In the category of commutative rings, if S is either a quotient or a localization of R, the map $R \to S$ is an epimorphism. Thus, epimorphisms need not be surjective.

A morphism in $\mathcal{A}$ is a monomorphism if and only if it is an epimorphism in $\mathcal{A}^{\mathrm{op}}$. Thus, one might speak of comonomorphisms instead of epimorphisms or coepimorphisms instead of monomorphisms. However, this is terminology is not actually being used.

Examples. In the category of commutative rings, the inclusion $\mathbb{Z} \subseteq \mathbb{Q}$ is both a monomorphism and an epimorphism, but not an isomorphism. In the category of topological spaces, the map $\mathbb{Q} \subseteq \mathbb{R}$ is both a monomorphism and an epimorphism but not an isomorphism.

A *product* for objects A and B in $\mathcal{A}$ consists of a triple $(X,\, \pi_A,\, \pi_B)$ where X is an object, $\pi_A : X \to A$, and $\pi_B : X \to B$, such that for every object Y the map

$$\mathrm{Hom}\,(Y,\, X) \to \mathrm{Hom}\,(Y,\, A) \times \mathrm{Hom}\,(Y,\, B)$$

given by $f \mapsto (\pi_A f,\, \pi_B f)$ is an isomorphism of sets. Roughly speaking, to give a morphism from Y to the product X is equivalent to giving a morphism from $Y \to A$ and a morphism from $Y \to B$. The product, if it exists, is determined up to unique isomorphism and is denoted $A \times B$ or $A \prod B$. We shall use the former notation. The morphisms π_A, π_B are referred to as the *product projections*. They need not be epimorphisms in general. Let $f : Y \to A$ and $g : Y \to B$. In the Lecture Notes from Math 614 we used the notation $(f,\, g)$ for the corresponding morphism $Y \to X$. This notation is suggested by the case of the category of sets, where the category-theoretic notion of product coincides with the Cartesian product, and the value of $(f,\, g)$ on $y \in Y$ is $\big(f(y),\, g(y)\big)$. Products exist in the categories of sets, topological spaces, groups, abelian groups, commutative rings, R-algebras, rings, and R-modules. In all cases, the underlying set is the Cartesian product, and the product projections are given by the usual set-theoretic maps. In the case of topological spaces, one uses the product topology. In the cases of groups, commutative rings, and R-modules, one uses the Cartesian product with algebraic operations performed coordinate-wise. In dealing with abelian categories, it will be useful to have an alternative notation for $(f,\, g)$, namely $\begin{bmatrix} f \\ g \end{bmatrix}$.

The coproduct of two objects in $\mathcal{A}$ is the same as the product of two objects in $\mathcal{A}^{\mathrm{op}}$. Explicitly, a coproduct for A and B consists of an object X and maps $\iota_A : A \to X$ and $\iota_B : B \to X$ such that for every object Y the map

$$\mathrm{Hom}\,(X,\, Y) \to \mathrm{Hom}\,(A,\, Y) \times \mathrm{Hom}\,(B,\, Y)$$

given by $f \mapsto (f\iota_A,\, f\iota_B)$ is an isomorphism of sets. The morphisms $\iota_A,\, \iota_B$ need not, in general, be monomorphisms. (In the category of commutative rings with identity, the coproduct of $\mathbb{Z}/2Z$ and $\mathbb{Z}/3\mathbb{Z}$ turns out to be the zero ring.) Roughly speaking, to give a morphism from the coproduct X to Y is equivalent to giving a morphism from $A \to Y$ and a morphism from $B \to Y$. The coproduct, if it exists, is determined up to unique isomorphism and is denoted $A \oplus B$ or $A \coprod B$. We shall use the former notation. We shall use the notation $[\, f \quad g\,]$ for the morphism $Y \to X$ corresponding to $f : A \to X$ and $g : B \to X$. Coproducts exist in the categories of sets, topological spaces, groups, abelian groups, commutative rings, commutative R-algebras, and R-modules. In sets and topological spaces the coproduct is the disjoint union. In groups it is the free join. Note that the coproduct of two free groups on one generator in the category of groups is the free (non-commutative) group on two generators. Coproducts in the categories of abelian groups and of R-modules are given by direct sum. Coproduct in the category of commutative R-algebras is given by tensor product over R: in the case of commutative rings, one uses tensor product over $\mathbb{Z}$.

To give a morphism $A \oplus B \to C \times D$ is equivalent to giving morphisms $A \to C \times D$ and $B \to C \times D$, which, in turn, is equivalent to giving four morphisms, $f_{11} : A \to C$, $f_{21} : A \to D$, $f_{12} : B \to C$, and $f_{22} : B \to D$. The corresponding morphism $A \oplus B \to C \times D$ may be described as

$$\begin{bmatrix} \begin{bmatrix} f_{11} \\ f_{21} \end{bmatrix} & \begin{bmatrix} f_{12} \\ f_{22} \end{bmatrix} \end{bmatrix}$$

or

$$\begin{bmatrix} [\, f_{11} & f_{12}\,] \\ [\, f_{21} & f_{22}\,] \end{bmatrix},$$

but we shall prefer the notation

$$\begin{bmatrix} f_{11} & f_{12} \\ f_{21} & f_{22} \end{bmatrix}.$$

An object in a category is call an *initial object* if there is a unique morphism from it to every object in the category. Initial objects are unique up to unique isomorphism. The categories of sets and topological spaces have $\emptyset$ is an initial object. The category of commutative rings (recall that this means with multiplicative identity such the morphisms preserve the identity) has $\mathbb{Z}$ as an initial object. The 0 ring is not an initial object, because a homomorphism from it to a nonzero ring cannot preserve the identity. If we allow rings without an identity, dropping the condition that ring homomorphisms preserve the identity, then 0 is an initial object. The categories of groups, abelian groups, and R-modules have an initial object which is the trivial group $\{1\}$ in the first instance and the trivial abelian group or R-module 0 in the latter two instances.

An object of an category is called a *final* object if every object has a unique morphism to it. Final objects are unique up to unique isomorphism. An object is initial in $\mathcal{A}$ if and only if it is final in $\mathcal{A}^{\mathrm{op}}$. In the categories of sets and of topological spaces, a one point set or space is a final object. In the categories of groups, the trivial group is a final object. In the categories of rings, abelian groups, and R-modules, 0 is a final object.

If an object of a category is both initial and final it is called a *zero object*, and is often denoted 0. A zero object is unique up to unique isomorphism.

In a category with a 0 object we can define the notions of kernel, cokernel, image and coimage (although they need not exist). However, each of these will be a morphism, rather than an object. Thus, in the category of groups, a kernel for $f : G \to H$ will be a monomorphism $N \to G$ whose image is the set of elements of G that map to the identity. However, quite generally, if $A \to B$ has kernel $N \to A$, we shall also refer to the kernel, imprecisely, as N. Similar remarks apply to the other three terms.

Before defining these notions, we note that in a category with a zero object 0, we can define the zero morphism $A \to B$ as the composite morphism $A \to 0 \to B$. The composition of the zero morphism with any other morphism is again a zero morphism. The usual practice is to denote all of these morphisms 0, although one should keep in mind that 0 may denote either a zero object or one of many 0 morphisms with various domains and targets.

A *kernel* for $f : A \to B$ is a morphism $\iota : N \to A$ such that $f\iota = 0$ and for any morphism $g : X \to A$ such that $fg = 0$, there is a unique morphism $h : X \to N$ such that $g = \iota h$. That is, for all X the map $\mathrm{Hom}\,(X,\, N) \to \mathrm{Hom}\,(X,\, A)$ induced by composition with ι is a set-theoretic isomorphism of $\mathrm{Hom}\,(X,\, N)$ with $\{g \in \mathrm{Hom}\,(X,\, A) : fg = 0\}$. A kernel is automatically a monomorphism: if two maps h, h' from X to N agree upon composition with ι, they must be the same, or else $g = \iota h = \iota h'$ will have two different

factorizations through N. Kernels exist in the categories of groups, rings without identity, and R-modules, and coincide with the inclusion map of the subobject of elements that map to the identity in the first case and to 0 in the latter two cases into the domain.

A *cokernel* for $f : A \to B$ is a morphism $\pi : B \to Q$ such that $\pi f = 0$ and for any morphism $g : B \to Y$ such that $gf = 0$, there is a unique morphism $h : C \to Y$ such that $g = h\pi$. That is, for all Y the map $\mathrm{Hom}\,(Q, Y) \to \mathrm{Hom}\,(B, Y)$ induced by composition with π is a set-theoretic isomorphism of $\mathrm{Hom}\,(Q, Y)$ with $\{g \in \mathrm{Hom}\,(B, Y) : gf = 0\}$. A cokernel is automatically an epimorphism. Note that a kernel for a morphism is the same a cokernel for the corresponding morphism in $\mathcal{A}^{\mathrm{op}}$.

We can now define the coimage of f as the cokernel of the kernel of f and the image of f as the kernel of the cokernel of f. We use the notations $\mathrm{Ker}\,(f)$, $\mathrm{Coker}\,(f)$, $\mathrm{Coim}(f)$, and $\mathrm{Im}\,(f)$ for these. Each is a morphism. Note that the coimage of $f : A \to B$ is an epimorphism $A \to C$ that kills the kernel $\iota : N \to A$ under composition. Somewhat imprecisely, C is also referred to as the coimage. Likewise, the image is a monomorphism $C' \to B$ that is killed by composition with the cokernel $B \to Q$. Since

$$A \to C \to B \to Q$$

is 0, and

$$A \to C \xrightarrow{0} Q$$

is 0, we have that $C \to B \to Q$ is 0, and this implies that $C \to B$ factors $C \to C' \to B$ (we are using that $A \to C$ is an epimorphism). Thus, there is a canonical morphism from the target of the coimage to the domain of image, which we refer to somewhat imprecisely as a morphism from the coimage to the image.

Example. If $f : A \to B$ is an R-linear map of R-modules the kernel N is the usual notion. The coimage is A/N, which not only maps to the image $C' \subseteq B$, it is isomorphic with the image. C' is indeed the kernel of the epimorphism $B \to \mathrm{Coker}\,(f)$. However, in the category of rings without identity, the cokernel of a map $R \to S$ exists, but is the quotient of S by the ideal generated by the set-theoretic image of R. The target of the coimage is not isomorphic with the domain of the image.

In a category with zero object there is a canonical morphism $A \oplus B \to A \times B$, given in matrix notation by

$$\begin{bmatrix} 1_A & 0 \\ 0 & 1_B \end{bmatrix}.$$

This gives a natural transformation of functors of two variables. Notice that for the category of groups this natural transformation is not an isomorphism, but that it is for the categories of abelian groups and R-modules.

We now consider six properties for a category $\mathcal{A}$.

A_0 $\mathcal{A}$ has a 0 object.

A_1 All products and coproducts exist in $\mathcal{A}$.

A_2 The canonical natural transformation $A \oplus B \to A \times B$ given by

$$\begin{bmatrix} 1_A & 0 \\ 0 & 1_B \end{bmatrix}$$

is an isomorphism.

A_3 Every morphism that is both a monomorphism and an epimorphism is an isomorphism.

B_0 Every morphism has a kernel and a cokernel.

B_1 For every morphism f, the canonical morphism from the target of $\mathrm{Coim}(f)$ to the domain of $\mathrm{Im}\,(f)$ is an isomorphism.

A category that satisfies the axioms A_0, A_1, A_2 and A_3 is called an *additive category*. If, moreover, B_0 and B_1 hold, it is called an *abelian category*.

It is immediate from the axioms that if $\mathcal{A}$ is additive, so is $\mathcal{A}^{\mathrm{op}}$. Likewise, if $\mathcal{A}$ is abelian, so is $\mathcal{A}^{\mathrm{op}}$.

Math 615: Lecture of March 31, 2012

Assuming that the relevant coproducts exist, note that given $f : A \to C$ and $g : B \to D$ we get a morphism $[\,\iota_C f \quad \iota_D g\,] : A \oplus B \to C \oplus D$: we write $f \oplus g$ for this morphism. Dually, assuming that the relevant products exist, we have a morphism

$$\begin{bmatrix} f\pi_C \\ f\pi_D \end{bmatrix} \to A \times B,$$

which is denoted $f \times g$. Observe that if A, B, C, and D are abelian groups or R-modules then $(f \oplus g)(a \oplus b) = f(a) \oplus g(b)$, and if A, B, C, and D are sets, topological spaces, groups, rings, or R-modules, $(f \times g)(a, b) = \big(f(a), g(b)\big)$.

We also note there is a morphism $\Delta_A : A \to A \times A$ when the product exists, given by $\Delta_A = \begin{bmatrix} 1_A \\ 1_A \end{bmatrix}$: if A is a set, $\Delta_A(a) = (a, a)$. Δ_A is called the *diagonal morphism* for A. Dually, there is a morphism $\Sigma_B : B \oplus B \to B$ given by $\Sigma_B = [\,1_A \quad 1_A\,]$. If B is an abelian group or R-module, $\Sigma_B(b \oplus b') = b + b'$. Σ_B is called the *sum morphism* for B.

We next observe that in an additive category, for any two objects A, B, $\mathrm{Hom}\,(A, B)$ has the structure of an abelian group. Given f, $g \in \mathrm{Hom}\,(A, B)$ we want to define

$$f + g : A \to B.$$

Consider the following commutative diagram:

$$\begin{array}{ccccc} & & A \times A & \xrightarrow{\cong} & A \oplus A & & \\ & \overset{\Delta_A}{\nearrow} & \downarrow{\scriptstyle f\times g} & & \downarrow{\scriptstyle f\oplus g} & \searrow^{[f\ g]} & \\ A & & & & & & B \\ & \underset{[g]}{\searrow} & & & & \nearrow_{\Sigma_B} & \\ & & B \times B & \xrightarrow{\cong} & B \oplus B & & \end{array}$$

In this diagram, the horizontal isomorphisms are the inverses of

$$\begin{bmatrix} 1_A & 0 \\ 0 & 1_A \end{bmatrix}$$

and

$$\begin{bmatrix} 1_B & 0 \\ 0 & 1_B \end{bmatrix},$$

respectively. We define $f + g$ as the composite map $A \to B$ obtained from any of the paths traversing this diagram.

The fact that this notion of addition on $\mathrm{Hom}\,(A,\, B)$ gives a commutative associative operation with additive identity 0 already follows from the conditions A_0, A_1, and A_2 in the definition of additive category. It also follows that composition on either side distributes over addition when defined.

Condition A_3 implies the existence of inverses under addition, so that one gets an abelian group. The idea of the proof is as follows. Given objects A, B and $f \in \mathrm{Hom}\,(A,\, B)$, identify

$$A \oplus B \cong A \times B,$$

and consider the morphism

$$\theta = \begin{bmatrix} 1_A & 0 \\ f & 1_B \end{bmatrix} : A \oplus B \to A \oplus B$$

It is straightforward to verify that compositions of maps described by matrices are given by "matrix multiplication," where one makes an automatic identification of the direct sums and the direct products that arise. One shows that θ is both a monomorphism and an epimorphism, and then it follows from A_3 that it has an inverse. An easy calculation shows that the inverse must have the form

$$\begin{bmatrix} 1_A & 0 \\ g & 1_B \end{bmatrix}$$

for $g \in \mathrm{Hom}\,(A,\, B)$ where $f + g = 0$.

A functor F from one additive category $\mathcal{A}$ to another $\mathcal{A}'$, whether covariant or contravariant, is called an *additive functor* if it preserves coproducts and products. It is then automatic that it preserves addition of maps, e.g., in the covariant case that

$$F : \mathrm{Hom}_{\mathcal{A}}(A,\, B) \to \mathrm{Hom}_{\mathcal{A}'}\big(F(A),\, F(B)\big)$$

is a homomorphism of abelian groups for all objects A, B of $\mathcal{A}$.

In an abelian category we can define exact sequences and homology. For example

$$M_2 \xrightarrow{f} M_1 \xrightarrow{g} M_0$$

is exact at M_1 provided that $gf = 0$ and the induced monomorphism from the target of $\mathrm{Im}\,(f)$ to the domain of $\mathrm{Ker}\,(g)$ is an isomorphism. Thus, if we write $B \to M_1$ for $\mathrm{Im}\,(f)$ and $Z \to M_1$ for $\mathrm{Ker}\,(g)$, both of which are monomorphisms, the condition that $gf = 0$ is equivalent to the condition that $B \to M_1$ factor

$$B \xrightarrow{\alpha} Z \to M_1.$$

The condition for exactness is that α be an isomorphism. In general, when $gf = 0$, we can define the homology at M_1 as $\mathrm{Coker}\,(\alpha)$, and it is 0 iff the sequence is exact at M_1. We can define complexes as in the category of R-modules: the composition of any two consecutive maps is 0. We then have the notion of the homology or cohomology of a complex defined in any abelian category.

A functor from an abelian category $\mathcal{A}$ to another $\mathcal{A}'$, whether covariant or contravariant, is called an *exact functor* if it preserves exactness.

The following two results show that our abstract notion of abelian category is not so far removed from categories of abelian groups and R-modules. A proof the first theorem may be found in [P. Freyd, *Abelian Categories*, Harper and Row, 1964], and also in [B. Mitchell, *Theory of Categories*, Academic Press, 1965], where the second theorem is also proved. A readable introduction to this material that is more detailed than our treatment here (but without proofs of the embedding theorems) may be found in [H. Bass, *Algebraic K-Theory*, Benjamin, 1968].

Theorem (P. Freyd, S. Lubkin, A. Grothendieck). *For any abelian category $\mathcal{A}$ whose objects form a set, there is an exact covariant functor F from $\mathcal{A}$ into the category of abelian groups that is injective on both objects and modules.*

This functor necessarily will preserve products, direct sums, kernels, cokernels, images, and coimages. One consequence of this result is that results like the five lemma, the snake lemma, the double complex lemma, and the basic theory of spectral sequences that are typically proved by a diagram chase involving elements all follow for arbitrary abelian categories: one can "pretend" that the object in an arbitrary abelian category have elements.

The second theorem is quite a bit sharper:

Theorem (B. Mitchell). *For any abelian category $\mathcal{A}$ whose objects form a set, there is a not necessarily commutative ring with identity R and an exact covariant functor G from $\mathcal{A}$ into the category of R-modules that is injective on both objects and modules, and whose image is a full subcategory of the category of R-modules.*

Math 615: Lecture of April 2, 2012

It is easy to verify that $\mathrm{Hom}\,(M, \_\,)$ and $\mathrm{Hom}\,(\_\,, N)$ have the same exactness properties in any abelian category that they do in the category or R-modules, i.e., if

$$0 \to N_0 \to N_1 \to N_2$$

is exact then

$$0 \to \mathrm{Hom}\,(M,\, N_0) \to \mathrm{Hom}\,(M,\, N_1) \to \mathrm{Hom}\,(M,\, N_2)$$

is exact (we have that $\mathrm{Hom}\,(M,\, N_0) \to \mathrm{Hom}\,(M,\, N_1)$ is injective by the definition of monomorphism applied to $N_0 \to N_1$, and exactness in the middle is essentially the universal mapping property for the kernel $N_0 \to N_1$), while if

$$M_0 \to M_1 \to M_2 \to 0$$

is exact then

$$0 \to \mathrm{Hom}\,(M_2,\, N) \to \mathrm{Hom}\,(M_1,\, N) \to \mathrm{Hom}\,(M_0,\, N)$$

is exact similarly.

An object P of an abelian category is called *projective* if, equivalently, $\mathrm{Hom}\,(P,\, \_\,)$ is exact, or if whenever $h : M \to N$ is an epimorphism and $f : P \to N$, there is a morphism $g : P \to M$ such that $hg = f$. An abelian category is said *to have enough injectives* if for every object M there exists a projective object P and an epimorphism $P \to M$. In this case we can construct projective resolutions for M: if $P_0 \to M$ is an epimorphism and

$$P_i \to P_{i-1} \to \cdots \to P_1 \to P_0 \to M \to 0$$

has been constructed, with the P_j projective, so as to be exact at M, P_0, P_1, $\ldots$, P_{i-1}, we can continue by choosing an epimorphism from a projective P_{i+1} to $Z_i = \mathrm{Ker}\,(P_i \to P_{i-1})$. We can even define Z_{i-1} to be an ith syzygy of M. Given an acyclic left complex

$$\cdots \to N_i \to \cdots \to N_1 \to N_0 \to 0$$

with augmentation N (so that

$$\cdots \to N_i \to \cdots \to N_1 \to N_0 \to N \to 0$$

is exact) and a projective complex $P_\bullet$ with augmentation M, a morphism $M \to N$ lifts to a morphism $P_\bullet \to N_\bullet$ that is unique up to homotopy.

The theory of injectives is simply the dual theory: an injective in $\mathcal{A}$ is the same as a projective in $\mathcal{A}^{\mathrm{op}}$. However, we make the theory explicit. An object E of an abelian category is called *injective* if, equivalently, $\mathrm{Hom}\,(\,\_\,,\, E)$ is exact, or if whenever $h : M \to N$ is a monomorphism and $f : M \to E$, there is a morphism $g : N \to E$ such that $gh = f$. An abelian category is said *to have enough injectives* if for every object M there exists an injective object E and a monomorphism $M \to E$. In this case we can construct injective resolutions for M: if $M \to E_0$ is a monomorphism and

$$0 \to M \to E_0 \to E_1 \to \cdots \to E_{i-1} \to E_i$$

has been constructed, with the E_j injective, so as to be exact at M, E_0, E_1, $\ldots$, E_{i-1}, we can continue by choosing a monomorphism from $C_i = \mathrm{Coker}\,(E_{i-1} \to E_i)$ to an injective

E_{i+1}. We can even define C_{i-1} to be an ith cosyzygy of M. Given an acyclic right complex

$$0 \to M_0 \to M_1 \to \cdots \to M_i \to \cdots$$

with augmentation M (so that

$$0 \to M \to M_0 \to M_1 \to \cdots \to M_i \to \cdots$$

is exact) and an injective right complex $E^\bullet$ with augmentation N, a morphism $N \to M$ lifts to a morphism of $M^\bullet \to E^\bullet$ that is unique up to homotopy.

We next want to define derived functors of $F : \mathcal{A} \to \mathcal{B}$. For simplicity we give definitions only for covariant functors: contravariant functors can simply be regarded as covariant functors to $\mathcal{B}^{\mathrm{op}}$.

A functor $F : \mathcal{A} \to \mathcal{B}$ between abelian categories is called *left exact* if whenever

$$0 \to M_0 \to M_1 \to M_2$$

is exact, so is

$$0 \to F(M_0) \to F(M_1) \to F(M_2).$$

If F is left exact and $\mathcal{A}$ has enough injectives, we define the *right derived functors* R^nF as follows: $R^nF(A) = H^n(F(E^\bullet))$ where $E^\bullet$ is an injective resolution of A. Given two different resolutions one has morphisms in both directions, unique up to homotopy, and their compositions in either order are homotopic to the identity on the relevant injective resolution. The homotopies persist when one applies F, and homotopic morphisms of complexes induce the same morphism of cohomology. Thus, $R^nF(A)$ is independent of the resolution. It vanishes for $n < 0$, while

$$R^0F(A) \cong \mathrm{Ker}\left(F(E_0) \to F(E_1)\right)$$

may be identified canonically with $F(A)$: by the left exactness of F, we have that

$$0 \to F(A) \to F(E_0) \to F(E_1)$$

is exact.

A morphism of objects lifts to a morphism of injective resolutions, and so $R^\bullet(F)$ is a covariant functor. Given a short exact sequence of modules

$$0 \to M_0 \to M_1 \to M_2 \to 0$$

one can choose injective resolutions $E_0^\bullet$ of M_0 and $E_2^\bullet$ of M_2, and then construct a resolution of M_1 in which the then nth object is $E_0^n \oplus E_2^n$. Just to get started, we have a morphism $M_1 \to M_2 \to E_2^0$, and the morphism $M_0 \to E_0^0$ extends to a morphism $M_1 \to E_0^0$. This gives a morphism

$$M_1 \to E_0^0 \times E_2^0 \cong E_0^0 \oplus E_2^0.$$

One proceeds further by replacing

$$0 \to M_0 \to M_1 \to M_2 \to 0$$

by the sequence of cokernels. For the corresponding construction for projective resolutions see p. 4 of the Lecture Notes for February 6, which was used to give one of the proofs that there is a long exact sequence for Tor: that case is formally dual to this one. Applying F and using the snake lemma gives a long exact sequence for cohomology that is functorial in the short exact sequence:

$$0 \to F(M_0) \to F(M_1) \to F(M_2) \to R^1F(M_0) \to R^1F(M_1) \to R^1F(M_2) \to$$

$$\cdots \to R^nF(M_0) \to R^nF(M_1) \to R^nF(M_2) \to R^{n+1}F(M_0) \to \cdots$$

One may similarly define the left derived functors of a right exact functor if the abelian category has enough projectives. The remarks of the preceding two paragraphs apply without essential change. This theory is the dual theory: i.e., it is the theory of right derived functors for $\mathcal{A}^{\mathrm{op}}$. The details are left to the reader.

In an abelian category with enough injectives we may therefore define $\mathrm{Ext}^n(M, N)$ as $R^nF(N)$ where $F = \mathrm{Hom}\,(M, \_)$. If there are enough projectives we may define $\mathrm{Ext}^n(M, N)$ as $L^nG(M)$, where $G = \mathrm{Hom}\,(\_, N)$ taking values in the opposite of the category of R-modules (so that we may think of it as covariant). However, in a small abelian category we may also define Ext even if there are neither enough injective nor enough projectives, using the analogue of the Yoneda definition that we discussed for R-modules, in which the elements of $\mathrm{Ext}^n_R(M, N)$ correspond to equivalence classes of exact sequences

$$0 \to N \to B_{n-1} \to \cdots \to B_1 \to B_0 \to M \to 0.$$

Of course, working in the category of R-modules, we have that

$$\mathrm{Tor}^R_n(M, N) = L^nF(N) \cong L^nG(M),$$

where F is $M \otimes_R \_$, and G is $\_ \otimes_R N$.

The Yoneda pairing generalizes to a Yoneda-Cartier pairing. Let $\mathcal{A}$ have enough injectives and $\mathcal{B}$ be arbitrary. Let $F : \mathcal{A} \to \mathcal{B}$ be a left exact functor. Then there is pairing

$$R^pF(A) \times \mathrm{Ext}^q(A, B) \to R^{p+q}F(B)$$

for all objects A and B. This pairing is compatible with the connecting homomorphisms arising from short exact sequences. To see this, choose injective resolutions $E^\bullet$ of A and $I^\bullet$ of B. An element of $\mathrm{Ext}^q(A, B)$ is represented by an element of $\mathrm{Hom}\,(A, I^q)$ that is killed when one composes with $I^q \to I^{q+1}$: it therefore factors through $\mathrm{Im}\,(I^{q-1} \to I^q)$:

call this object C^q, so that we may think of an element of $\mathrm{Ext}^q(A,\, B)$ as represented by a map $\phi : A \to C^q$. Then ϕ lifts to a morphism of complexes:

$$\begin{array}{ccccccccccc}
C^q & \longrightarrow & I^q & \longrightarrow & I^{q+1} & \longrightarrow & \cdots & \longrightarrow & I^{p+q} & \longrightarrow & \cdots \\
\uparrow & & \uparrow & & \uparrow & & & & \uparrow & & \\
A & \longrightarrow & E^0 & \longrightarrow & E^1 & \longrightarrow & \cdots & \longrightarrow & E^p & \longrightarrow & \cdots
\end{array}$$

and so induces a morphism $E^p \to I^{p+q}$, unique up to homotopy, for all $p \geq 0$. This morphism induces morphisms $F(E^p) \to F(I^{p+q})$ which in turn give morphisms

$$R^pF(A) \cong H^p\big(F(E^\bullet)\big) \to H^{p+q}\big(F(I^\bullet)\big) \cong R^{p+q}F(B).$$

This gives a morphism

$$\mathrm{Ext}^q(A,\, B) \to \mathrm{Hom}\left(R^pF(A),\, R^{p+q}F(B)\right)$$

and, hence, a pairing

$$R^pF(A) \times \mathrm{Ext}^q(A,\, B) \to R^{p+q}F(B).$$

If $\mathcal{A} = \mathcal{B}$ and F is $\mathrm{Hom}\,(C,\, \_\,)$, we get a pairing

$$\mathrm{Ext}^p(C,\, A) \times \mathrm{Ext}^q(A,\, B) \to \mathrm{Ext}^{p+q}(C,\, A)$$

which agrees with the Yoneda pairing discussed earlier in case $\mathcal{A}$ is the category of R-modules.

Finally, we discuss the spectral sequence of a composite functor. Let $\mathcal{A}$ be an abelian category with enough injectives and $0 \to \mathcal{K}^0 \to \mathcal{K}^1 \to \cdots$ a right complex.

By a *Cartan-Eilenberg* resolution of $\mathcal{K}^\bullet$ we mean a cohomological double complex of injective objects $E^{\bullet\bullet}$ with the following properties:

(1) For all j, the j th column $E^{\bullet,j}$ is an injective resolution of $\mathcal{K}_j$.

(2) For all i, j, if $Z^{i,j}$ denotes the cocycles in $E^{i,j}$ with respect to $E^{i,j} \to E^{i+1,j}$, then $Z^{\bullet,j}$ is an injective resolution of the cocycles Z^j in $\mathcal{K}^j$.

(3) For all i, j, if $B^{i,j}$ denotes the coboundaries in $E^{i,j}$ with respect to $E^{i-1,j} \to E^{i,j}$, then $B^{\bullet,j}$ is an injective resolution of the coboundaries B^j in $\mathcal{K}^j$.

(4) For all i, j, if $H_{\mathrm{II}}^{i,\,j}(E^{\bullet\bullet})$ denotes the cohomology $Z^{i,j}/B^{i,j}$ of the i th row at the j th spot, then $H_{\mathrm{II}}^{\bullet,\,j}(E^{\bullet\bullet})$ is an injective resolution of $H^j(\mathcal{K}^\bullet)$.

Cartan-Eilenberg resolutions exist. For every j choose injective resolutions $E^\bullet_{H^j}$ of $H^j(\mathcal{K}^\bullet)$ and $E^\bullet_{B^j}$ of B_j. We for all j we have short exact sequences

$$0 \to B^j \to Z^j \to H^j(\mathcal{K}^\bullet) \to 0$$

from which we can construct injective resolutions $E^\bullet_{Z^j}$ of the Z^j, where $E^i_{Z^j} = E^i_{H^j} \oplus E^i_{B^j}$ as in the paragraph on the second page of today's Lecture Notes describing the proof that there is a long exact sequence for derived functors. Note, however, that the morphisms in the resolution require choices of certain extension morphisms. Then, from the exact sequences

$$0 \to Z^j \to \mathcal{K}^j \to B^{j+1} \to 0$$

we also get injective resolutions $E^\bullet_{\mathcal{K}^j}$ of the objects $\mathcal{K}^j$ by the construction just described, where

$$E^i_{\mathcal{K}^j} = E^i_{Z^j} \oplus E^i_{B^{j+1}} = E^i_{H^j} \oplus E^i_{B^j} \oplus E^i_{B^{j+1}}.$$

The morphism $E^i_{\mathcal{K}^j} \to E^i_{\mathcal{K}^{j+1}}$ kills $E^i_{H^j} \oplus E^i_{B^j}$ and morphisms $E^i_{B^{j+1}}$ to

$$E^i_{H^{j+1}} \oplus E^i_{B^{j+1}} \oplus E^i_{B^{j+2}}$$

via the obvious direct sum injection.

A key point about Cartan-Eilenberg resolutions is that if we apply any additive functor to the rows, the action of that functor commutes with the calculation of cocycles, coboundaries, and cohomology: all of the modules involved in any of the short exact sequences relating these are injective, and the sequences are therefore split.

Theorem (spectral sequence of a composite functor). *Let $G : \mathcal{A} \to \mathcal{B}$ and $F : \mathcal{B} \to \mathcal{C}$ where $\mathcal{A}$ and $\mathcal{B}$ have enough injectives, F is left exact and G is an additive functor that takes injectives to F-acyclic objects (that is, if I is injective in $\mathcal{B}$, then $R^iF\big(G(I)\big) = 0$ for $i \geq 1$). Then for all objects A in $\mathcal{A}$ there is a spectral sequence*

$$R^pF(R^qG(A)) \underset{p}{\Longrightarrow} R^{p+q}(F \circ G)(A).$$

Proof. Choose an injective resolution $I^\bullet$ of A in $\mathcal{A}$. Then $G(I^\bullet)$ is a right complex in $\mathcal{B}$ and has a Cartan Eilenberg resolution $E^{\bullet\bullet}$. All of the rows can be decomposed into split short exact sequences of injectives relating cohomology, coboundaries, cocycles, and objects. Now apply F to the $E^{\bullet\bullet}$. The cohomology of the column corresponding to $j = q$ is the cohomology of F applied to an injective resolution of $G(I^q)$ which vanishes except in degree 0, where it is $FG(I^q)$: the higher terms vanish because $G(I^q)$ is F-acyclic. Thus, the iterated cohomology $H_{\mathrm{I}}H_{\mathrm{II}}$ in degree n is the same as the cohomology of the total complex and is $R^n(F \circ G)(A)$. On the other hand if we fix the row corresponding to $i = p$ the cohomology is is simply $F(E^p_{H_j})$, and then taking cohomology of columns gives that $H_{\mathrm{I}}H_{\mathrm{II}}$ is $R^pF(R^qG(A))$. Thus, the spectral sequence we seek is simply one of the spectral sequences associated with the double complex. $\square$

While we shall return to the subject of spectral sequences, and, in particular, apply them, we next want to aim towards proving the result that over a regular Noetherian ring R, if M and N are finitely generated R-modules then whenever $\mathrm{Tor}^R_i(M, N)$ vanishes so does $\mathrm{Tor}^R_j(M, N)$ for all $j \geq i$. Note that if there is a counterexample, we can localize at a prime in the support of $\mathrm{Tor}^R_j(M, N)$: Tor commutes with localization, and with flat base change more generally. Therefore, there is no loss of generality in assuming that the ring

is local. Likewise, we may complete, and so we may assume that R is a complete regular local ring. If R contains a field, we know that such a ring has the form $K[[x_1, \ldots, x_d]]$, where K is a field and $x_1, \ldots, x_d$ are formal indeterminates. In the equicharacteristic case the idea of the proof is to show that the Tors may be viewed as Koszul homology. If we were working over a polynomial ring $R = K[x_1, \ldots, x_d]$ instead, we could consider $M \otimes_K N$ as a module over $S = R \otimes_K R$ which is a polynomial ring over K in the $2n$ variables $x_1 \otimes 1, \ldots, x_n \otimes 1, 1 \otimes x_1, \ldots, 1 \otimes x_n$, which we rename $x_1, \ldots, x_n, y_1, \ldots, y_n$. It turns out that $\operatorname{Tor}_i^R(M, N)$ may be identified with $\operatorname{Tor}_i^S(M \otimes_K N, S/I)$ where $I = (x_1 - y_1, \ldots, x_d - y_d)S$ is generated by a regular sequence. Let $z_j = x_j - y_j$, and let $\underline{z} = z_1, \ldots, z_d$. A Koszul complex can be used to resolve S/I and calculate the values of Tor, and we have that

$$\operatorname{Tor}_i^R(M, N) \cong \operatorname{Tor}_i^S(M \otimes_K N, S/I) \cong H_i(\underline{z}; M \otimes_K N).$$

The result on vanishing of Tor then follows because we already know the corresponding fact for Koszul homology.

The complete local case can be handled by a similar technique. However, $R \otimes_K R$ is not Noetherian: one can define a complete version of the tensor product, denoted $R \widehat{\otimes}_K R$, which turns out to be $\cong K[[x_1, \ldots, x_d, y_1, \ldots, y_d]]$ when $R = K[[x_1, \ldots, x_d]]$, and one has a completed module $M \widehat{\otimes}_K N$ over $R \widehat{\otimes}_K R$ as well. One can now imitate the proof above, and one obtains that $\operatorname{Tor}_i^R(M, N) \cong H_i(\underline{z}; M \widehat{\otimes}_K N)$.

We shall do these arguments in detail later. Notice that this method gives the result when the ring contains a field. When that is not assumed, the argument becomes more complicated. One needs to understand the structure of complete local rings in the case when the ring does not contain a field, including the structure of complete regular local rings. One also needs some spectral sequence arguments.

Math 615: Lecture of April 4, 2012

Consider a complete local ring (R, m, K). If K has characteristic 0, then $\mathbb{Z} \to R \to K$ is injective, and $\mathbb{Z} \subseteq R$. Moreover, no element of $W = \mathbb{Z} - \{0\}$ is in m, since no element of W maps to 0 in $R/m = K$, and so every element of $\mathbb{Z} - \{0\}$ has an inverse in R. By the universal mapping property of localization, we have a unique map of $W^{-1}\mathbb{Z} = \mathbb{Q}$ into R, and so R is an equicharacteristic 0 ring. We already know that R has a coefficient field. We also know this when R has prime characteristic $p > 0$, i.e., when $\mathbb{Z}/p\mathbb{Z} \subseteq R$.

We now want to develop the structure theory of complete local rings when R need not contain a field. From the remarks above, we only need to consider the case where K has prime characteristic $p > 0$, and we shall assume this in the further development of the theory. The coefficient rings that we are about to describe also exist in the complete separated quasi-local case, but, for simplicity, we only treat the Noetherian case.

We shall say that V is a *coefficient ring* if it is a field or if it is complete local of the form (V, pV, K), where K has characteristic $p > 0$. If R is complete local we shall say

that V is a coefficient ring for R if V is a coefficient ring, $V \subseteq R$ is local, and the induced map of residue fields is an isomorphism. We shall prove that coefficient rings always exist.

In the case where the characteristic of K is $p > 0$, there are three possibilities. It may be that $p = 0$ in R (and V), in which case V is a field: we have already handled this case. It may be that p is not nilpotent in V: in this case it turns out that V is a Noetherian discrete valuation domain (DVR), like the p-adic integers. Finally, it may turn out that p is not zero, but is nilpotent. Although it is not obvious, we will prove that in this case, and when V is a field of characteristic $p > 0$, V has the form W/p^nW where $n \geq 1$ and W is a DVR with maximal ideal pW.

We first note:

Lemma. *Let (R, m, K) be local with K of prime characteristic $p > 0$. If $r, s \in R$ are such that $r \equiv s \bmod m$, and $n \geq 1$ is an integer, then for all $N \geq n - 1$, with $q = p^N$ we have that $r^q \cong s^q \bmod m^n$.*

Proof. This is clear if $n = 1$. We use induction. If $n > 1$, we know from the induction hypothesis that $r^q \equiv y^q \bmod m^N$ if $N \geq n - 2$, and it suffices to show that $r^{pq} \equiv y^{pq} \bmod m^{N+1}$. Since $r^q = s^q + u$ with $u \in m^N$, we have that $r^{pq} = (s^q + u)^p = s^{pq} + puw + u^p$, where puw is a sum of terms from the binomial expansion each of which has the form $\binom{pq}{j} s^j u^{p-j}$ for some j, $1 \leq j \leq p - 1$, and in each of these terms the binomial coefficient is divisible by p. Since $u \in m^N$ and $p \cdot 1_R \in m$, $puw \in m^{N+1}$, while $u^p \in m^{Np} \subseteq m^{N+1}$ as well. $\square$

Recall that a p-base for a field K of prime characteristic $p > 0$ is a maximal set of elements Λ of $K - K^p$ such that for every finite subset of distinct elements $\lambda_1, \ldots, \lambda_h$ of Λ, $[K(\lambda_1, \ldots, \lambda_h) : K] = p^h$. K has a p-base by Zorn's lemma. The empty set is a p-base for K if and only if K is perfect. The set of monomials in the the elements of the p-base Λ such that every exponent is at most $p-1$ is a K^p-basis for K over K^p, and, more generally, $(*)$ for every $q = p^N$, the set of monomials in the elements of Λ such that every exponent is at most $q - 1$ is a basis for K over $K^q = \{a^q : a \in K\}$. See the third and fourth pages of the Lecture Notes from January 11.

The following Proposition, which constructs coefficient rings when the maximal ideal of the ring is nilpotent, is the heart of the proof of the existence of coefficient rings. Before giving the proof, we introduce the following notation, which we will use in another argument later. Let x, y be indeterminates over $\mathbb{Z}$. Let q be a power of p, a prime. Then $(x + y)^q - x^q - y^q$ is divisible by p in $Z[x, y]$, since the binomial coefficients that occur are all divisible by p, and we write $G_q(x, y) \in \mathbb{Z}[x, y]$ for the quotient, so that $(x + y)^q = x^q + y^q + pG_q(x, y)$.

Proposition. *Suppose that (R, m, K) is local where K has characteristic $p > 0$, and that $m^n = 0$. Choose a p-base Λ for K, and a lifting of the p-base to R: that is, for every $\lambda \in \Lambda$ choose an element $\tau_\lambda \in R$ with residue λ. Let $T = \{\tau_\lambda : \lambda \in \Lambda\}$. Then R has a unique coefficient ring V that contains T. In fact, suppose that we fix any sufficiently large power $q = p^N$ of p (in particular, $N \geq n - 1$ suffices) and let S_N be the set of all expressions of the form $\sum_{\mu \in \mathcal{M}} r_\mu^q \mu$, where the $\mathcal{M}$ is a finite set of mutually distinct monomials in*

the elements of T such that the exponent on every element of T is $\leq q-1$ and every $r_\mu^q \in R^q = \{r^q : r \in R\}$. Then we may take

$$V = S_N + pS_N + p^2S_N + \cdots + p^{n-1}S_N,$$

which will be the same as the smallest subring of R containing R^q and T.

Before giving the proof, we note that it is not true in general that R^q is closed under addition, and neither is S_N, but we will show that for large N, V is closed under addition and multiplication, and this will imply at once that it is the smallest subring of R containing R^q and T.

Proof of the Proposition. We first note if $r \equiv s \bmod m$ then $r^q \equiv s^q \bmod m^n$ if $N \geq n-1$, by the preceding Lemma. Therefore R^q maps bijectively onto $K^q = \{a^q : a \in K\}$ when we take residue classes mod m. By the property (*) of p-bases, the residue class map $R \to K$ sends S_N bijectively onto K.

Suppose that W is a coefficient ring containing T. For each $r \in R$, if $w \equiv r \bmod m$, then $w^q = r^q$. Thus, $R^q \subseteq W$. Then $S_N \subseteq W$, and so $V \subseteq W$. Now consider any element $w \in W$. Since S_n contains a complete set of representatives of elements of K, every element of W has the form $\sigma_0 + u$ where $u \in m \cap W = pW$, and so $w = \sigma_0 + pw_1$. But we may also write w_1 in this way and substitute, to get an expression $w = \sigma_0 + p\sigma_1 + p^2w_2$, where σ_0, $\sigma_1 \in S_n$ and $w_2 \in W$. Continuing in this way, we find, by a straightforward induction, that

$$W = S_N + pS_N + \cdots + p^jS_N$$

for every $j \geq 1$. We may apply this with $j = n$ and note that $p^n = 0$ to conclude that $W = V$. Thus, if there is a coefficient ring, it must be V. However, at this point we do not even know that V is closed under addition.

We next claim that V is a ring. Let V' be the closure of V under addition. Then we can see that V' is a ring, since, by the distributive law, it suffices to show that the product of two elements $p^ir^q\mu$ and $p^jr'^q\mu'$ has the same form. The point is that $\mu\mu'$ can be rewritten in the form $\nu^q\mu''$ where μ'' has all exponents $\leq q-1$, and $p^{i+j}(rr'\nu)^q\mu''$ has the correct form. Thus, V' is the smallest ring that contains R^q and T.

We next prove that V itself is closed under addition. We shall prove by reverse induction on j that $p^jV = p^jV'$ for all j, $0 \leq j \leq n$. The case that we are really aiming for is, of course, where $j = 0$. The statement is obvious when $j = n$, since $p^nV' = 0$. Now suppose that $p^{j+1}V = p^{j+1}V'$. We shall show that $p^jV = p^jV'$, thereby completing the inductive step. Since p^jV' is spanned over $p^{j+1}V' = p^{j+1}V$ by p^jS_n, it will suffice to show that given any two elements of p^jS_n, their sum differs from an element of p^jS_n by an element of $p^{j+1}V' = p^{j+1}V$. Call the two elements

$$v = p^j \sum_{\mu \in \mathcal{M}} r_\mu^q \mu$$

and

$$v' = p^j \sum_{\mu \in \mathcal{M}} r'_m u^q \mu,$$

where $r_\mu, r'_m u \in R$ and $\mathcal{M}$ is a finite set of monomials in elements of T, with exponents $\leq q-1$, large enough to contain all those monomials that occur with nonzero coefficient in the expressions for v and v'. Since S_n gives a complete set of representatives of K and r^q only depends on what r is mod m, we may assume that all of the r_μ and r'_μ are elements of S_n. Let

$$v'' = p^j \sum_{\mu \in \mathcal{M}} (r_\mu + r'_\mu)^q \mu.$$

Then

$$v'' - v - v' = p^j \sum_{\mu \in \mathcal{M}} pG_q(r_\mu, r'_\mu)\mu = p^{j+1} \sum_{\mu \in \mathcal{M}} G_q(r_\mu, r'_\mu)\mu \in p^{j+1}V',$$

as required, since all the r_μ, $r'_\mu \in S_N$ and V' is a ring. This completes the proof that $V' = V$, and so V is a subring of R.

We have now shown that V is a subring of R, and that it is the only possible coefficient ring. It is clear that $pV \subseteq m$, while an element of $V - pV$ has nonzero image in K: its constant term in S_N is nonzero, and S_N maps bijectively to K. Thus, $m \cap V = pV$, and we know that $V/pV \cong K$, since S_N maps onto K. It follows that pV is a maximal ideal of V generated by a nilpotent, and so pV is the only prime ideal of V. Any nonzero element of the maximal ideal can be written as $p^t u$ with t as large as possible (we must have that $t < n$), and then u must be a unit. Thus, every nonzero element of V is either a unit, or a unit times a power of p. It follows that every nonzero proper ideal is generated by p^k for some positive integer k, where k is as small as possible such that p^k is in the ideal. It follows that V is a principal ideal ring. Thus, V is a Noetherian local ring, and, in fact, an Artin local ring. $\square$

Math 615: Lecture of April 6, 2012

Theorem. *Let K, K' be isomorphic fields of characteristic $p > 0$ and let $g : K \to K'$ be the isomorphism. Let (V, pV, K) and (V', pV', K') be two coefficient rings of the same characteristic, $p^n > 0$. We shall also write a' for the image of $a \in K$ under g. Let Λ be a p-base for K and let $\Lambda' = g(\Lambda)$ be the corresponding p-base for K'. Let T be a lifting of Λ to V and let T' be a lifting of Λ' to T'. We have an obvious bijection $\widetilde{g} : T \to T'$ such that if $\tau \in T$ lifts $\lambda \in \Lambda$ then $\widetilde{g}(\tau) \in T'$ lifts $\lambda' = g(\lambda)$. Then $\widetilde{g}$ extends uniquely to an isomorphism of V with V' that lifts $g : K \to K'$.*

Proof. As in the proof of the Proposition in the Lecture Notes of April 4 showing the existence of a coefficient ring when $m^n = 0$, we choose $N \geq n-1$ and let $q = p^N$. For every element $a \in K$ there is a unique element $\rho_a \in V^q$ that maps to $a^q \in K^q$. Similarly, there is a unique element $\rho'_{a'} \in V'^q$ that maps to a'^q for every $a' \in K'$. If there is an isomorphism $V \cong V'$ as stated, it must map $\rho_a \to \rho'_{a'}$ for every $a \in K$. Said otherwise, we have an obvious bijection $V^q \to V'^q$, and $\widetilde{g}$ must extend it. Just as in the proof of the Proposition, we can define $S_N = S$ to consist of linear combinations of distinct monomials in T such that in every monomial, every exponent is $\leq q-1$, and such that every coefficient

is in V^q. Then S will map bijectively onto K. We define $S'_N = S' \subseteq V'$ analogously. Since S' maps bijectively onto K', we have an obvious bijection $\widetilde{g} : S \to S'$. We use σ' for the element of S' corresponding to $\sigma \in S$.

Every element $v \in V$ must have the form $\sigma_0 + pv_1$ where σ_0 is the unique element of S that has the same residue as v modulo pV. Continuing this way, as in the proof of the previous Proposition, we get a representation

$$v = \sigma_0 + p\sigma_1 + p^2\sigma_2 + \cdots + p^{n-1}\sigma_{n-1}$$

for the element $v \in V$, where the $\sigma_j \in S$. We claim this is unique. Suppose we have another such representation

$$v = \sigma_0^* + p\sigma_1^* + \cdots + p^{n-1}\sigma_{n-1}^*.$$

Suppose that $\sigma_i = \sigma_i^*$ for $i < j$. We want to show that $\sigma_j = \sigma_j^*$ as well. Working in $V/p^{j+1}V$ we have that $\sigma_j p^j = \sigma_{j+1} p^j$, i.e., that $(\sigma_j - \sigma_j^*)$ kills p^j working mod p^{j+1}. By part (a) of the Lemma that follows just below, we have that $\sigma_j - \sigma_j^* \in pV$, and so σ_j and σ_j^* represent the same element of $K = V/pV$, and therefore are equal.

Evidently, any isomorphism $V \cong V'$ satisfying the specified conditions must take

$$\sigma_0 + p\sigma_1 + \cdots + p^{n-1}\sigma_{n-1}$$

to

$$\sigma'_0 + p\sigma'_1 + \cdots + p^{n-1}\sigma'_{n-1}.$$

To show that this map really does give an isomorphism of V with V' one shows simultaneously, by induction on j, that addition is preserved in p^jV, and that multiplication is preserved when one multiplies elements in p^hV and p^iV such that $h + i \geq j$. For every element $a \in K$, let σ_a denote the unique element of S that maps to a. Note that we may write ρ_a as σ_a^q, since σ_a has residue a mod pV.

Now,

$$p^j\rho_a\mu + p^j\rho_b\mu = p^j(\sigma_a^q + \sigma_b^q)\mu = p^j\big((\sigma_a + \sigma_b)^q - pG_q(\sigma_a, \sigma_b)\big),$$

where $G_q(x, y) \in \mathbb{Z}[x, y]$ is such that $(x + y)^q = x^q + y^q + pG_q(x, y)$. Since $\sigma_a + \sigma_b$ has residue $a + b$ mod pV, we have that $(\sigma_a + \sigma_b)^q = \rho_{a+b}$, and it follows that

$$p^j\rho_a\mu + p^j\rho_b\mu = p^j\rho_{a+b}\mu - p^{j+1}G_q(\sigma_a, \sigma_b)\mu.$$

We have similarly that

$$p^j\rho'_{a'}\mu + p^j\rho'_{b'}\mu' = p^j\rho'_{a'+b'}\mu' - p^{j+1}G_q(\sigma'_{a'}, \sigma'_{b'})\mu',$$

and it follows easily that addition is preserved by our map $p^jV \to p^jV'$: note that $p^{j+1}G_q(\sigma_a, \sigma_b)\mu$ maps to $p^{j+1}G_q(\sigma'_{a'}, \sigma'_{b'})\mu'$ because all terms are multiples of p^{j+1} (the argument here needs the certain multiplications are preserved as well addition).

Once we have that our map preserves addition on terms in p^jV, the fact that it preserves products of pairs of terms from $p^hV \times p^iV$ for $h+i \geq j$ follows from the distributive law, the fact that addition in p^jV is preserved, and the fact that there is a unique way of writing $\mu_1\mu_2$, where μ_1 and μ_2 are monomials in the elements of T with all exponents $\leq q-1$, in the form $\nu^q\mu_3$ where all exponents in μ_3 are $\leq q-1$, and

$$(p^h\rho_a\mu_1)(p^i\rho_b\mu_2) = p^{h+i}(\sigma_a\sigma_b\nu)^q\mu_3$$

in V, while

$$(p^h\rho'_{a'}\mu'_1)(p^i\rho'_{b'}\mu'_2) = p^{h+i}(\sigma'_{a'}\sigma'_{b'}\nu')^q\mu'_3$$

in V'. $\square$

Lemma. *Let K be a field of characteristic $p > 0$ and let (V, pV, K), (W, pW, K) and (V_n, pV_n, K), $n \in \mathbb{N}$, be coefficient rings.*

(a) *If $p^t = 0$ while $p^{t-1} \neq 0$ in V, which is equivalent to the statement that p^t is the characteristic of V, then $\operatorname{Ann}_V p^jV = p^{t-j}V$, $0 \leq j \leq t$. Moreover, if $p^s = 0$ while $p^{s-1} \neq 0$ in W, and $W \twoheadrightarrow V$ is a surjection, then $V = W/p^tW$.*

(b) *Suppose that*

$$V_0 \twoheadleftarrow V_1 \twoheadleftarrow \cdots \twoheadleftarrow V_n \twoheadleftarrow \cdots$$

is an inverse limit system of coefficient rings and surjective maps, and that the characteristic of V_n is $p^{t(n)}$ where $t(n) \geq 1$. Then either $t(n)$ is eventually constant, in which case the maps $h_n : V_{n+1} \twoheadrightarrow V_n$ are eventually all isomorphisms, and the inverse limit is isomorphic with V_n for any sufficiently large n, or $t(n) \to \infty$ as $n \to \infty$, in which case the inverse limit is a complete local principal ideal V with maximal ideal pV and residue class field K. In particular, the inverse limit V is a coefficient ring.

Proof. (a) Every ideal of V (respectively, W) has the form p^kV (respectively, p^W)for a unique integer k, $0 \leq k \leq t$ (respectively, $0 \leq k \leq s$) The first statement follows because $k+j \geq n$ iff $k \geq n-j$. The second statement follows because V must have the form S/p^kS for some k, $0 \leq k \leq S$, and the characteristic of S/p^kS is p^k, which must be equal to p^t.

(b) If $t(n)$ is eventually constant it is clear that all the maps are eventually isomorphisms. Therefore, we may assume that $t(n) \to \infty$ as $n \to \infty$. By passing to an infinite subsequence of the V_n we may assume without loss of generality that $t(n)$ is strictly increasing with n. We may think of an element of the inverse limit as a sequence of elements $v_n \in V_n$ such that v_n is the image of v_{n+1} for every n. It is easy to see that one of the v_n is a unit if and only if all of them are. Suppose on the other hand that none of the v_n is a unit. Then each v_n can be written as pw_n for $w_n \in V_n$. The problem is that while pw_{n+1} maps to pw_n, for all n, it is not necessarily true that w_{n+1} maps to w_n.

Let h_n be the map $V_{n+1} \to V_n$. For all n, let $w'_n = h_n(w_{n+1})$. We will show that for all n, $v_n = pw'_n$ and that $h_n(w'_{n+1}) = w'_n$ for all n. Note first that $h_n(pw_{n+1}) = pw_n = v_n$, and it is also pw'_n. This establishes the first statement. Since $p(w_{n+1} - w'_{n+1}) = 0$, it follows that $w_{n+1} - w'_{n+1} = p^{t(n+1)-1}\delta$, by part (a). Then

$$w'_n = h_n(w_{n+1}) = h_n(w'_{n+1}) + p^{t(n+1)-1}h_n(\delta) = h_n(w'_{n+1}),$$

as required, since $p^{t(n+1)-1}$ is divisible by $p^{t(n)}$, the characteristic of V_n.

It follows that the inverse limit has a unique maximal ideal generated by p. No nonzero element is divisible by arbitrarily high powers of p, since the element will have nonzero image in V_n for some n, and its image in this ring is not divisible by arbitrarily high powers of p. It follows that every nonzero element can be written as a power of p times a unit, and no power of p is 0, because the ring maps onto V/p^t for arbitrarily large values of t. It is forced to be an a principal ideal domain in which every nonzero ideal is generated by a power of p. The fact that the ring arises as an inverse limit implies that it is complete. □

Theorem. *Let K be a field of characteristic $p > 0$. Then there exists a complete Noetherian valuation domain (V, pV, K) with residue class field K.*

Proof. It suffices to prove that there exists a Noetherian valuation domain (V, pV, K): its completion will then be complete with the required properties. Choose a well-ordering of K in which 0 is the first element. We construct, by transfinite induction, a direct limit system of Noetherian valuation domains $\{V_a, pV_a, K_a\}$ indexed by the well-ordered set K and injections $K_a \hookrightarrow K$ such that

(1) $K_0 \cong \mathbb{Z}/p\mathbb{Z}$

(2) The image of K_a in K contains a.

(3) The diagrams

$$\begin{array}{ccccc} V_b & \twoheadrightarrow & K_b & \hookrightarrow & K \\ \uparrow & & \uparrow & & \| \\ V_a & \twoheadrightarrow & K_a & \hookrightarrow & K \end{array}$$

commute for all $a \leq b \in K$.

Note the given a direct limit system of Noetherian valuation domains and injective local maps such that the same element, say, t (in our case $t = p$) generates all of their maximal ideals, the direct limit, which may be thought of as a directed union, of all of them is a Noetherian discrete valuation domain such that t generates the maximal ideal, and such that the residue class field is the directed union of the residue class fields. Every element of any of these rings not divisible by t is a unit (even in that ring): thus, if W is the directed union, pW is the unique maximal ideal. Every nonzero element of the union is a power of t times a unit, since that is true in any of the valuation domains that contain it, and it follows that every nonzero ideal is generated by the smallest power of p that it contains. The statement about residue class fields is then quite straightforward.

Once we have a direct limit system as described, the direct limit will be a discrete Noetherian valuation domain in which p generates the maximal ideal and the residue class field is isomorphic with K.

It will therefore suffice to construct the direct limit system.

We may take $V_0 = \mathbb{Z}_P$ where $P = p\mathbb{Z}$. We next consider an element $b \in K$ which is the immediate successor of $a \in K$. We have a Noetherian discrete valuation domain (V_a, pV_a, K_a) and an embedding $K_a \hookrightarrow K$. We want to enlarge V_a suitably to form V_b. If b is transcendental over K_a we simply let V_b be the localization of the polynomial ring $V_a[x]$

in one variable over V_a at the expansion of pV_a: the residue class field may be identified with $K_a(x)$, and the embedding of $K_a \hookrightarrow K$ may be extended to the simple transcendental extension $K_a(x)$ so that x maps to $b \in K$.

If b is already in the image of K_a we may take $V - b = V_a$. If instead b is algebraic over the image of K_a, but not in the image, then it satisfies a minimal monic polynomial $g = g(x)$ of degree at least 2 with coefficients in the image of K_a. Lift the coefficients to V_a so as to obtain a monic polynomial $G = G(x)$ of the same degree over V_a. We shall show that $V_b = V_a[x]/\big(G(x)\big)$ has the required properties. If G were reducible over the fraction field of V_a, by Gauss' Lemma it would be reducible over V_a, and then g would be reducible over the image of K_a in K. If follows that $\big(G(x)\big)$ is prime in $V_a[x]$m and so V_b is a domain that is a module-finite extension of V_a. Consider a maximal ideal m of V_b. Then the chain $m \supset (0)$ in V_b lies over a chain of distinct primes in V_a: since V_a has only two distinct primes, we see that m lies over pV_a and so $p \in m$. But

$$V_b/pV_a \cong \mathrm{Im}\,(K_a)[x]/g(x) \cong \mathrm{Im}\,(K_a)[b],$$

and so p must generate a unique maximal ideal in V_b, and the residue class field behaves as we require as well.

Finally, if b is a limit ordinal, we first take the direct limit of the system of Noetherian discrete valuation domains indexed by the predecessors of b, and then enlarge this ring as in the preceding paragraph so that the image of its residue class field contains b. □

Corollary. *If p is a positive prime integer and K is field of characteristic p, there is, up to isomorphism, a unique coefficient ring of characteristic $p > 0$ with residue class field K and characteristic p^t, and it has the form V/p^tV, where (V, pV, K) is a Noetherian discrete valuation domain.*

Proof. By the preceding Theorem, we can construct V so that it has residue field K. Then V/p^tV is a coefficient ring with residue class field K of characteristic p, and we already know that such all rings are isomorphic, which establishes the uniqueness statement. □

Corollary. *Let p be a positive prime integer, K a field of characteristic p, and suppose that (V, pV, K) and (W, pW, K) are complete Noetherian discrete valuation domains with residue class field K. Fix a p-base Λ for K. Let T be a lifting of Λ to V and T' a lifting to W. Then there is a unique isomorphism of V with W that maps each element of T to the element with the same residue in Λ in T'.*

Proof. By our results for the case where the maximal ideal is nilpotent, we get a unique such isomorphism $V/p^nV \cong W/p^nW$ for every n, and this gives an isomorphism of the inverse limit systems

$$V/pV \twoheadleftarrow V/p^2V \twoheadleftarrow \cdots \twoheadleftarrow V/p^nV \twoheadleftarrow \cdots$$

and

$$W/pW \twoheadleftarrow W/p^2W \twoheadleftarrow \cdots \twoheadleftarrow W/p^nW \twoheadleftarrow \cdots$$

that takes the image of T in each V/p^nV to the image of T' in the corresponding W/p^nW. This induces an isomorphism of the inverse limits, which are V and W, respectively. □

Theorem (I. S. Cohen). *Every complete local ring (R, m, K) has a coefficient ring. If the residue class field has characteristic $p > 0$, there is a unique coefficient ring containing a given lifting T to R of a p-base Λ for K.*

Proof. We may assume that K has characteristic $p > 0$: we already know that there is a coefficient field if the characteristic of K is 0.

Any coefficient ring for R containing T must map onto a coefficient ring for R/m^n containing the image of T. Here, there is a unique coefficient ring V_n, which may be described, for any sufficiently large $q = p^N$, as the smallest subring containing all qth powers and the image of T . We may take q large enough that it may be used in the description of coefficient rings V_{n+1} for R_{n+1} and V_n for R_n, and it is then clear that $R_{n+1} \twoheadrightarrow R_n$ induces $V_{n+1} \twoheadrightarrow V_n$. If we construct $\varprojlim_n V_n$ and $\varprojlim_n R_n$ as sequences of elements $\{r_n\}_n$ such that r_{n+1} maps to r_n for all n, it is clear that $\varprojlim_n V_n \subseteq \varprojlim_n R_n$. By part (b) of the Lemma on p. 2, $V = \varprojlim_n V_n$ is a coefficient ring, and so V is a coefficient ring for R. $\square$

Math 615: Lecture of April 9, 2012

Corollary. *Every complete local ring (R, m, K) is a homomorphic image of a complete regular local ring. In the equicharacteristic case, this may be taken to be a formal power series ring over a field. If R does not contain a field, we may take the regular ring to be formal power series over a Noetherian discrete valuation ring that maps onto a coefficient ring for R.*

Proof. We already know this in the equicharacteristic case. In the remaining cases, K has characteristic p and R has a coefficient ring which is either a Noetherian discrete valuation ring (V, pV, K) or of the form V/p^nV for such a ring V. Let $p, u_1, \ldots, u_s$ be generators for the maximal ideal of R, and map $V[X_1, \ldots, X_s] \to R$ as a V-algebra such that $X_j \mapsto u_j$, $1 \leq j \leq s$, which induces a map $V[[X_1, \ldots, X_s]] \to R$. By part (c) of the second Proposition on the third page of the Lecture Notes of January 9, this map is surjective. $\square$

Corollary. *Let (R, m, K) be a complete local ring of mixed characteristic $p > 0$. Let (V, pV, K) be a coefficient ring for R, and let $x_1, \ldots, x_{d-1} \in R$ have images that are a system of parameters for R/pR. Map $V[[X_1, \ldots, X_{d-1}]] \to R$ as V-algebras by sending X_j to x_j, $1 \leq j \leq d-1$. Then R is module-finite over the image of $V[[X_1, \ldots, X_{d-1}]]$, and if R is a domain, or, more generally, if p is part of a system of parameters for R (equivalently, p is not in any minimal prime of R such that $\dim(R/P) = \dim(R)$), then V is a Noetherian discrete valuation domain, and R is a module-finite extension of $V[[X_1, \ldots, X_{d-1}]]$.*

Proof. That R is module-finite over the image is immediate form part (b) of the second Proposition on the third page of the Lecture Notes of January 9. If p is part of a system of parameters, then $\dim(R) = d$. It follows that the kernel of the map from the domain

$V[[X_1, \ldots, X_{d-1}]]$ to R is (0), or else R will be module-finite over a domain of dimension $d-1$. $\square$

Note, however, that $R = V[[x]]/px$ is not module-finite over a formal power series ring over a coefficient ring. V is a coefficient ring, but p is not part of a system of parameters. R is one dimensional, and it is not module-finite over V.

A regular local ring (R, m, p) of mixed characteristic p is called *unramified* if, equivalently:

(1) $p \notin m^2$.

(2) R/pR is also regular.

Recall from the problem **4.** of Problem Set #2 that a quotient of a regular local ring by an ideal J is regular if and only if J is generated by part of a minimal set of generators for the maximal ideal of the regular local ring. In particular, R/pR is regular if and only if p is part of a minimal set of generators for m, and this holds if and only if $p \notin m^2$. Note that if Q is a prime ideal of an unramified regular local ring of mixed characteristic, then if $p \notin Q$ we have that R_Q is an equicharacteristic 0 regular local ring, while if $p \in Q$ then R_Q is again unramified, because R_Q/pR_Q is a localization of R/pR and therefore is again regular.

Theorem. *Let (R, m, K) be a complete regular local ring of Krull dimension d. If R is equicharacteristic then $R \cong K[[X_1, \ldots, X_d]]$. If R is mixed characteristic with K of characteristic $p > 0$ then R is unramified if and only if $R \cong V[[X_1, \ldots, X_{d-1}]]$, a formal power series ring, where (V, pV, K) is a coefficient ring (and so is a complete Noetherian discrete valuation domain). If R is mixed characteristic with K of characteristic $p > 0$ then R is ramified regular iff $R \cong T/(p-G)$ where V is a coefficient ring that is a Noetherian discrete valuation domain, $T = V[[x_1, \ldots, x_d]]$ is a formal power series ring with maximal ideal m_T, and and $G \in m_T^2 - pT$.*

Proof. In the unramified case, p may be extended to a minimal set of generators for m, say $p, x_1, \ldots, x_{d-1}$. We are now in the situation of both preceding corollaries: we get a map $V[[X_1, \ldots, X_{d-1}]] \to R$ such that the residue field of V maps onto that of R, while the images of $p, x_1, \ldots, x_{d-1}$ generate m. This implies that the map is onto. But, as in preceding Corollary, the map is injective. Thus, $R \cong V[[X_1, \ldots, X_{d-1}]]$. Conversely, with (V, pV, K) a Noetherian complete discrete valuation domain, $V[[X_1, \ldots, X_{d-1}]]$ is a complete regular local ring of mixed characteristic and $p \notin m^2$.

Now suppose that $p \in m^2$. Choose a minimal set of generators $x_1, \ldots, x_d$ for m. The we still get a surjection $V[[X_1, \ldots, X_d]] \twoheadrightarrow R$. Since R is regular it is a domain, and the kernel must be a height one prime of $T = V[[x_1, \ldots, x_d]]$, since $\dim(R) = d$. But $V[[x_1, \ldots, x_d]]$ is regular, and therefore a UFD, and so this height one prime P is principal. Since $p \in m^2$ and m_T^2 maps onto m^2, we get an element of $\mathrm{Ker}\,(T \twoheadrightarrow R)$ of the form $p - G$, where $G \in m_T^2$. The element G cannot be divisible by p: if it were, $G = pG_0$ with $G_0 \in m$, and then $p - G = p(1 - G_0)$ generates pT, since $1 - G_0$ is a unit, while $p \neq 0$ in R. Conversely, if $G \in m_T^2$ and $G \notin pT$, then $p - G \in m_T - m_T^2$, and so it is part of a minimal set of generators for m_T. Therefore $R = T/(p-G)$ is regular. Since $G \notin pT$, $p - G$ and p are

not associates, and, in particular, p is not a multiple of $p - G$. Since p is nonzero in R, R is of mixed characteristic. Since $G \in m_T^2$, p is in the square of the maximal ideal of R, i.e., R is a ramified regular local ring. $\square$

We shall retain the following hypotheses for a while. Let A be a Noetherian ring, let R and S be A-algebras that are Noetherian rings, let $\mathfrak{m} \subseteq R$ and $\mathfrak{n} \subseteq S$ be ideals such that $R/\mathfrak{m}$ has finite length as an A-module, and $S/\mathfrak{n}$ has finite length as an A-module. Let M be a finitely generated R-module and N be a finitely generated S-module.

We note that for all s and t, the modules $M/\mathfrak{m}^s M$ and $N/\mathfrak{n}^t N$ have finite length as A-modules. (E.g., the former has a finite filtration by modules $\mathfrak{m}^h M/\mathfrak{m}^{h+1}$ each of which is finitely generated over R and killed by $\mathfrak{m}$, and so finitely generated over $R/\mathfrak{m}R$, which has finite length over A). When U and V have finite length over A (or even if one has finite length and the other is finitely generated), every $\operatorname{Tor}_j^A(U, V)$ has finite length: a finitely generated module has finite length if and only if its support consists of a finite set of maximal ideals, and we know that

$$\operatorname{Supp}\left(\operatorname{Tor}_j^A(U, V)\right) \subseteq \operatorname{Supp}(U) \cap \operatorname{Supp}(V),$$

since Tor commutes with localization.

Therefore the modules $\operatorname{Tor}_n^A(M/\mathfrak{m}^s M, N/\mathfrak{n}^t N)$ have finite length as A-modules. The set $\mathbb{N} \times \mathbb{N}$ is directed, since given (s, t) and (s', t'), both pairs are bounded by the pair

$$(\max\{s, s'\}, \max\{t, t'\}).$$

Therefore, we may consider $\mathbb{N}\times\mathbb{N}$ as a directed set under the partial ordering $(s, t) \leq (s', t')$ if $s \leq s'$ and $t \leq t'$, and we may take inverse limits over this set. Note that if $s \leq s'$ and $t \leq t'$ we have A-linear maps $M/\mathfrak{m}^{s'} M \twoheadrightarrow M/\mathfrak{m}^s M$ and $N/\mathfrak{n}^{t'} N \twoheadrightarrow n/\mathfrak{n}^t N$ and therefore a map

$$\operatorname{Tor}_j^A(M/\mathfrak{m}^{s'} M, N/\mathfrak{n}^{t'} N) \to \operatorname{Tor}_j^A(M/\mathfrak{m}^s M, N/\mathfrak{n}^t N).$$

We may therefore define

$$\hat{\operatorname{Tor}}_j^A(M, N) = \varprojlim_{s,t} \operatorname{Tor}_j^A(M/\mathfrak{m}^s M, N/\mathfrak{n}^t N).$$

For $j = 0$ we write $M \widehat{\otimes}_A N$ for

$$\hat{\operatorname{Tor}}_0^A(M, N) = \varprojlim_{s,t} (M/\mathfrak{m}^s M) \otimes_A (N/\mathfrak{n}^t N).$$

Note that given $s, t \in \mathbb{N}$ we can choose $n = \max\{s, t\}$, and then $(n, n) \geq (s, t)$. Thus, the elements (n, n) are cofinal in the directed set $\mathbb{N} \times \mathbb{N}$, and we may also write

$$\hat{\operatorname{Tor}}_j^A(M, N) = \varprojlim_{n} \operatorname{Tor}_j^A(M/\mathfrak{m}^n M, N/\mathfrak{n}^n N),$$

and

$$M\widehat{\otimes}_A N = \varprojlim_n M/\mathfrak{m}^n M\widehat{\otimes}_A N/\mathfrak{n}^n N.$$

By a *coset* in an A-module B we mean a subset of the form $u + D$ where D is an A-submodule of B. D is recoverable from the coset C as $\{v - w : v, w \in C\}$. On the other hand, u is not unique unless $D = 0$: if v is any element of a coset C, the $C = v + D$ as well. The image of a coset under an A-linear map is evidently a coset. Notice that if $f : B' \to B$ is linear then the inverse image of $u \in B$ is either empty, if u is not in $\mathrm{Im}\,(f)$, or else a coset in B': if v is one element of the inverse image, then the inverse image is $v + \mathrm{Ker}\,(f)$. If $C \subseteq C'$ are cosets and the associated modules are the same, then $C = C'$: if $u \in C$, and D is the module, then $C = u + D$ and $C' = u + D$. It follows that in a module of finite length (or one with DCC), the set of all cosets has DCC: given a descending sequence of cosets, the associated sequence of submodules is also descending, and therefore eventually constant. But then the sequence of cosets is eventually constant as well.

Notice that the intersection of two cosets $u + D_1$ and $v + D_2$ may be empty, but if w is in the intersection it will have the form $w + (D_1 \cap D_2)$.

Studying cosets in modules is completely analogous to studying linear subspaces of vector spaces that need not contain 0: this is simply the special case where the base ring is a field.

In general, although a direct limit of exact sequences is exact, an inverse limit of exact sequences is not: consider the inverse limit system of exact sequences of $\mathbb{Z}$-modules:

$$\begin{array}{ccccccccc}
0 & \to & 2\mathbb{Z} & \subseteq & \mathbb{Z} & \twoheadrightarrow & \mathbb{Z}/2\mathbb{Z} & \to & 0 \\
 & & \cup & & \| & & \uparrow\uparrow & & \\
0 & \to & 4\mathbb{Z} & \subseteq & \mathbb{Z} & \twoheadrightarrow & \mathbb{Z}/4\mathbb{Z} & \to & 0 \\
 & & \cup & & \| & & \uparrow\uparrow & & \\
 & & \vdots & & \vdots & & \vdots & & \\
 & & \cup & & \| & & \uparrow\uparrow & & \\
0 & \to & 2^n\mathbb{Z} & \subseteq & \mathbb{Z} & \twoheadrightarrow & \mathbb{Z}/2^n\mathbb{Z} & \to & 0 \\
 & & \cup & & \| & & \uparrow\uparrow & & \\
0 & \to & 2^{n+1}\mathbb{Z} & \subseteq & \mathbb{Z} & \twoheadrightarrow & \mathbb{Z}/2^{n+1}\mathbb{Z} & \to & 0 \\
 & & \cup & & \| & & \uparrow\uparrow & & \\
 & & \vdots & & \vdots & & \vdots & &
\end{array}$$

The inverse limits corresponding to the three nonzero columns are $\bigcap_n 2^n\mathbb{Z} = 0$, $\mathbb{Z}$, and the 2-adic integers $\widehat{\mathbb{Z}_P}$ where $P = 2\mathbb{Z}$, respectively. But the sequence

$$0 \to 0 \to \mathbb{Z} \to \widehat{\mathbb{Z}_P} \to 0$$

is not exact, since $\mathbb{Z} \to \widehat{\mathbb{Z}_P}$ is not surjective.

However, we have the following:

Theorem. *The inverse limit of a sequence of exact sequences of finite length A-modules is exact.*

Proof. Suppose the typical three consecutive terms at the nth spots are

$$B'_n \to B_n \to B''_n$$

It is clear that the composite map

$$(\varprojlim{}_n B_n \to \varprojlim{}_n B''_n) \circ (\varprojlim{}_n B'_n \to \varprojlim{}_n B_n)$$

is zero. Let $\{u_n\}_n$ be a sequence of elements, with $u_n \in B_n$, representing an element of $\varprojlim_n B_n$, so that u_{n+1} maps to u_n under the inverse limit system map $B_{n+1} \to B_n$ for all n. Suppose that this element maps to 0 in $\varprojlim_n B''_n$. This simply means that every u_n maps to 0 in B''_n. Let C_n denote the inverse image of u_n in B'_n. Then the coset C_n is nonempty for all n, since every

$$B'_n \to B_n \to B''_n$$

is exact. For every i, let $Q_{i,n}$ denote denote the image of C_n in B'_i for $n \geq i$. Evidently, for fixed i, $Q_{i,n}$ is descending as n increases. Since these are cosets in a module of finite length, we have that $Q_{i,n}$ is stable for all sufficiently large $n \gg i$. Call the stable value Q_i^∞. Evidently, the map $B'_{i+1} \to B'_i$ maps $Q_{i+1}^\infty \to Q_i^\infty$. Even better, the restricted map $Q_{i+1}^\infty \to Q_i^\infty$ is onto: for large n the images of C_n in B'_{i+1} and in B'_i are both stable, and the image in B'_{i+1} maps onto the image in B'_i. Since the maps $Q_{i+1}^\infty \to Q_i^\infty$ are surjective and the Q_i^∞ are nonempty, we have that $\varprojlim_n Q_n^\infty$ is nonempty. An element of this inverse limit is an element of $\varprojlim_n B'_n$ mapping to $\{u_n\}_n$, as required. $\square$

Corollary. *If $0 \to M_2 \to M_1 \to M_0 \to 0$ is an exact sequence of finitely generated R-modules such that each $M_i/\mathfrak{m}M_i$ has finite length over A, then there is a long exact sequence for complete Tor:*

$$\cdots \to \hat{\mathrm{Tor}}_n^A(M_2,\, N) \to \hat{\mathrm{Tor}}_n^A(M_1,\, N) \to \hat{\mathrm{Tor}}_n^A(M_0,\, N) \to \hat{\mathrm{Tor}}_{n-1}^A(M_2,\, N) \to$$

$$\cdots \to \hat{\mathrm{Tor}}_1^A(M_0,\, N) \to M_2 \widehat{\otimes}_A N \to M_1 \widehat{\otimes}_A N \to M_0 \widehat{\otimes}_A N \to 0.$$

If $0 \to N_2 \to N_1 \to N_0 \to 0$ is an exact sequence of finitely generated S-modules such that each $N_j/\mathfrak{n}N_j$ has finite length over A, there is an analogous long exact sequence for Tôr *as well.*

Proof. For all s and t there is a short exact sequence

$$0 \to M_2/(\mathfrak{m}^s M_1 \cap M_2) \to M_1/\mathfrak{m}^s M_1 \to M_0/\mathfrak{m}^s M_0 \to 0,$$

and we may form the long exact sequence for $\mathrm{Tor}_\bullet^A$ with $N/\mathfrak{n}^t N$. By the preceding Proposition, the inverse limit of these sequences is exact. Because the inherited $\mathfrak{m}$-adic filtration $(\mathfrak{m}^s M_1) \cap M_2$ on M_2 is stably $\mathfrak{m}$-adic,

$$\varprojlim{}_{s,t} \mathrm{Tor}_j^A\big(M_2/(\mathfrak{m}^s M_1 \cap M_2),\, N/\mathfrak{n}^t N\big) \cong \varprojlim{}_{s,t} \mathrm{Tor}_j^A(M_2/\mathfrak{m}^s M_2,\, N/\mathfrak{n}^t N),$$

which gives the required result. $\square$

Math 615: Lecture of April 11, 2012

We continue with the following fixed notations: A is a Noetherian ring, R and S are Noetherian A-algebras, $\mathfrak{m} \subseteq R$ and $\mathfrak{n} \subseteq S$ are ideals such that $R/\mathfrak{m}$ and $S/\mathfrak{n}$ have finite length over A, M is a finitely generated R-module, and N is a finitely generated S-module.

Theorem. *With hypothesis as above, let $T = R \otimes_A S$ and let $\mathfrak{q}_{s,t}$ be the sum of the images of $\mathfrak{m}^s \otimes_A S$ and $S \otimes_A \mathfrak{n}^t$ in T, so that $T/\mathfrak{q}_{s,t} \cong R/\mathfrak{m}^s \otimes_A S/\mathfrak{n}^t$. Let $\mathfrak{q} = \mathfrak{q}_{1,1}$. Then $R\widehat{\otimes}_A S$ is the $\mathfrak{q}$-adic completion of $R \otimes_A S$, and $M\widehat{\otimes}_A N$ is the $\mathfrak{q}$-adic completion of $M \otimes_A N$. Moreover, $R\widehat{\otimes}_A S$ is a Noetherian ring, and $M\widehat{\otimes}_A N$ is a finitely generated module over $R\widehat{\otimes}_A S$.*

Proof. Let $\mathfrak{m}$ have generators $u_1, \ldots, u_h$ and let $\mathfrak{n}$ have generators $v_1, \ldots, v_k$. Of course, $\mathfrak{q}_{n,n} \subseteq \mathfrak{q}_{s,t}$ if $n \geq \min\{s, t\}$ and the sequences of ideals $\mathfrak{q}_{n,n}$ and $\mathfrak{q}^n$ are cofinal as well: $\mathfrak{q}_{n,n} \subseteq \mathfrak{q}^n$, and $\mathfrak{q}^{(h+k)n}$ is generated by monomials of degree $(h+k)n$ in the images of the elements $u_1, \ldots, u_h, v_1, \ldots, v_k$, and either some u_i or some v_j must occur with exponent at least n in each of these monomials. It follows that, $\mathfrak{q}^{(h+k)n} \subseteq \mathfrak{q}_{n,n}$. Consequently, $R\widehat{\otimes}_A S \cong \lim_n T/\mathfrak{q}^n$, the $\mathfrak{q}$-adic completion of T, as claimed.

Let $\underline{X} = X_1, \ldots, X_h$ and $\underline{Y} = Y_1, \ldots, Y_k$. Map the polynomial ring $A[\underline{X}, \underline{Y}]$ to $R \otimes_A S = T$ as an A-algebra by sending X_i to u_i and Y_j to v_j. Then there is an induced map $A[[\underline{X}, \underline{Y}]] \to R\widehat{\otimes}_A S$ with the same property. By the Proposition on page 2 of the Lecture Notes from January 9, $R\widehat{\otimes}_A S$ is module-finite over $A[[\underline{X}, \underline{Y}]]$: the quotient by the expansion of $(\underline{X}, \underline{Y})$, which is $\mathfrak{q}(R\widehat{\otimes}_A S)$, is $R/\mathfrak{m} \otimes_A S/\mathfrak{n}$, which has finite length over A and so is finitely generated over A. Likewise,

$$(M\widehat{\otimes}_A N)/\big((\underline{X}, \underline{Y})(M\widehat{\otimes}_A N)\big) \cong (M \otimes_A N)/\mathfrak{q}(M \otimes_A N) \cong (M/\mathfrak{m}M) \otimes_A (N/\mathfrak{n}N),$$

which is a finite length module over A, and so is finitely generated as an A-module. It then follows, from the same Proposition, that $M\widehat{\otimes}_A N$ is finitely generated as an $A[[\underline{X}, \underline{Y}]]$-module, and, hence, as a module of $R\widehat{\otimes}_A S$. $\square$

Note that we have an A-bilinear map

$$M \times N \to M\widehat{\otimes}_A N$$

since we have a map $M \otimes_A N \to M\widehat{\otimes}N$: the image of (u, v) is denoted $u\widehat{\otimes}v$. Likewise we have A-algebra homomorphisms $R \to R\widehat{\otimes}_A S$ and $S \leq R\widehat{\otimes}_A S$ sending r to $r\widehat{\otimes}1$ and s to $1\widehat{\otimes}s$, respectively.

Theorem. *Let (A, μ) be regular local of Krull dimension n, let hypotheses be as in the first paragraph, and suppose that* $\operatorname{depth}_\mu M \geq d$. *Then* $\hat{\operatorname{Tor}}_j^A(M, N) = 0$ *for all* $j > n - d$.

Proof. We first reduce to the case where N has been replaced by $N_t = N/\mathfrak{n}^t N$ and so has finite length over A (since it has a finite filtration with factors $\mathfrak{n}^i N/\mathfrak{n}^{i+1}N$, $0 \leq i < t$, that are finitely generated $(S/\mathfrak{n}S)$-modules). Assuming that case, for $j > n - d$ we have $0 = \varprojlim_t \hat{\operatorname{Tor}}_j^A(M, N_t)$ (since every term is 0) and this is

$$\varprojlim_t \big(\varprojlim_s \operatorname{Tor}_j^A(M/\mathfrak{m}^s M,\, N_t/\mathfrak{n}^s N_t)\big).$$

Since $\mathfrak{n}^s N_t = 0$ for $s \geq t$, this is the same as

$$\varprojlim_t \big(\varprojlim_s \operatorname{Tor}_j^A(M/\mathfrak{m}^s M,\, N_t)\big) = \varprojlim_{s,t} \operatorname{Tor}_j^A(M/\mathfrak{m}^s M,\, N/\mathfrak{n}^t N) = \hat{\operatorname{Tor}}_j^A(M, N).$$

Thus, we may assume without loss of generality that N has finite length over A, and so is killed by a power of μ.

Since $\operatorname{depth}_\mu M \geq d$, we may choose a sequence of elements $a_1, \ldots, a_d \in \mu$ that is a regular sequence on M. Replacing them by powers if necessary, we may assume that each of these elements kills N. We now prove by induction on d that the existence of such a sequence forces the stated vanishing of complete Tor.

If $d = 0$, we know that since A is regular of Krull dimension d, every $\operatorname{Tor}_j^A(U, V) = 0$ for $j > n = n - d$, and this forces the vanishing of all the complete Tor modules as well, because each of them is an inverse limits of Tor modules that vanish. Now suppose that $d > 0$ and apply the induction hypothesis to $M/a_1 M$ and the sequence $a_2, \ldots, a_d$. Because $a = a_1$ kills N, it kills all complete Tors with N, and the short exact sequence

$$0 \to M \xrightarrow{a} M \to M/aM \to 0$$

yields a long exact sequence for complete Tor that breaks up into short exact sequences as follows:

$$0 \to \hat{\operatorname{Tor}}_{j+1}^A(M, N) \to \hat{\operatorname{Tor}}_{j+1}^A(M/aM, N) \to \hat{\operatorname{Tor}}_j^A(M, N) \to 0$$

By the induction hypothesis, $\hat{\operatorname{Tor}}_{j+1}^A(M/aM, N) = 0$ for $j + 1 > n - d - 1$, i.e., $j \geq n - d$, and the vanishing of the middle term gives the vanishing of both end terms. $\square$

Now suppose that (A, μ) is regular local of Krull dimension n and that $\operatorname{depth}_\mu R = n$. Fix N. Then the functor $\mathcal{F} = \_ \mathbin{\widehat{\otimes}}_A N$ is right exact (from the terms of degree 0 in the long exact sequence for complete Tor), and vanishes on finitely generated projective R-modules, which are free, and have depth n on μ. Moreover, there is a functorial long exact sequence for $\hat{\operatorname{Tor}}_\bullet^A(\_, N)$. This implies that $\hat{\operatorname{Tor}}_j^A(\_, \mathbb{N})$ agrees with the jth left derived functor $L_j\mathcal{F}$ of $\mathcal{F} = \_ \mathbin{\widehat{\otimes}}_A N$. That is, $\hat{\operatorname{Tor}}_j^A(M, N)$ may be computed from a projective resolution $P_\bullet$ of M by finitely generated projective ($\equiv$ free) R-modules by applying $\mathcal{F}$ and taking homology:

$$\hat{\operatorname{Tor}}_j^A(M, N) = H_j(P_\bullet \mathbin{\widehat{\otimes}}_A N).$$

The point is that the left derived functors of $\_\widehat{\otimes}_A N$ agree with complete Tor in degree 0, vanish in higher degree on finitely generated projective modules, and also have a functorial long exact sequence for Tor. Thus, if we write $0 \to M' \to P \to M \to 0$ where P is a finitely generated free module, the two long exact sequences break up in the same way to give:

$$0 \to \hat{\mathrm{Tor}}_1^A(M,\, N) \to M'\widehat{\otimes}_A N \to P\widehat{\otimes}_A N \to M\widehat{\otimes}_A N \to 0$$

and

$$0 \to L_1\mathcal{F}(M) \to M'\widehat{\otimes}_A N \to P\widehat{\otimes}_A N \to M\widehat{\otimes}_A N \to 0,$$

which yields an isomorphism

$$L^1\mathcal{F}(M) \cong \hat{\mathrm{Tor}}_1^A(M,\, N).$$

The long exact sequences also yield:

$$0 \to \hat{\mathrm{Tor}}_{j+1}^A(M,\, N) \to \hat{\mathrm{Tor}}_j^A(M',\, N) \to 0$$

and

$$0 \to L_{j+1}\mathcal{F}(M) \cong L_j\mathcal{F}(M') \to 0$$

for $j \geq 1$. The long exact sequence for Tôr shows that $\hat{\mathrm{Tor}}_1^A(M,\, N)$ is always finitely generated over $R\widehat{\otimes}_A S$, and then it follows that all of the $\hat{\mathrm{Tor}}_j^A(M,\, N)$ are, since $\hat{\mathrm{Tor}}_j^A(M,\, N) \cong \hat{\mathrm{Tor}}_1(M_{j-1},\, N)$ for $j \geq 2$, where M_{j-1} is a finitely generated $(j-1)$ st module of syzygies for M. Thus:

Theorem. *Let $(A,\, \mu)$ be regular local of Krull dimension n, let hypotheses be as in the first paragraph, and suppose that*$\mathrm{depth}_\mu R \geq d$. *Then all of the modules $\hat{\mathrm{Tor}}_j^A(M,\, N)$ are finitely generated over $R\widehat{\otimes}_A S$, and one may compute them from a resolution $P_\bullet$ of M by finitely generated free R-modules as $H_j(P_\bullet\widehat{\otimes}_A N)$. That is, $\hat{\mathrm{Tor}}_j^A(\_,\, N)$ is the j th left derived functor $L_j\mathcal{F}(\_)$, where $\mathcal{F}(\_) = \_\widehat{\otimes}_A N$.* $\square$

We now want to consider the situation where A is either a field K or a complete Noetherian discrete valuation domain V, where $R = A[[x_1,\, \ldots\, , x_n]]$, and $S = A[[y_1,\, \ldots\, , y_m]]$, and $\mathfrak{m}$, $\mathfrak{n}$ are the respective maximal ideals in R and S respectively. Let $\underline{x} = x_1,\, \ldots\, , x_n$ and $\underline{y} = y_1,\, \ldots\, , y_m$. It is then straightforward to verify that $R\widehat{\otimes}_A S$ is $A[[\underline{x},\, \underline{y}]]$. In fact,

$$R \otimes_A S/\mathfrak{q}^s \cong A[\underline{x},\, \underline{y}]/(\mu, \underline{x},\, \underline{y})^s,$$

and so the inverse limit is $A[[\underline{x},\, \underline{y}]]$. If $A = K$ is field, both of the functors $M\widehat{\otimes}_K \_$ and $\_\widehat{\otimes}_K N$ are exact, from the long exact sequence, since it is evident that all higher complete Tor modules vanish.

If $A = V$ is a Noetherian discrete valuation domain, then all $\hat{\mathrm{Tor}}_j^V(M,\, N)$ vanish for $j \geq 2$: we have only $\hat{\mathrm{Tor}}_1^V(M,\, ,N)$ to be concerned about among the higher complete Tor modules. Moreover, we also know that $\hat{\mathrm{Tor}}_1^V(M,\, N) = 0$ if either M or N is torsion-free over V.

We want to use these ideas to reinterpret Tor modules over a complete regular local ring as Koszul homology. In the equicharacteristic case this is relatively easy. Suppose that $R = S = K[[x_1, \ldots, x_n]]$ and let

$$T = R\widehat{\otimes}_K S \cong K[[x_1, \ldots, x_n, y_1, \ldots, y_n]],$$

where we are writing x_j instead of $x_j\widehat{\otimes}1$ and y_j instead of $1\widehat{\otimes}x_j$. Notice that there is a map $T \to R$ that is the identity on the images of R and S in T, and its kernel is the ideal $(x_1 - y_1, \ldots, x_n - y_n)T$, which is generated by a regular sequence. We want to prove next that if M and N are finitely generated R-modules then

$$\operatorname{Tor}_j^R(M, N) \cong \operatorname{Tor}_j^T(M\widehat{\otimes}_K N, R)$$

where $R = T/(x_1 - y_1, \ldots, x_n - y_n)T$. The ideal is generated by a regular sequence in T, and so the quotient R may be resolved using a Koszul complex. We shall consequently be able to show that

$$\operatorname{Tor}_j^R(M, N) \cong H_j(x_1 - y_1, \ldots, x_n - y_n; M\widehat{\otimes}_K N).$$

From this, it will follow that if $\operatorname{Tor}_j^R(M, N) = 0$, then then $\operatorname{Tor}_k^R(M, N) = 0$ whenever $k \geq j$.

Math 615: Lecture of April 13, 2012

Suppose that we are interested in studying the intersection of two closed algebraic sets $X = V(I)$ and $Y = V(J)$, both embedded in $\mathbb{A}_K^n$ over an algebraically closed field K. Set-theoretically, $X \cap Y \cong (X \times Y) \cap \Delta$ where Δ is the diagonal $\{(z, z) : z \in \mathbb{A}_K^n\}$. The idea of studying $(X \times Y) \cap \Delta$ instead of $X \cap Y$ directly is called *reduction to the diagonal*, and it is useful in many forms of geometry.

Algebraically, let $R = K[x_1, \ldots, x_n]$ be the coordinate ring of $\mathbb{A}_K^n$ and $T = R \otimes_K R = K[x_1, \ldots, x_n, y_1, \ldots, y_n]$ where we think of x_j as corresponding to $x_j \otimes 1$ and y_j as corresponding to $1 \otimes y_j$. $X \cap Y$ has coordinate ring $R/(I + J)$ (up to nilpotents, and in the theory of schemes it is preferable to let the nilpotents stay, so to speak), and $R/I \otimes_R R/J = R/(I + J)$. Therefore, heuristically, when one tensors two cyclic modules one should think of intersecting corresponding varieties (or schemes). However, experience has shown that information about the intersection is carried not only by the tensor product itself but by all the Tor modules collectively. Moreover, since every finitely generated module has a filtration by cyclic modules, it is reasonable to extend the analogy and think of studying all the $\operatorname{Tor}_j^R(M, N)$ as doing some sort of intersection theory (and, in fact, the alternating sum of the classes $[\operatorname{Tor}_j^R(M, N)]$, interpreted in a suitable Grothendieck group, carries significant numerical information about the intersection). This suggests that instead of studying the Tor modules directly, one might want to use reduction to the diagonal. Algebraically, $X \times Y$ has coordinate ring $K[X] \otimes_K K[Y] \cong (R/I) \otimes_K (R/J)$,

and $K[\Delta]$ may be identified with R thought of as a module over $R \otimes_K R$, where the map $R \otimes_K R \twoheadrightarrow R$ sends $r \otimes s \mapsto rs$: the kernel is $(x_1 - y_1, \ldots, x_n - y_n)$, the defining ideal of the diagonal Δ. Algebraically,

$$(R/I) \otimes_R (R/J) \cong \big((R/I) \otimes_K (R/J)\big) \otimes_T R$$

and, more generally,

$$M \otimes_R N \cong (M \otimes_K N) \otimes_T R.$$

There is a corresponding fact about Tor, namely that for all j,

$$\operatorname{Tor}_j^R(M, N) \cong \operatorname{Tor}_j^T(M \otimes_K N, R),$$

which we won't prove explicitly, although the proof is essentially the same as for the complete local version that we will do explicitly in the sequel.

We next want to develop the machinery to study $\operatorname{Tor}_\bullet^R(M, N)$ over a complete regular local ring R by the method of *reduction to the diagonal*. The method is very similar to preceding discussion when R contains a field, except that the complete tensor product is used instead of the ordinary tensor product. However, since we will also need corresponding tools over a Noetherian discrete valuation domain V, we build the theory in greater generality.

Therefore, let (A, μ) be a complete regular local ring and let $R = A[[x_1, \ldots, x_n]]$. Let M and N respectively by finitely generated free R-modules. Form the double complex $\mathcal{D}_{\bullet\bullet} = P_\bullet \widehat{\otimes}_A Q_\bullet$ and its total complex $\mathcal{T}_\bullet$. Let $T = R\widehat{\otimes}_A R$ and let $\mathcal{K}_\bullet$ be a free resolution of

$$R = T/(x_1 - y_1, \ldots, x_n - y_n)$$

as a T-module. We may use

$$\mathcal{K}_\bullet = \mathcal{K}_\bullet(x_1 - y_1, \ldots, x_n - y_n; T).$$

Note that each module occurring in $\mathcal{D}_{\bullet\bullet}$, and, hence, also in $\mathcal{T}_\bullet$, has the form $R^s \widehat{\otimes}_A R^t \cong (R \otimes_A R)^{st} = T^{st}$. Thus, $\mathcal{T}$ is a free complex of T-modules. Since $R\widehat{\otimes}_A \_$ and $\_\widehat{\otimes}_A R$ are both exact, all rows and columns in $\mathcal{D}_{\bullet\bullet}$ are exact except at the 0 spot. One gets a single row of augmentations of columns and a single column of augmentations of rows. We know that the homology of either one is $\hat{\operatorname{Tor}}_\bullet^A(M, N)$. We also know that this is the homology of the total complex $\mathcal{T}$. If A is a field K, all the higher complete Tor modules vanish, and this tells us that $\mathcal{T}_\bullet$ is free resolution of $M \otimes_K N$ over T.

Also note that

$$(*) \quad (M\widehat{\otimes}_A N) \otimes_T R \cong M \otimes_R N$$

as functors of M and N. In one direction we have a bilinear map $(u, v) \mapsto (u\widehat{\otimes}v) \otimes 1$. Note that $(ru\widehat{\otimes}v) \otimes 1 = (u\widehat{\otimes}v) \otimes r = (u\widehat{\otimes}rv) \otimes 1$. Thus, we have a map

$$M \otimes_R N \to (M\widehat{\otimes}_A N) \otimes R$$

which is natural. The verification that this map is an isomorphism is straightforward, since the map is easily checked to be an isomorphism for $M_1 \oplus M_2$ (respectively $N_1 \oplus N_2$) iff it is an isomorphism for each summand separately, and to be an isomorphism when $M = N = R$. It follows that it is an isomorphism when M and N are finitely generated free modules. One can then do the case where M is free by taking a presentation of N, and, finally, the general case by taking a presentation of M, in each instance using a presentation by finitely generated free modules.

From the identification $(*)$ it follows readily that $\mathcal{D}_{\bullet\bullet} \otimes_T R \cong P_\bullet \otimes_R Q_\bullet$, and so $\mathcal{T} \otimes_T R$ is isomorphic with the total complex of $P_\bullet \otimes_R Q_\bullet$.

We now specialize for the moment to the case where $A = K$ is a field. Since the higher Tôr modules all vanish over a field K, in this case $\mathcal{T}$ is a free resolution of $M \widehat{\otimes}_K N$ over T. Now,

$$\operatorname{Tor}_\bullet^T(M \widehat{\otimes}_K N,\, R) \cong H_\bullet(\mathcal{T} \otimes_T R)$$

and $\mathcal{T} \otimes_T R$ is the same as the total complex of $\mathcal{D}_{\bullet\bullet} \otimes_T R$, which is the total complex of $P_\bullet \otimes_R Q_\bullet$. Thus,

$$\operatorname{Tor}_\bullet^T(M \widehat{\otimes}_K N,\, R) \cong H_\bullet(\mathcal{T}(P_\bullet \otimes_R Q_\bullet) = \operatorname{Tor}_\bullet^R(M,\, N),$$

the result we have been targeting for a while. We state this formally:

Theorem (reduction of Tor to the diagonal in the complete equicharacteristic case). *Let $R = K[[x_1, \dots, x_n]]$, a formal power series ring over a field K, and let $T = R \widehat{\otimes}_K R \cong K[[x_1, \dots, x_n, y_1, \dots, y_n]]$, where $x_j \in T$ corresponds to $x_j \widehat{\otimes} 1$ and $y_j \in T$ to $1 \widehat{\otimes} x_j$. View R as a T-module via the continuous map $T \twoheadrightarrow R$ that sends $r \widehat{\otimes} s$ to rs, whose kernel is $(x_1 - y_1, \dots, x_n - y_n)T$. Let M and N be finitely generated T-modules. Then for all j,*

$$\operatorname{Tor}_j^R(M,\, N) = \operatorname{Tôr}_j^T(M \widehat{\otimes}_K N,\, R) \cong H_j(x_1 - y_1, \dots, x_n - y_n;\, M \widehat{\otimes}_K N),$$

since $x_1 - y_1, \dots, x_n - y_n$ is a regular sequence in T. $\square$

Although we have sketched the argument earlier, before all the tools for the proof were available, we now give it more formally:

Theorem (M. Auslander). *Let R be an equicharacteristic regular ring and let M and N be finitely generated R-modules. If $\operatorname{Tor}_i^R(M,\, N) = 0$, then $\operatorname{Tor}_j^R(M,\, N) = 0$ for all $j \geq i$.*

Proof. Suppose that one has a counterexample. If $\operatorname{Tor}_j(M,\, N) \neq 0$ we may localize at a prime in its support, and so obtain a counterexample over a regular local ring R. We are using that calculation of Tor commutes with localization. We may likewise apply $\widehat{R} \otimes_R \_$, using that $\widehat{R}$ is faithfully flat over R to get a counterexample over a complete equicharacteristic regular ring. But then $R \cong K[[x_1, \dots, x_n]]$, a formal power series ring. By reduction to the diagonal, as described in the preceding Theorem, we may consider $H_j(x_1 - y_1, \dots, x_n - y_n;\, M \widehat{\otimes}_K N)$ instead, where $H_i(x_1 - y_1, \dots, x_n - y_n;\, M \widehat{\otimes}_K N) = 0$.

But we know the corresponding result for Koszul homology: see the second Corollary on the first page of the Lecture Notes from February 20. $\square$

We are aiming to prove the same result, which is sometimes referred to as the *rigidity* of Tor over regular rings, without the assumption that the regular ring R is equicharacteristic. This is quite a bit harder, and we will need to use more spectral sequence results.

We return to the study of reduction to the diagonal when $R = A[[x_1, \dots, x_n]]$ and (A, μ) is complete regular local. If $P_\bullet$ and $Q_\bullet$ are free resolutions of the finitely generated R-modules M and N respectively by finitely generated free R-modules, we still know that $\mathcal{D}_{\bullet\bullet} = P_\bullet \widehat{\otimes}_A Q_\bullet$ is a double complex consisting of finitely generated free T-modules, where $T = R\widehat{\otimes}_A R$, and that the homology of its total complex $\mathcal{T}_\bullet$ is $\hat{\mathrm{Tor}}^A_\bullet(M, N)$. We view R as a T-module as before, so that the kernel of $T \twoheadrightarrow R$ is $(x_1 - y_1, \dots, x_n - y_n)$. Let $\mathcal{K}_\bullet$ be a free resolution of R over T: in fact, we may take $\mathcal{K}_\bullet$ to be the Koszul complex $\mathcal{K}_\bullet(x_1 - y_1, \dots, x_n - y_n; T)$. We want to consider the spectral sequences associated with double complex $\mathcal{T}_\bullet \otimes_T \mathcal{K}_\bullet$, in which a typical term is $\mathcal{T}_q \otimes_T \mathcal{K}_p$. If we take the homology of the column obtained by fixing $\mathcal{T}_q$, we get a nonzero result only in the 0 spot, namely, $\mathcal{T}_q \otimes_T R$, which may be identified with the total complex of $P_\bullet \otimes_R Q_\bullet$. Therefore, if we take the homology of this single nonzero row of column augmentations, we see that the homology of the total complex of $\mathcal{T}_\bullet \otimes_R \mathcal{K}_\bullet$ is simply $\mathrm{Tor}^R_\bullet(M, N)$. On the other hand, if we fix the row indexed by p and take homology we get $\hat{\mathrm{Tor}}^A_\bullet(M, N) \otimes_T \mathcal{K}_p$. Thus, the E^2 term of the spectral sequence for $H_{\mathrm{I}}H_{\mathrm{II}}$ is $\mathrm{Tor}^T_p(\hat{\mathrm{Tor}}^A_q(M, N), R)$, and we have

$$\mathrm{Tor}^T_p(\hat{\mathrm{Tor}}^A_q(M, N), R) \underset{p}{\Longrightarrow} \mathrm{Tor}^R_{p+q}(M, N).$$

This is sometimes referred to as *the spectral sequence of reduction to the diagonal*. When $A = K$ is a field, we get nonzero terms in E^2 only if $q = 0$, and we recover the result that we derived earlier for the field case. The only other instance of this spectral sequence that we need to study in detail is the case where $A = V$, a Noetherian discrete valuation domain. Now, there are only two nonzero rows, corresponding to $q = 0$ and $q = 1$. We shall show that whenever the E^2 term of the spectral sequence of a double complex with filtration index p has nonzero terms only for $q = 0, 1$, the information given by the spectral sequence can be encoded in a long exact sequence. We are considering here the homological case, and so $d_r : E^2_{p,q} \to E^2_{p-r,q+r-1}$. We shall work this out in complete generality.

We have that $d_r = 0$ for $r \geq 3$, since, of any two terms indexed by values of q that differ by 2 or more, at least one is 0. Thus, the E^∞ term, which is an associated graded of the homology of the total complex $\mathcal{T}_\bullet$, is the same as the E^3 term, and there are only two q indices to worry about, 0 and 1. In particular, we have

$$E^\infty_{p,0} = E^3_{p,0} = \mathrm{Ker}\,(E^2_{p,0} \to E^2_{p-2,1})$$

since $\mathrm{Im}\,(E^{p+2,-1}) = \mathrm{Im}\,(0) = 0$, and

$$E^\infty_{p,1} = E^3_{p,1} = \mathrm{Ker}\,(E^2_{p,1} \to E^2_{p-2,2})/\mathrm{Im}\,(E^2_{p+2,0}) = E^2_{p,1}/\mathrm{Im}\,(E^2_{p+2,0})$$

since $E^2_{p-2,2} = 0$. Thus, the associated graded of $H_j(\mathcal{T}_\bullet)$ has only two graded pieces that might not be zero: one is the cokernel of $E^2_{p+2,0} \to E^2_{p,1}$ for $p = j-1$, which will be a submodule of $H_j(\mathcal{T}_\bullet)$, so that

$$E^2_{j+1,0} \to E^2_{j-1,1} \to H_j(\mathcal{T}_\bullet)$$

is exact, and the other, which will be quotient of $H_j(\mathcal{T}_\bullet)$ by by the image of $E^2_{j-1,1}$, is

$$\mathrm{Ker}\,(E^2_{j,0} \to E^2_{j-2,1}).$$

This fits together to give an exact sequence

$$E^2_{j+1,0} \to E^2_{j-1,1} \to H_j(\mathcal{T}_\bullet) \to E^2_{j,0} \to E^2_{j-2,1}$$

and these obviously paste together to give a long exact sequence:

$$\cdots \to E^2_{j-1,1} \to H_j(\mathcal{T}_\bullet) \to E^2_{j,0} \to E^2_{j-2,1} \to \cdots$$

where we may think of the leftmost three terms as a "typical" trio, and the rightmost term as the first term of the "next" trio.

We now make the resulting long exact sequence explicit in the case of the spectral sequence for reduction to the diagonal for the case where $A = V$, a complete Noetherian discrete valuation domain. The long exact sequence is:

$$\cdots \to \mathrm{Tor}^T_{j-1}(\hat{\mathrm{Tor}}^V_1(M,\, N),\, R) \to \mathrm{Tor}_j(M,\, N) \to \mathrm{Tor}^T_j(M \widehat{\otimes}_V N,\, V)$$
$$\to \mathrm{Tor}^T_{j-2}(\hat{\mathrm{Tor}}^V_1(M,\, N),\, R) \to \cdots$$

Math 615: Lecture of April 16, 2012

Let $R \to S$ be a ring homomorphism, let M be an R-module and let N be an S-module. Let $P_\bullet$ be a projective resolution of M over R and let $Q_\bullet$ be a projective resolution of N over S. We consider the spectral sequences of the double complex $P_\bullet \otimes_R Q_\bullet$. The homology of the column indexed by q is zero except in the zero spot, and so one gets a single row of column augmentations $P_\bullet \otimes_R N$ whose homology is $\mathrm{Tor}^R_\bullet(M,\, N)$, and this is also the homology of the total complex. The homology of the row indexed by p may be identified with $\mathrm{Tor}^R_\bullet(M, Q_p) \cong \mathrm{Tor}^R_\bullet(M, S) \otimes_S Q_p$, and then the homology of columns is $\mathrm{Tor}^S_p(\mathrm{Tor}^R_q(M,\, S), N)$ and we have $\mathrm{Tor}^S_p(\mathrm{Tor}^R_q(M,\, S),\, N) \underset{p}{\Longrightarrow} \mathrm{Tor}^R_{p+q}(M,\, N)$. This is called the *spectral sequence for change of rings for Tor*.

Now suppose that S is R/fR where f is not a zerodivisor in R. Then $\mathrm{Tor}^R_q(M,\, S) = 0$ except for $q = 0, 1$. Moreover, $\mathrm{Tor}^R_0(M, R/fR) = M \otimes_R R/fR \cong M/fM$, while

$\mathrm{Tor}_1^R(M,\, R/fR) \cong \mathrm{Ann}_M f$. The spectral sequence degenerates to give a long exact sequence:

$$\cdots \to \mathrm{Tor}_{j-1}^S(\mathrm{Ann}_M f,\, N) \to \mathrm{Tor}_j^R(M,\, N) \to \mathrm{Tor}_j^S(M/fM,\, N)$$
$$\to \mathrm{Tor}_{j-2}^R(\mathrm{Ann}_M f,\, N) \to \cdots$$

Here, M is an R-module while N is an R/fR-module.

Suppose that $x_1, \ldots, x_n \in R$ and M is an R-module. Let A be any ring that maps to R such as $\mathbb{Z}$ or R and let $B = A[X_1, \ldots, X_n]$. Make R into a B-algebra via the A-algebra map that sends X_j to x_j for all j. Let $N = B/(X_1, \ldots, X_n)$. Let B play the role of R in the long exact sequence of the preceding paragraph, and X_n the role of f, so that $S = A[X_1, \ldots, X_{n-1}]$. (We had to pass to the auxiliary ring B because x_n might not be a nonzerodivisor in R.) Note that when N is considered as a module over B, a Tor module with N over B may be calculated as Koszul homology with respect to $X_1, \ldots, X_n$, but if N is regarded as a module over $S = B/X_nB$, a Tor module over with N over S may be calculated as Koszul homology with respect to $X_1, \ldots, X_{n-1}$. The long exact sequence above yields at once:

Proposition. *Let M be any R-module, and $\underline{x} = x_1, \ldots, x_n \in R$. Then there is a long exact sequence:*

$$\cdots \to H_{j-1}(x_1, \ldots, x_{n-1}; \mathrm{Ann}_M x_n) \to H_j(\underline{x};\, M) \to H_j(x_1, \ldots, x_{n-1};\, M/x_nM)$$
$$\to H_{j-2}(x_1, \ldots, x_{n-1};\, \mathrm{Ann}_M x_n) \to \cdots .$$

Recall that over a local ring $(R,\, m,\, K)$, if $\underline{x} = x_1, \ldots, x_n \in m$, then $\chi(x_1, \ldots, x_n;\, M)$ is defined whenever $\ell\big(M/(\underline{x})M\big)$ is finite, i.e., whenever $\mathrm{Ann}_R M + (\underline{x})R$ is m-primary, in which case

$$\chi(\underline{x};\, M) = \sum_{j=0}^{n} (-1)^n \ell\big(H_j(\underline{x};\, M)\big).$$

Immediately from the long exact sequence in the Proposition, we get:

Corollary. *Let M be a finitely generated module over a local ring $(R,\, m)$, and let $\underline{x} = x_1, \ldots, x_n \in m$. Then*

$$\chi(\underline{x};\, M) = \chi(x_1, \ldots, x_{n-1}; M/x_nM) - \chi(x_1, \ldots, x_{n-1}; \mathrm{Ann}_M x_n)$$

when these are defined.

We can define *truncated Euler characteristics* as well. If $\underline{x} = x_1, \ldots, x_n$ and all of the modules $H_j(\underline{x};\, M)$ are finite length for $j \geq i$, we can let

$$\chi_i(\underline{x};\, M) = \sum_{j=i}^{n} (-1)^{j-i} \ell\big(H_j(\underline{x};\, M)\big).$$

Note that $\chi_0(\underline{x};\, M) = \chi(\underline{x};\, M)$ and that

$$\chi_1(\underline{x};\, M) = \ell\big(M/(\underline{x})M\big) - \chi(\underline{x};\, M)$$

whenever these are defined.

We already know the following result following the proof of Serre (cf. the proof of the Theorem on p. 2 of the Lecture Notes of March 14), but we give a new proof based on Lichtenbaum's ideas.

Theorem (J.-P. Serre). *Let M be finitely generated over a local ring $(R,\, m,\, K)$ and let $x_1, \ldots, x_n \in m$. If $M/(\underline{x})M$ has finite length, then $\chi(\underline{x}; M) \geq 0$ with equality iff $\dim(M) < n$.*

Proof. (S. Lichtenbaum) Note that this is true even if $n = 0$, where $\underline{x}$ is empty and $(\underline{x})R = 0$: we interpret $H_0(\emptyset;\, M)$ as $M/(0)M \cong M$, and so $\chi(\emptyset;\, M) = \ell(M) \geq 0$, and is 0 iff $M = 0$, i.e., iff $\dim(M) = -1 < 0$.

We use induction on n. If $n \geq 1$ and x_n is nilpotent on M then x_n^t kills M for some t, and then M has a finite filtration by modules $x_n^i M/x_n^{i+1}M$ for $0 \leq i < t$, each of which is killed by x_n. It suffices to prove that each of these has dimension at most $n-1$, and that $\chi(\underline{x};\, \_\,)$ vanishes for every factor, for $\chi(\underline{x};\, \_\,)$ is additive. Thus, this case reduces to the case where x_n kills M. Then $\dim(M) = \dim(R/I)$ where $I = \mathrm{Ann}_R M$, and the image of x_n is already 0 in this ring. Since $M/(\underline{x})M$ has finite length, $(x_1, \ldots, x_n)(R/I) = (x_1, \ldots, x_{n-1})R/I$ is primary to m/I, which shows that $\dim(R/I) \leq n-1$, as required. Moreover, when x_n kills M, we have from the preceding Corollary that, if $\underline{x}^- = x_1, \ldots, x_{n-1}$, then

$$\chi(\underline{x}; M) = \chi(\underline{x}^-;\, M/x_nM) - \chi(\underline{x}^-, \mathrm{Ann}_M x_n) = \chi(\underline{x}^-;\, M) - \chi(\underline{x}^-;\, M) = 0.$$

In the general case, let $N = \bigcup_t \mathrm{Ann}_M x_n^t$: the union stabilizes, and is equal to $\mathrm{Ann}_M x_n^t$ for any $t \gg 0$, so that N is killed by a power of x_n. Since $\chi(\underline{x};\, M) = \chi(\underline{x};\, M/N) + \chi(\underline{x};\, N)$, and we know that the last term is 0 by the preceding paragraph, and it follows that we may replace M by M/N (note that we know $\dim(N) \leq n-1$, and so the issue of whether $\dim(M) \leq n-1$ is also unaffected by this replacement). But x_n is not a zerodivisor on M/N: if $u \in M$ represents an element killed by x_n and x_n^t kills N, then $x_n^t(x_n u) = 0$, which implies that $u \in N$. Thus, we may assume without loss of generality that x_n is not a zerodivisor on M. But then $\chi(\underline{x};\, M) = \chi(x_1, \ldots, x_{n-1};\, M/x_nM)$, and the result follows from the induction hypothesis. $\square$

We next want to prove a subtle result about the behavior of truncated Euler characteristics of Koszul homology. We need a preliminary result, which generalizes **2.** in Problem Set #4.

Lemma. *Let $(R,\, m,\, K)$ be a local ring and M a finitely generated R-module of depth $\geq d$. Then M has no nonzero submodule N of dimension $< d$.*

Proof. We use induction on d. If $d = 0$ the statement is clear. Assume that $d \geq 1$.

If there were such a submodule there would be a maximal such submodule, since M has ACC. Let N be maximal, and let N' be any other submodule of M of dimension $< d$. Then $N \oplus N'$ maps onto $N + N' \subseteq M$, and so $N \subseteq N + N'$ and $N + N'$ has dimension $< d$. It follows that $N' \subseteq N$, and N is actually a largest submodule of M of dimension $\leq d$. Let $J = \mathrm{Ann}_R N$. Let $x_1, \ldots, x_d$ be a regular sequence on M. Then x_1 is not a zerodivisor on M, and, hence, not a zerodivisor on $N \subseteq M$.

We claim that x_1 is not a zerodivisor on M/N. To see this, suppose that $u \in M - N$ were such that $x_1 u \in N$. Then $Jx_1 u = 0$, and since x_1 is not a zerodivisor, we have that $Ju = 0$ as well. Then $\dim(N) = \dim(R/J) \geq \dim(Ru)$, and it follows that $u \in N$ after all.

Then N/x_1N injects into M/x_1M, for if $v \in N$ represents an element of N/x_1N mapping to 0, we have that $v = x_1 u$ with $u \in M$, and since $x_1 u$ is 0 in M/N, $u \in N$. But $\mathrm{depth}\, M/x_1M \geq d-1$, while $\dim(N/x_1N) = \dim(N) - 1 \leq d-2$ and N/x_1N is nonzero by Nakayama's lemma, contradicting the induction hypothesis. $\square$

We note for emphasis that in the result that follows we are assuming that the modules $H_j(\underline{x};\, M)$ have finite length for $j \geq i \geq 1$: but that we do not, however, need to assume this for $j < i$. Also note that if $H_i(\underline{x};\, M)$ has finite length, where M is Noetherian, then $H_j(\underline{x};\, M)$ has finite length for all $j \geq i$: if we localize at a prime not in the support of $H_i(\underline{x};\, M)$, it vanishes, and then the localization of $H_j(\underline{x};\, M)$ vanishes for all $j \geq i$ as well. Thus, supports of Koszul homology modules are descending with i. For a finitely generated module, finite length is characterized by the condition that the support be a finite set of maximal ideals (in the local case, that the support be at most the unique maximal ideal).

Theorem. *If (R, m) is local, $x_1, \ldots, x_n \in M$, and $\chi_i(\underline{x};\, M)$ is defined for a certain $i \geq 1$, then $\chi_i(\underline{x};\, M) \geq 0$, with equality iff $H_j(\underline{x};\, M) = 0$ for all $j \geq i$.*

Proof. If $i > 1$ we want to reduce to the case where $i = 1$ by taking modules of syzygies: the problem is that we do not necessarily know that $x_1, \ldots, x_n$ is a regular sequence in R. However, we may adjoin indeterminates $X_1, \ldots, X_n$ to R and map $S = R[X_1, \ldots, X_n] \to R$ by sending $X_j \mapsto x_j$, $1 \leq j \leq n$. The maximal ideal m of R contracts to $\mathcal{M} = (m, X_1, \ldots, X_n)S$, a maximal ideal of S, and we have a local map $S_{\mathcal{M}} \to R$ such that $X_j \mapsto x_j$, $1 \leq j \leq n$. The Koszul homology $H_\bullet(X_1, \ldots, X_n;\, M)$ is the same as the Koszul homology $H_\bullet(x_1, \ldots, x_n;\, M)$, and so the problem does not change if we replace R by S, and think of M as a module over the local ring S.

We may therefore assume without loss of generality that $x_1, \ldots, x_n$ is a regular sequence in R. We use induction on i to reduce to the case where $i = 1$. If $i > 1$, we may form a short exact sequence $0 \to M' \to R^b \to M \to 0$ for a suitable positive integer b, and since $x_1, \ldots, x_n$ is a regular sequence in R, we have that $H_j(\underline{x};\, R^b) = 0$ for all $j \geq 1$. The long exact sequence for Koszul homology then implies that

$$H_j(\underline{x};\, M) \cong H_{j-1}(\underline{x};\, M')$$

for $j \geq 2$, and by studying M' instead of M we reduce to the case where i is replaced by $i - 1$.

It remains to prove the result when $i = 1$. We use induction on n. The case $n \leq 1$ is obvious, and we assume that $n \geq 2$. We write ${}^{-}\underline{x} = x_2, \ldots, x_n$. From the long exact sequence for change of rings for Tor we have a finite long exact sequence for Koszul homology which has the following form (with x_1 now playing the role of x_n):

$$0 \to H_{n-1}({}^{-}\underline{x};\, \mathrm{Ann}_M x_1) \to H_n(\underline{x};\, M) \to H_n({}^{-}\underline{x};\, M/x_1M) \to \cdots \to$$

$$H_{j-1}({}^{-}\underline{x};\, \mathrm{Ann}_M x_1) \to H_j(\underline{x};\, M) \to H_j({}^{-}\underline{x};\, M/x_1M) \to H_{j-2}({}^{-}\underline{x};\, \mathrm{Ann}_M x_1)$$
$$\to \cdots \to H_0({}^{-}\underline{x};\, \mathrm{Ann}_M x_1) \to H_1(\underline{x};\, M) \to H_1({}^{-}\underline{x};\, M/x_1M) \to 0$$

where the final (i.e., rightmost) 0 displayed is $H_{-1}({}^{-}\underline{x};\, \mathrm{Ann}_M x_1) = 0$. The first three terms of the middle displayed line are a typical trio of terms. We know that $H_1(\underline{x};\, M)$ has finite length. We claim that all the other modules in this sequence have finite length: the point is that if we localize at any prime ideal P strictly contained in M, all terms vanish. To see this, note that since $H_1(\underline{x};\, M)_P$ vanishes, either the images of $x_1, \ldots, x_n$ in R_P generate the unit ideal, or else the images form a regular sequence in R_P. All of the modules in the sequence are killed by x_1 and by $(x_2, \ldots, x_n)$, and so vanish if $(x_1, \ldots, x_n)$ expands to the unit ideal. On the other hand, if $x_1, \ldots, x_n$ is a regular sequence in R_P then $\mathrm{Ann}_M x_1$ localizes to become 0, and it is evident that all terms vanish because the images of $x_2, \ldots, x_n$ are a regular sequence on the localization of M/x_1M. Since all terms have finite length, we may take the alternating sum of the lengths to conclude that

$$(\#) \quad \chi_1(\underline{x};\, M) = \chi_1(x_2, \ldots, x_n;\, M/x_1M) + \chi(x_2, \ldots, x_n;\, \mathrm{Ann}_M x_1).$$

The first term is nonnegative by the induction hypothesis and the second by the Theorem on p. 2. This shows that $\chi_1(\underline{x};\, M) \geq 0$.

It remains only to show that if $\chi_1(\underline{x};\, M) = 0$ then $x_1, \ldots, x_n$ is a regular sequence on M. But the vanishing of $\chi_1(\underline{x};\, M)$ implies that both terms in the sum on the right in (#) vanish. The induction hypothesis and the vanishing of the first of the two terms shows that $x_2, \ldots, x_n$ is a regular sequence on M/x_1M, which has depth $\geq n-1$ in consequence. The vanishing of the second term shows that $\dim(\mathrm{Ann}_M x_1) \leq n-2$, again by the Theorem on p. 2.

Let $x = x_1$. Let $W = \mathrm{Ann}_M x$. We only need to show that $W = 0$. Assume that $W \neq 0$, and choose s such that $W \subseteq x^{s-1}M$ but $W \not\subseteq x^sM$: with $W \neq 0$, we cannot have $W \subseteq x^sM$ for all s. We claim that $M/xM \cong x^jM/x^{j+1}M$ for $j \leq s-1$ via the map that sends the class of u to the class of x^ju. This evidently gives a well-defined map $M \twoheadrightarrow x^jM$ that maps xM to $x^{j+1}M$. Thus, we have a surjection $M/xM \twoheadrightarrow x^jM/x^{j+1}M$. We show that the map is injective by induction on j: the case where $j = 0$ is obvious. If u represents an element of the kernel, then $x^ju = x^{j+1}v$ with $v \in M$. Then $x(x^{j-1}u - x^jv) = 0$, so that $x^{j-1}u - x^jv \in W \subseteq x^jM$, and so $x^{j-1}u \in x^jM$. This shows that the class of u in M/xM maps to 0 in $M/x^{j-1}M$, and now the induction hypothesis shows that $u \in xM$.

Thus, we have $M/xM \cong x^{s-1}/x^sM$, and so the second module has depth at least $n-1$. But the image of W in $x^{s-1}M/x^sM$ is nonzero, since $W \not\subseteq x^sM$, and this gives

a submodule of $x^{s-1}M/x^sM$ that has dimension $\leq n-2$, contradicting the preceding Lemma. $\square$

Math 615: Supplementary Lecture of April 18, 2012

If M and N are finitely generated modules over a Noetherian regular ring R, we can define $\chi_i(M,\, N)$ whenever $\operatorname{Tor}_j^R(M,\, N)$ has finite length for $j \geq i$ as

$$\sum_{j\geq i}(-1)^{j-i}\ell\big(\operatorname{Tor}_j^R(M,\, N)\big).$$

If it is necessary to indicate over which ring we are calculating $\chi_i(M,\, N)$, we use the ring as a superscript, and write $\chi_i^R(M,\, N)$.

The sum will be finite, since over a regular ring, every finitely generated module has finite projective dimension, and all the Tor modules will vanish for $j > \operatorname{pd}_R M$ (and for $j > \operatorname{pd}_R(N)$). For $\chi_0(M,\, N)$ one writes instead $\chi(M,\, N)$: this was defined in the local case in the first Extra Credit Problem in Problem Set #5: it is the Serre intersection multiplicity. We are almost ready to prove that if $\operatorname{Tor}_i^R(M,\, N) = 0$ over the regular ring R, then $\operatorname{Tor}_j^R(M,\, N) = 0$ for all $j \geq i$. We first need to observe:

Corollary (S. Lichtenbaum). *Let R be a regular local ring whose completion is isomorphic with a formal power series ring over a field K or over a complete Noetherian discrete valuation domain $(V,\, zV)$. Let M and N be finitely generated R-modules. Suppose that $i \geq 1$ and that either*

(1) *the base ring is a field or*
(2) *the base ring is a Noetherian discrete valuation domain and z is not a zerodivisor on M (or on N) or*
(3) *$i \geq 2$.*

Then $\operatorname{Tor}_i^R(M,\, N) = 0$ implies that $\operatorname{Tor}_j(M,\, N) \geq 0$ for $j \geq i$, and if $\chi_i(M,\, N)$ is defined it is nonnegative and vanishes iff $\operatorname{Tor}_j^R(M,\, N) = 0$ for $j \geq i$.

Proof. Note that (3) follows from (2) by replacing M by a module of syzygies M', and using that $\operatorname{Tor}_j^R(M,\, N) \cong \operatorname{Tor}_{j-1}^R(M,\, N)$ for $j \geq 2$. Note that M' is torsion-free over V, since it is a submodule of a free module.

In cases (1) and (2)

$$\operatorname{Tor}_j^R(M,\, N) \cong \operatorname{Tor}_j^T(M\widehat{\otimes}N,\, R).$$

We have already seen this if the base is K. In case (2), when the base is V, the fact that z is not a zerodivisor on M, say, implies that $\hat{\operatorname{Tor}}_j^V(M,\, N) = 0$ for $j \geq 1$, by the Theorem on the first page of the Lecture Notes of April 11. The long exact sequence that concludes the Lecture Notes of April 13 gives the required isomorphisms at once.

We can now rewrite the Tors as Koszul homology, and the result is immediate from our prior results on Koszul homology: in particular, the last statement follows from the final Theorem of the Lecture Notes of April 16. $\square$

The restriction that $i \geq 2$ was removed independently by O. Gabber, unpublished, and in [M. Hochster, *Euler characteristics over unramified regular local rings*, Illinois J. Math. **28** (1984) 281–5] making additional use of the spectral sequence of reduction to the diagonal over V.

Theorem (S. Lichtenbaum). *Let R be a regular Noetherian ring and let M and N be finitely generated R-modules. If* $\operatorname{Tor}_i(M,\, N) = 0$ *then* $\operatorname{Tor}_j^R(M,\, N) = 0$ *for all $j \geq i$.*

Moreover, if $j \geq i$ then $\operatorname{Supp}\big(\operatorname{Tor}_j^R(M,\, N)\big) \subseteq \operatorname{Supp}\big(\operatorname{Tor}_i^R(M,\, N)\big)$ *and if* $\operatorname{Tor}_i^R(M,\, N)$ *has finite length then so does* $\operatorname{Tor}_j^R(M,\, N)$.

Proof. The final statements are immediate from the first statement and the fact that Tor commutes with localization, so that we need only prove the first statement.

If $i > 1$ we may reduce to the case $i = 1$ by repeatedly replacing M by its first module of syzygies: i decreases by 1 with each such replacement. Therefore, we may assume that $i = 1$. If there is a counterexample we may localize at a prime in the support of $\operatorname{Tor}_j^R(M,\, N)$ for $j > 1$. Thus, we may assume that R is local, say of Krull dimension d. Now localize at a minimal prime of the support of $\bigoplus_{j=2}^{d} \operatorname{Tor}_j^R(M,\, N)$. We may consequently assume that R is regular local, that $\operatorname{Tor}_1^R(M,\, N) = 0$, that some $\operatorname{Tor}_j^R(M,\, N) \neq 0$ for $j > 1$, but that all $\operatorname{Tor}_j^R(M,\, N)$ have finite length for $j > 1$. Since $\widehat{R}$ is faithfully flat over R, we may apply $\widehat{R} \otimes_R \_$, and so assume that R is complete as well.

We already know the case where R contains a field. In general, in the case where R does not contain a field, we may assume from the structure theory of complete regular local rings that $R = T/fT$, where T is formal power series over a Noetherian discrete valuation domain: see the Theorem at the top of p. 2 of the Lecture Notes of April 9. The long exact sequence for change of rings for Tor yields

$$\cdots \to \operatorname{Tor}_{j-1}^R(M,\, N) \to \operatorname{Tor}_j^T(M,\, N) \to \operatorname{Tor}_j^R(M,\, N) \to \operatorname{Tor}_{j-2}^R(M,\, N) \to$$

$$\cdots \to \operatorname{Tor}_1^R(M,\, N) \to \operatorname{Tor}_2^T(M,\, N) \to \operatorname{Tor}_2^R(M,\, N) \to W \to 0$$

where W is the image of $\operatorname{Tor}_2^R(M,\, N)$ in $\operatorname{Tor}_0^R(M,\, N) = M \otimes_R N$. All the $\operatorname{Tor}_j^T(M,\, N)$ for $j \geq 2$ have finite length, since each is both preceded and followed in the exact sequence above by a value of $\operatorname{Tor}_i^R(M,\, N)$ of finite length. The alternating sum of the lengths of the terms is 0, and this yields

$$\ell(W) + \chi_2^T(M, N) = \chi_2^R(M,\, N) + \chi_1^R(M,\, N)$$

But almost all of the terms in $\chi_2^R(M,\, N) + \chi_1^R(M,\, N)$ cancel, leaving $\ell\big(\operatorname{Tor}_1^R(M,\, N)\big) = 0$. Therefore $\ell(W) = 0 + \chi_2^T(M, N) = 0$, and by part (3) of the preceding Corollary, $\chi_2^T(M,\, N) \geq 0$. It follows that $W = 0$, and that $\chi_2^T(M, N) = 0$. Again, by part (3) of the preceding Corollary we have that $\operatorname{Tor}_j^T(M,\, N) = 0$ for all $j \geq 2$. From the long exact sequence, we have that $\operatorname{Tor}_2^R(M, N) = 0$, and we also get $Tor_j^R(M,\, N) \cong \operatorname{Tor}_{j-2}^R(M,\, N)$ for $j \geq 3$. It follows that all of the modules $\operatorname{Tor}_j^R(M,\, N) = 0$ for $j \geq 1$, as required, $\square$